**1.1. Псевдослучайные числа**

При статистическом моделировании систем одним из основных вопросов является учёт стохастических воздействий. Для их формирования обычно используют последовательности случайных чисел с заданными вероятностными характеристиками.

Количество случайных чисел, требуемых для получения статистически устойчивых оценок параметров процессов функционирования системы S при реализации моделирующего алгоритма на ЭВМ, колеблется в достаточно широких пределах в зависимости от

- класса объекта моделирования,

- вида оцениваемых параметров,

- необходимой точности,

- достоверности результатов моделирования.

Метод статистического моделирования на ЭВМ

- большое число операций => большая доля машинного времени расходуется на действия со случайными числами.

- результаты статистического моделирования существенно зависят от качества исходных последовательностей случайных чисел.

* Простые и экономичные способы формирования последовательностей случайных чисел требуемого качества во многом определяет возможности практического использования машинного моделирования систем.

Алгоритмический способ получения последовательностей случайных чисел в настоящее время считается наиболее эффективным - каждое случайное число вычисляется с помощью соответствующей программы по мере возникновения необходимости.

Программная имитация случайных воздействий любой сложности сводится к генерированию некоторых стандартных (базовых) случайных процессов и к их последующему функциональному преобразованию. В качестве базового может быть принят любой удобный процесс. Как показывает практика, оптимальным базовым процессом является последовательность чисел {X}=x1,x2,…,xn, представляющих собой реализацию равномерно распределенной на интервале (0,1) случайной величины ξ, или - в статистических терминах - повторную выборку из равномерно распределенной на (0,1) генеральной совокупности значений величины ξ.

*Непрерывная случайная величина ξ имеет равномерное распределение в интервале (a,b), если ее функции плотности fξ(x) и функция распределения Fξ(x) соответственно имеют вид:*



*Числовые характеристики случайной величины ξ, принимающей значения x - математическое ожидание, дисперсию и среднее квадратическое отклонение соответственно*:



Для случайной величины равномерно распределенной на интервале (0,1), когда границы интервала a=0 и b=1, функция плотности и функция распределения соответственно имеют вид:



Такое распределение имеет математическое ожидание

M[ξ]=0.5 и дисперсию D[ξ]= (≈0,083), а σξ= (≈0,3).

Это распределение получить на цифровой ЭВМ невозможно, так как машина оперирует с n-разрядными числами. Поэтому на ЭВМ вместо непрерывной совокупности равномерных случайных чисел интервала (0,1) используют дискретную последовательность из 2n случайных чисел того же интервала. Закон распределения такой дискретной последовательности называют квазиравномерным распределением.

СВ ξ, имеющая квазиравномерное распределение в интервале (0,1) принимает значения  с вероятностями pi=i/(2n-1), i=0,…,2n-1.

Математическое ожидание и дисперсия квазиравномерной случайной величины соответственно имеют вид:



Таким образом, математическое ожидание квазиравномерной случайной величины совпадает с математическим ожиданием равномерной случайной последовательности интервала (0,1), а дисперсия отличается только множителем , который при достаточно больших n близок к единице.

На ЭВМ невозможно получить идеальную последовательность случайных чисел хотя бы потому, что на ней можно оперировать только с конечным множеством чисел. Кроме того, для получения значений x случайной величины ξ используются формулы (алгоритмы). Поэтому такие последовательности, являющиеся по своей сути детерминированными, называются псевдослучайными.

Набор требований, которым должен удовлетворять идеальный генератор:

- полученные с помощью идеального генератора псевдослучайные последовательности чисел должны состоять из квазиравномерно распределенных чисел,

- содержать статистически независимые числа,

- быть воспроизводимыми,

- иметь неповторяющиеся числа,

- получаться с минимальными затратами машинного времени,

- занимать минимальный объем машинной памяти.

Наибольшее применение в практике моделирования на ЭВМ для генерации последовательностей псевдослучайных чисел находят алгоритмы вида:

xi+1=Ф(xi),

представляющие собой рекуррентные соотношения первого порядка, для которых начальное число x0 и постоянные параметры заданы.

Рассмотрим некоторые процедуры получения последовательностей псевдослучайных квазиравномерно распределенных чисел, которые нашли применение в практике статистического моделирования систем на ЭВМ.

1. **Метод серединных квадратов.**

Имеется 2n - разрядное число, меньшее 1: xi=0,a1a2…a2n. Возведем его в квадрат: xi2=0,b1b2…b4n, а затем выделим средние 2n разрядов xi+1=bn+1bn+2…b3n, которые и будут являться очередным числом псевдослучайной последовательности.

Недостаток этого метода - наличие корреляции между числами последовательности, а в ряде случаев случайность вообще может отсутствовать. Например, если x0=0.4500, то (x0)2=0.20250000, x1=0.2500, (x1)2=0.06250000, , (x2)2=0.06250000, x3=0.2500 и т.д. Кроме того, при достижении некоторых  вообще может наблюдаться вырождение последовательности, т.е. xi=0 при . Это существенно ограничивает возможности использования метода серединных квадратов.

1. **Мультипликативный метод**

Задает последовательность неотрицательных целых чисел , не превосходящих , по формуле:



т.е. частный случай соотношения при .

В силу детерминированности метода получаются воспроизводимые последовательности. Требуемый объем машинной памяти при этом минимален, а с вычислительной точки зрения необходим последовательный подсчет произведения двух целых чисел, т.е. выполнение операции, которая быстро реализуется современными ЭВМ.

Для машинной реализации наиболее удобна версия

,

где  - число цифр в системе счисления, принятой в ЭВМ ( для двоичной и  для десятичной машины);

 - число бит в машинном слове.

Тогда вычисление остатка от деления на  - выделение  младших разрядов делимого,

преобразование целого числа  в рациональную дробь из интервала (0, 1) - подстановка слева от  двоичной или десятичной запятой.

Алгоритм построения последовательности для двоичной машины  сводится к выполнению следующих операций:

1) выбрать в качестве  произвольное нечетное число;

2) вычислить коэффициент , где  - любое целое положительное число;

3) найти произведение , содержащее не более  значащих разрядов;

4) взять  младших разрядов в качестве первого члена последовательности , а остальные отбросить;

5) определить дробь  из интервала (0,1);

6) присвоить ;

7) вернуться к п.З.

1. **Смешанный метод**

Позволяет вычислить последовательность неотрицательных чисел , не превосходящих , по формуле

,

т.е. в отличие от мультипликативного метода .

С вычислительной точки зрения смешанный метод генерации сложнее мультипликативного на одну операцию сложения, но при этом возможность выбора дополнительного параметра позволяет уменьшить возможную корреляцию получаемых чисел.

Качество конкретной версии такого генератора можно оценить только с помощью соответствующего машинного эксперимента.

В настоящее время почти все библиотеки стандартных, программ универсальных ЭВМ для вычисления последовательностей равномерно распределенных случайных чисел основаны на конгруэнтной процедуре.

Вычислительный алгоритм Д.Лемера - линейно-конгруэнтный метод генерации псевдослучайных чисел.

*Xi+1 = (aXi + c) mod m*

*a*,*c,m* — некоторые положительные целые числа 

Качество РРСЧ, весьма существенно зависит от выбора *a*, *c, m*, *X0* где параметры  и *X0* влияют на статистические свойства получаемых чисел, а параметр - на период их повторения.

Значение переменной *X0* должно быть:

а) меньше;

в) достаточно большим;

г) желательно простым числом;

г) содержать в двоичном представлена сравнительно большее число единиц.

В таблице ниже приведены наиболее часто используемые параметры линейных конгруэнтных генераторов, в частности, в стандартных библиотеках различных компиляторов (функция rand()).

При реализации выгодно выбирать M = 2n, где n — число битов в машинном слове, поскольку это позволяет избавиться от относительно медленной операции приведения по модулю.

|  |  |  |  |
| --- | --- | --- | --- |
| **Название библиотеки** | ***m*** | ***a*** | ***c*** |
| Numerical Recipes | 232 | 1664525 | 1013904223 |
| MMIX by Donald Knuth | 264 | 6364136223846793005 | 1442695040888963407 |
| Borland C/C++ | 232 | 22695477 | 1 |
| GNU Compiler Collection | 232 | 69069 | 5 |
| ANSI C: Open Watcom, Digital Mars, Metrowerks, IBM VisualAge C/C++ | 232 | 1103515245 | 12345 |
| Borland Delphi, Virtual Pascal | 232 | 134775813 | 1 |
| Microsoft Visual/Quick C/C++ | 232 | 214013 | 2531011 |
| Apple CarbonLib | 231 -1 | 16807 | 0 |

Приведенное соотношение имеет следующий смысл: *Xi+1* равно остатку от деления *(aXi + c)* на *m*.

Запишем алгоритм в виде пошаговой процедуры.

Ш а г 1. Коэффициент *a* умножается на число *Xi*

Ш а г 2. К результату умножения (*aXi*) прибавляется числ *с*

Ш а г 3. Результат сложения *(aXi + c)*  делится на *m*

*aXi + c = q·m+ Xi+1*

где *qm* - целая часть (*q* = 0,1,2,...), *Xi+1* - остаток от деления .

Ш а г 4. Остаток от деления *Xi+1* делится на *m*, чтобы получить искомое случайное число между нулем и единицей:

Следует отметить, что данный метод не обладает криптографической стойкостью, однако входит в большинство современных стандартных библиотек различных компиляторов.

Пример.

х0 = 7(0111)

а = 5 (0101)

с = 3 (0011)

m = 2n

n – число бит в машинном слове

Пусть n = 4, тогда m = 24 = 16

*х1* = (*a·х0 + c) mod m* = (5·7 + 3) *mod* 16 = 38 (00100110) *mod* 16 = 6 (0110)

*х1\** = 6 /16 = 0,375

*х2* = *a·х1 + c* = 5·6 + 3 = 33

*х2* = (*a·х1 + c) mod m* = (5·6 + 3) *mod* 16 = 33 (00100001) *mod* 16 = 1 (0001)

*х2\** = 1 /16 = 0,063

**……………….**

**Математическое ожидание** квазиравномерной случайной величины:



N – количество элементов массива, – элемент нашей последовательности.



**Дисперсия квазиравномерной случайной величины - мера разброса случайной величины, т.е. её отклонение от математического ожидания.**



N – количество элементов массива, – математическое ожидание, – элемент нашей последовательности.



СКО квазиравномерной случайной величины - показатель рассеивания значений случайной величины относительно её математического ожидания.



Эффективность статистического моделирования систем на ЭВМ и достоверность получаемых результатов существенным образом зависят от качества исходных (базовых) последовательностей псевдослучайных чисел, которые являются основой для получения стохастических воздействий на элементы моделируемой системы.

Проверка качества последовательностей РРСЧ

1) Проверка равномерности

2) Проверка стохастичности

3) Проверка независимости

Проверка равномерности последовательностей псевдослучайных квазиравномерно распределенных чисел {хi} может быть выполнена по гистограмме или с использованием косвенных признаков.

а) Проверка по гистограмме.

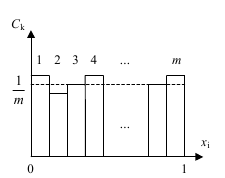
Суть проверки по гистограмме сводится к следующему. Выдвигается гипотеза о равномерности распределения чиел в интервале (0 1). Затем интервал (0 1) разбивается на m равных частей. При генерации последовательности РРСЧ подсчитывается количество попаданий Nk в каждый из m подинтервалов. Вычисляется относительная частота попадания случайных чисел последовательности {хi} в каждый из подинтервалов

Ck= Nk/N,

где N − общее количество чисел в последовательности {хi}.

Очевидно, что при равномерности последовательности чисел, частоты должны быть близкими при достаточно больших N к теоретической вероятности попадания в подинтервалы, равной 1/m.

Оценка степени приближения, т. е. равномерности последовательности{хi}, может быть проведена с использованием критериев согласия. На практике обычно принимается m = 20÷50, N = (102÷103)*m*.



б) Проверка по косвенным признакам.

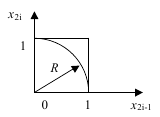
Вся последовательность {хi} разбивается на пары чисел:

(x1, x2), (x3, x4), ... , (x2i-1, x2i), ... , (xN-1, xN).

Затем подсчитывают число пар K, для которых выполняется условие:

<1

Геометрически это означает, что точка с координатами (x2i-1, x2i) расположена внутри четверти круга радиуса R=1, вписанного в единичный квадрат.



В общем случае точка (x2i-1, x2i) всегда попадет внутрь единичного квадрата. Тогда теоретическая вероятность попадания этой точки в четверть круга равна отношению площади четверти круга к площади единичного квадрата:

P = S1/4 круга/Sквадрата = π/4.

Если числа последовательности {хi} равномерны, то в силу закона больших чисел теории вероятностей при больших N относительная частота попадания точки в единичный квадрат, равная отношению числа K пар (x2i-1, x2i), для которых проверочное условие выполнилось к общему числу N/2 пар последовательности должна сходиться к Р:

