УДК 621.391:004.73

В.В. Веретельник

Черкасский государственный технологический университет, Черкассы

ЛИНЕЙНЫЙ ГЕНЕРАТОР КОНГРУЭНТНЫХ ЧИСЕЛ

Рассматриваются некоторые мало исследованные свойства конгруэнтных последовательностей чисел, облегчающие подбор изменяемых параметров конгруэнтных генераторов. Описывается программный генератор конгруэнтных чисел, созданный для облегчения подбора сменных параметров под заданные требования к порождаемой последовательности. Приводится методика его использования для решения практических задач.

Ключевые слова: *генератор случайных чисел, генератор конгруэнтных чисел, равномерно распределенная последовательность чисел.*

Введение

Генератор конгруэнтных чисел – это устройство, которое производит итерационно вычисление последующего слова по его предшествующему значению следующим образом:

$$s(n) = \left| Ks(n-1) + C \right|_M , \qquad (1)$$

где K,C,M - численные параметры генератора, s(n) и s(n-1) – слова, порожденные генератором в текущий - «n» и в предшествующий - «(n-1)» дискретный момент времени. Начальное значение s(n-1), загружаемое при пуске генератора называется «вектор начальной загрузки - ВНЗ» и обозначается как s(0). Такие генераторы случайных чисел (ГСЧ) порождают псевдослучайную периодически повторяемую последовательность чисел (ПСП), которая представляет последовательность вычетов по модулю M и принимает конечное множество значений из интервала [0,(M-1)]. Несмотря на все недостатки им присущие, они широко используются во всех сферах человеческой деятельности, где необходимо использование случайных последовательностей чисел. Основным недостатком таких ГСЧ является то, что правила выбора параметров K,C,M для получения последовательности с нужными свойствами не определены. Сразу отметим, что из (1) следует, что значение вычета выражения $Ks(n-1)+C$ может принимать значения из интервала $[0, (M-1)]$, но вовсе не обозначает, что порождаемая ПСП содержит все слова из области определения. Многочисленные попытки модифицировать метод получения конгруэнтных чисел, например, использованием свойств чисел Фибоначчи [1], по существу ничего не дали. Не намного лучше обстоят дела в области теоретического анализа процесса формирования ПСП с нужными параметрами и методов тестирования ГСЧ. Уникальный труд Кнута [2] показал всю сложность проблемы, обосновал несколько различных критериев оценки ПСП и привел общие рекомендации по выбору параметров K,C,M, тоже , по существу, мало что решающие.

Выделение нерешенных ранее частей общей проблемы

Вместе с тем, применение линейных генераторов конгруэнтных чисел необходимо в целом ряде практически важных случаев, например, таких как создание таблиц перестановок, применяемых в процедурах декорреляции последовательностей и в процедурах криптографических преобразований. При всей глубине анализа принципов генерации ПСП генераторами конгруэнтных чисел, выполненного в работах [1, 2] аналитических выражений, связывающих параметры K, C, s(0) со статистикой генерируемой последовательности не существует. Это значит, что задача подбора этих параметров выполняется перебором «в слепую», что не гарантирует решение задачи за заданный интервал времени и приводит к необходимости создания средств (например, программных) для подбора параметров M, K, C, s(0), которые обеспечивают создание генератора конгруэнтных чисел с заданными свойствами.

Целью настоящей работы является создание программного линейного генератора конгруэнтных чисел, решающего задачи быстрого подбора параметров линейного генератора конгруэнтных чисел под заданные требования и методик его применения при решении практических задач.

Постановка задачи

С целью решения поставленной задачи в данной работе определены некоторые очевидные рекомендации по выбору параметров линейного генератора конгруэнтных чисел, обеспечивающие получение необходимых свойств генерируемой последовательности, дано описание программного генератора конгруэнтных чисел, приведена методика его применения для решения ряда практически важных задач.

Решение задачи

Определим некоторые очевидные рекомендации по выбору параметров линейного генератора конгруэнтных чисел, обеспечивающие получение необходимых свойств генерируемой последовательности. Прежде всего, отметим, что из уравнения линейного генератора конгруэнтных чисел (1) следует:

– $0 \le S(n) \le (M-1)$;

– генерируемая последовательность чисел равномерно распределена, если период повторения псевдослучайной последовательности чисел (ПСП) T = M, если T < M, то ошибка воспроизведения случайной величины отлична от нуля;

– число M определяет область определения случайной величины.

Отсюда следует, что выбор параметров линейного генератора конгруэнтных чисел необходимо начинать с выбора параметра M, как параметра, который определяет область определения случайной величины. Приступим к выбору значения параметров K, C и S(0) для чего перепишем равенство (1) в виде:

$$S(n) = \big|\,|KS(n-1)|_M + |C|_M\big|_M. \qquad (2)$$

Положим:

$$K = |K_0 + \nu M|_M,\ C = |C_0 + \nu M|_M,\ \nu \in \overline{1,\infty}.$$

Тогда первое и второе слагаемое в выражении (2), примут вид:

$$|(K_0 + \nu M)\cdot S(n-1)|_M \quad \text{и} \quad |C_0 + \nu M|_M.$$

Вычислив каждое из слагаемых получим:

$$|(K_0 + \nu M)\cdot S(n-1)|_M = |K_0 \cdot S(n-1)|_M; \qquad (3)$$

$$|C_0 + \nu M|_M = |C_0|_{M/}. \qquad (4).$$

Из полученных равенств (3) и (4) следует, что параметры K и C следует выбирать из условия

$$0 < K < M;\quad 0 \le C < M. \qquad (5)$$

Отметим также, что в случае, если требуется, что бы последовательность чисел была равномерно распределена, необходимо, что бы в ней каждое из чисел 0, 1,2…(M – 1) содержалось ровно по одному разу. В этом случае выбор параметра S(0) роли не играет, т.е. производится из условия

$$S(0) \in \overline{0,(M-1)}. \qquad (6)$$

С учетом изложенного сведем вместе рекомендации по выбору параметров линейного генератора конгруэнтных чисел:

- параметр M определяется областью определения случайной величины и численно равен длине ПСП, M = T;

- параметры K и C определяются подбором из условия K, C < M;

- для генерации равномерно распределенных чисел численное значение параметра S(0) не играет роли, S(0) есть любое число интервала $\overline{0,(M-1)}$.

Как показано в [3] при фиксированных параметрах K и C, перебором вектора начальной загрузки по принципу «решета Эратосфена », можно определить граф состояний ГСЧ, как совокупность непересекающихся циклов. В зависимости от выбора параметров K, C и ВНЗ, цикл может содержать одно или несколько слов из множества M, а может содержать и все слова этого множества. Здесь будем рассматривать следующие случаи: четное M; нечетное M.

Нечетное M может быть простым или составным. В частности при M - простом граф состояний содержит d циклов по слов каждое и один нуль цикл. При этом $d \cdot t = (M-1)$. С учетом ноль цикла число вершин графа состояний равно M, что и создает предпосылки для объединения всех обособленных циклов в один сверхцикл с числом вершин равным M. Для четного и нечетного составного M требуются дополнительные исследования структуры циклов, отметим лишь, что и в том, и другом случае может быть получен цикл T = M или d циклов длиной t, которые могут принимать любое значение, определяемое разложением числа M или числа (M – 1) на простые сомножители. Заметим, что структура графа полностью определяется значением параметров K и C генератора. Пусть, например, M = 101, тогда (M – 1) = 100= 2 Ч 2 Ч 5 Ч 5. Отсюда следует, что граф состояний содержит один нуль цикл и одну из комбинаций циклов: 1 Ч 100,2 Ч 50, 4 Ч 25, 5 Ч 20,10 Ч 10. Для M = 100 граф состояний также имеет одну из комбинации циклов: 1 Ч 100,2 Ч 50, 4 Ч 25, 5 Ч 20,10 Ч 10, но не имеет нуль цикла. Выбор конкретной топологии графа определяется решаемой задачей. В частности, равновероятная последовательность при M = 101 может быть получена при структуре графа 1 Ч 100 добавлением нуль - цикла (конкатенацией цикла длиной 100 и цикла, длиной единица), а при структуре графа 5 Ч 20 конкатенацией 5циклов длиной 20 слов и нуль цикла, длиной единица.

Исходя из изложенных подходов, создан программный генератор конгруэнтных чисел, панель управления которого приведена на рис. 1.

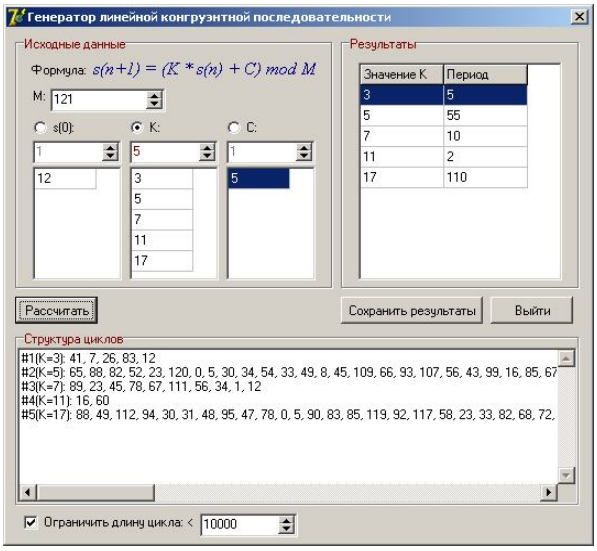

Рис. 1. Панель управления генератора

В панель управления генератором встроены следующие окна:

- окно параметра М, обеспечивающее изменение параметра М в диапазоне - 0….65535;
- окно параметра К, обеспечивающее изменение параметра К в диапазоне - 0…..65535;
- окно параметра С, обеспечивающее изменение параметра С в диапазоне - 0……65535;

Окна, задания численного значения параметра, изменяемого при подборе.

В окне параметров К, С, s(0) можно задавать как один , так и ряд значений параметра, ограничение длины цикла меняется $0..2^{32}$. Предусмотрены следующие режимы ГСЧ:

- подбор параметров ГСЧ для получения ПСП заданной длины;
- вычисление каждого из слов ПСП при заданных параметрах;
- вычисление представителей циклов;
- сохранение полученных результатов с последующим формирования файла в формате *.txt.

Рассмотрим методику использования генератора для некоторых практических задач. Прежде всего, отметим, что вначале задаем область определения случайной величины, откуда вытекает значение параметра М.

Пример 1. Пусть требуется создать генератор равномерно распределенных случайных чисел в диапазоне 0,…99.

Методика:

1) выберем четное М=100 (в окне М – 100);

2) при М=100 генерируемые числа будут меняться в интервале 0…99, поэтому в окне s(0) набираем любое число из этого интервала, например 6;

3) выберем также случайным образом из этого диапазона и число С=7; теперь будем подбирать параметр К, для чего попробуем взять 7 значений параметра К, которые наберем в окне К(6,7,8, 21,22,23) и нажмем клавишу «Рассчитать»;

4) полученный результат приводится в блокноте и имеет следующий вид:

M = 100, s(0) = 6, C = 7, K = 6, 7, 8, 21, 22 ,23/

Результаты:

Значение К	Период
6	26
7	4
8	20
21	100
22	21
23	20

Отсюда видно, что длина ПСП Т=100 получается при М=100, s(0)= 6, С=7, К=21

Можно подобрать и другие значения К для получения Т=100,например, К=21,41,61….

Пример 2. Пусть требуется создать таблицу перестановок на интервале Т=100

Используя результат примера1 зададим:

M = 100, s(0) = 6, C = 7, K = 61.

Нажмем клавишу «Рассчитать» в блокноте получим результат:

73, 60, 67, 94, 41, 8, 95, 2, 29, 76, 43, 30, 37, 64, 11, 78, 65, 72, 99, 46, 13, 0, 7, 34, 81, 48, 35, 42, 69, 16, 83, 70, 77, 4, 51, 18, 5, 12, 39, 86, 53, 40, 47, 74, 21, 88, 75, 82, 9, 56, 23, 10, 17, 44, 91, 58, 45, 52, 79, 26, 93, 80, 87, 14, 61, 28, 15, 22, 49, 96, 63, 50, 57, 84, 31, 98, 85, 92, 19, 66, 33, 20, 27, 54, 1, 68, 55, 62, 89, 36, 3, 90, 97, 24, 71, 38, 25, 32, 59, 6.

Учитывая, что при декорреляции слова входного массива переставляются в выходной массив по определенному правилу, полученный результат следует читать так:

Первое слово входного массива переставить на 73 позицию в выходном массиве, второе слово входного массива переставить на 60 позицию в выходном массиве, третье слово входного массива переставить на 67 позицию в выходном массиве и т.д. до конца, где сотое слово входного массива переставить на 6 позицию в выходном массиве.

Следует обратить внимание, что полученную таблицу необходимо проверить на корректность, это обозначает, что таблица должна обеспечить перестановку всех (без исключения) слов массива. Здесь в таблице 39-ое слово входной последовательности следует установить на 39 позицию в выходном массиве. Это обозначает, что 39 слово не переставляется.

Исправить ситуацию можно переставив 39 слово, на какое либо иное место, например, поменяв местами смежные слова.

Выполнив перестановку 39 слова на смежную (справа) позицию окончательно получим следующую корректную таблицу перестановок:

73, 60, 67, 94, 41, 8, 95, 2, 29, 76, 43, 30, 37, 64, 11, 78, 65, 72, 99, 46, 13, 0, 7, 34, 81, 48, 35, 42, 69, 16, 83, 70, 77, 4, 51, 18, 5, 12, 86, 39, 53, 40, 47, 74, 21, 88, 75, 82, 9, 56, 23, 10, 17, 44, 91, 58, 45, 52, 79, 26, 93, 80, 87, 14, 61, 28, 15, 22, 49, 96, 63, 50, 57, 84, 31, 98, 85, 92, 19, 66, 33, 20, 27, 54, 1, 68, 55, 62, 89, 36, 3, 90, 97, 24, 71, 38, 25, 32, 59, 6.

Пример 3. Пусть требуется создать генератор равномерно распределенных случайных чисел в диапазоне 0,…99.

Методика:

1) выберем простое М=101 (в окне М набираем 101);

2) при М=101 генерируемые числа с учетом ноль цикла будут меняться в интервале 0…100, поэтому в окне s(0) набираем любое число из этого интервала, например 6;

3) выберем так же случайным образом из этого диапазона и число C=7; теперь будем подбирать параметр K, для чего попробуем взять 7 значений параметра K, которые наберем в окне K несколько его значений и нажмем клавишу «Рассчитать»;

4) полученный результат приводится в блокноте и имеет следующий вид:

M = 101, s(0) = 6, C = 7,
K = 3, 5, 6, 7, 8, 9, 10, 11, 12, 13.

Результаты:

Значение K	Период
3	100
5	25
6	10
7	100
8	100
9	50
10	4
11	100

Отсюда видно, что K = 3, 7, 8, 11 обеспечивают T=100, при этом последовательность с K = 8 не содержит в своем составе числа 100. Это значит, что она содержит числа 0…99, что и требуется по условию задачи. Вывод: оптимальное решение M = 101, s(0) = 6, C = 7, K = 8 .

Пример 4. Пусть требуется создать генератор равномерно распределенных случайных чисел в диапазоне 0,…100 с большим периодом повторения последовательности (за счет рандомизации). Выберем простое M = 101, тогда (M – 1) = 100. Выберем конструкцию графа 5 Ч 20 (5 циклов длиной 20 каждый, плюс ноль цикл). В результате подбора параметров по ранее изложенным методикам получим требуемые параметры генератора и представителей всех циклов.

Исходные данные

M = 101, K = 41, C = 7, s(0): 0, 1, 2, 3, 9, 68.

Результаты:

Значение s(0)	Период
0	20
1	20
2	20
3	20
9	20
68	1 (это ноль цикл).

Структура циклов:

#1(s=0): 7, 92, 42, 12, 95, 64, 5, 10, 13, 35, 28, 44, 94, 23, 41, 72, 30, 25, 22, 0;

#2(s=1): 48, 56, 81, 96, 4, 70, 49, 97, 45, 34, 88, 80, 55, 40, 31, 66, 87, 39, 91, 1;

#3(s=2): 89, 20, 19, 79, 14, 76, 93, 83, 77, 33, 47, 15, 16, 57, 21, 60, 43, 53, 59, 2;

#4(s=3): 29, 85, 58, 62, 24, 82, 36, 69, 8, 32, 6, 51, 78, 74, 11, 54, 100, 67, 27, 3;

#5(s=9): 73, 71, 90, 61, 84, 17, 98, 86, 99, 26, 63, 65, 46, 75, 52, 18, 38, 50, 37, 9;

#6(s=68): 68.

Равновероятное распределение чисел в ПСП будет в том случае, если каждое слово интервала определения функции будет содержаться в ПСП ровно один раз. Этого можно достичь конкатенацией всех 6 циклов в один сверхцикл:

- загрузить (при M=101, K=41 ,C=7), s(0)=0, сгенерировать 20 слов, получим последовательность чисел строки1 в структуре циклов;

- загрузить s(0)=1, сгенерировать 20 слов, получим последовательность чисел строки 2 в структуре циклов;

- продолжая загружать поочередно s(0)= 2,3,9 и генерируя после каждой загрузки по 20 слов, получим последовательность чисел строк 3,4,5 структуры циклов.

Дополнить выходной поток нуль циклом - число 68. В результате получим равномерно распределенную на интервале $\overline{0,100}$ ПСП. Эта последовательность имеет период повторения T = M. Период повторения можно увеличить, если в конце каждого сверхцикла производить перестановки вектора начальной загрузки и места установки ноль цикла. В этом случае длина гиперцикла (конкатенации сверхциклов с разным порядком последовательности обхода вершит графа состояний) составит

$$T = M \cdot (t\ 1)! = 101 \cdot 5! = 12120.$$

Таким образом, выбор

M = 101, K = 41, C = 7, s(0): 0, 1, 2, 3, 9, 68

обеспечивает достижение поставленной цели.

Выводы

Создан уникальный программный продукт - генератор конгруэнтных чисел (ГСЧ), решающий уравнение (1) и обеспечивающий решение многих практических задач.

Список литературы

1. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с. – (СКБ – специалисту по компьютерной безопасности).

2. Кнут Д. Э. Искусство программирования. Т. 2. Получисленные алгоритмы / Дональд Э. Кнут. – М.: Вильямс, 2007. – 832 с.

3. Митянкина Т. В. Рандомизация последовательности конгруэнтных чисел / Т. В. Митянкина, В. В. Швыдкий, А. И. Щерба // Вестник Инженерной академии Украины. – 2008. – № 2. – С. 107 – 111.

Надійшла до редколегії 19.01.2012

Рецензент: д-р техн. наук, проф. В.Н. Рудницкий, Черкасский государственный технологический университет, Черкассы.

ЛІНІЙНИЙ ГЕНЕРАТОР КОНГРУЕНТНИХ ЧИСЕЛ

В. В. Веретільник

Розглядаються деякі мало досліджені властивості конгруентних послідовностей чисел, що полегшують підбір змінних параметрів конгруентних генераторів. Описується програмний генератор конгруентних чисел, створений для полегшення підбору змінних параметрів під задані вимоги до породжуваної послідовності. Приводиться методика його використання для вирішення практичних завдань.

Ключові слова: *генератор випадкових чисел, генератор конгруентних чисел, рівномірно розподілена послідовність чисел.*

LINEAL CONGRUENTIAL GENERATOR

V. V. Veretelnik

Some little-investigated behaviors of congruential sequences which facilitate the selection of variable congruential generator characteristics are considered in this study. A software-based congruential generator is described here, which was created to facilitate the selection of changeable characteristics to fit them to the specified requirements of the generated sequence. The methodology of its use for practical tasks' solution is also given here.

Keywords*: random numbers generator, congruent numbers generator, evenly distributed sequence of numbers.*