



Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Программное обеспечение ЭВМ и информационные технологии

**Лабораторная работа №1
по курсу “Моделирование”
по теме “Генераторы случайных чисел”**

Студент: Уласик Е.А.

Группа: ИУ7-71

Преподаватель: Рудаков И.В.

2020 г.

Оглавление

1. Формализация.....	3
1.1. Линейный конгруэнтный метод	3
1.2. Табличный метод.....	4
1.3 Критерий равномерности	4
2. Результат работы программы.....	4
3. Вывод.....	7

1. Формализация

Для алгоритмической генерации случайных чисел был выбран линейный конгруэнтный метод.

1.1. Линейный конгруэнтный метод

Получим последовательность случайных чисел $\langle X_n \rangle$, полагая

$$X_{n+1} = (aX_n + c) \bmod m, \quad n \geq 0,$$

где m – модуль; a – множитель; c – приращение; X_0 – начальное значение. Эта последовательность называется *линейной конгруэнтной последовательностью*.

Например, при $m = 10$ и $X_0 = a = c = 7$ будет получена последовательность:

$$7, 6, 9, 0, 7, 6, 9, 0 \dots$$

Данный пример иллюстрирует тот факт, что такая последовательность не может быть “случайной”, то есть обязательно существует цикл, повторяющийся бесконечное число раз. Повторяющиеся циклы называются *периодами*. В данном примере длина периода последовательности равна 4.

Выбор параметров

Линейная конгруэнтная последовательность имеет период длиной m тогда и только тогда, когда выполняются следующие условия:

- числа c и m взаимно простые;
- $a - 1$ кратно p для некоторого простого p , являющегося делителем m ;
- $a - 1$ кратно 4, если m кратно 4.

Тогда пусть $m = 2^{48}$, $c = 11$, $a = 25214903917$, $X_0 = 1$.

1.2. Табличный метод

В табличных генераторах в качестве источника случайных чисел используются специальным образом составленные таблицы, которые должны обеспечивать необходимый уровень случайности.

1.3 Критерий равномерности

Рассмотрим критерий равномерности (критерий частот). Выбирается некоторое число d . Такое, чтобы для каждого r , $0 \leq r \leq d$, подсчитывается число случаев, когда $Y_j = r$, для $0 \leq j \leq n$, а затем применяется χ^2 -критерий, принимая $k = d$, а вероятность $p_s = \frac{1}{d}$ для каждой категории.

Для вычисления значения χ^2 можно воспользоваться формулой:

$$V = \sum_{s=1}^k \frac{(Y_s - np_s)^2}{np_s} \sim \chi_{k-1}^2,$$

где k – количество категорий; n – количество независимых наблюдений; p_s – вероятность принадлежности наблюдения категории; Y_s – число наблюдений s .

Затем с помощью функции распределения χ^2 получим значение оценки “случайности” последовательности.

2. Результат работы программы

Длина последовательности случайных чисел равна 100 для каждого разряда.

Оценка проводилась для всех 100 чисел, но в таблицах приведены только первые 10 чисел полученных последовательностей.

Linear congruential generator

N	0-9	10-99	100-999
1	1	61	133
2	8	90	432
3	3	13	535
4	0	18	622
5	1	95	369
6	8	24	792
7	1	33	883
8	6	96	918
9	1	25	909
10	2	12	156

Eval	15.232	7.034	50.595

Рисунок 1. Результат генерации случайных чисел линейным конгруэнтным методом

Table generator

N	0-9	10-99	100-999
1	4	70	873
2	0	67	610
3	1	53	509
4	3	72	264
5	1	63	810
6	4	55	598
7	3	88	274
8	9	12	417
9	3	74	114
10	7	96	928

Eval	9.587	62.785	81.531

Рисунок 2. Результат генерации случайных чисел табличным методом

Приведённые оценки на рисунках 1 – 2 были получены при значениях $d = 10, 100, 1000$ для каждого столбца соответственно.

3. Вывод

Были рассмотрены алгоритмический (линейный конгруэнтный метод) и табличный генераторы случайных чисел. Оба способа удовлетворяют критерию равномерности, то есть полученные оценки лежат в 5-95%.

Числа, полученные с помощью алгоритмических генераторов случайных чисел, всегда являются псевдослучайными, то есть каждое следующее генерируемое число зависит от предыдущего. Достоинствами подобных генераторов являются их быстроедействие и малое количество занимаемых ресурсов памяти. Недостаток: зависимость каждого последующего числа от предыдущего из-за чего последовательности нельзя в полной мере назвать случайными.

Табличный метод даёт действительно случайные числа, так как таблица содержит проверенные некоррелированные числа, однако таблицы требуют большого количества памяти.