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»

Отчет по лабораторной работе №3 по курсу «Моделирование»

Тема Алгоритмы генерации псевдослучайных чисел

Студент Волков Г.В.

Группа ИУ7-71Б

Преподаватели Рудаков И.В.

Москва — 2023 г.

Задание

Разработать программу, которая генерирует последовательность псевдослучайных одно-, двух-, трехразярдных целых чисел. Обеспечить возможность ввода 10 чисел. Разработать критерий оценки случайности последовательности чисел. Для каждой последовательности вывести число — случайность данной последовательности.

Теоретические сведения

Способы генерации случайных чисел:

- Аппаратный способ;
- Табличный способ;
- Алгоритмический способ.

Алгоритмический способ

Для получения случайных чисел алгоритмическим способом выбран вихрь Мерсенна.

Вихрь Мерсенна — генератор псевдослучайных чисел (ГПСЧ), алгоритм, разработанный в 1997 году японскими учёными Макото Мацумото и Такудзи Нисимура. Вихрь Мерсенна генерирует псевдослучайные последовательности чисел с периодом равным одному из простых чисел Мерсенна, отсюда этот алгоритм и получил своё название и обеспечивает быструю генерацию высококачественных по критерию случайности псевдослучайных чисел.

Числом Мерсенна называется натуральное число $M_n = 2^n - 1$.

Существуют несколько вариантов алгоритма Мерсенна, различающихся только величиной используемого простого числа Мерсенна. В данной работе будет использован алгоритм MT19937.

Этапы алгоритма вихрь Мерсенна:

Шаг 0. Предварительно инициализируется значение констант u1, h1, a:

u1 ← 10...0 битовая маска старших w-r бит,

h1 ← 01...1 битовая маска младших r бит,

a ← aw-1aw-2...a0 последняя строка матрицы A.

Шаг 1. x[0], x[1],...,x[n-1] ← начальное заполнение

Шаг 2. Вычисление (xiu | xi+1l)

y ← (x[i] AND u1) OR (x[(i + 1) mod n] AND h1)

Шаг 3. Вычисляется значение следующего элемента последовательности по рекуррентному выражению

x[i] ← x[(i + m) mod n] XOR (y»1) XOR a если младший бит y = 1

или

x[i] ← x[(i + m) mod n] XOR (y»1) XOR 0 если младший бит y = 0

Шаг 4. Вычисление x[i]T

y ← x[i] y ← y XOR (y»u) y ← y XOR ((y«s) AND b) y ← y XOR ((y«t) AND c) z ← y XOR (y»l) вывод z

Шаг 5. i ← (i + 1) mod n

Шаг 6. Перейти к шагу 2.

Алгоритм работы вихря Мерсенна состоит из двух частей: рекурсивной генерации и закалки. Рекурсивная часть представляет собой регистр сдвига с линейной обратной связью, в котором все биты слова определяются рекурсивно.

Регистр сдвига состоит из 624 элементов (19937 клеток). Первый элемент состоит из 1 бита, а остальные – из 32. Процесс генерации начинается с логического умножения на битовую маску, которая отбрасывает 31 бит (кроме наиболее значащих). Следующим шагом выполняется инициализация (x0, x1,..., x623) любыми беззнаковыми 32-разрядными целыми числами. Следующие шаги включают в себя объединение и переходные состояния.

Табличный способ

В качестве таблицы для генерации случайных чисел табличным способом используются цифры из части таблицы «A Million Random Digits with 100,000 Normal Deviates» (1955 год).

Данная таблица сохранена в виде текстового файла, где все цифры

перечислены без пробелов. Для генерации чисел выбирается начальная позиция в файле, читаются следущие n цифр, где n — количество разрядов в генерируемом числе. Для генерации следующего числа происходит переход к следующей строке таблицы с сохранением номера столбца. При невозможности перейти к следующей строке в связи с окончанием файла позиция переводится на первую строку, а номер столбца увеличивается на единицу. В случае, если в строке не хватает для формирования числа, то они берутся из начала следующей строки файла.

Критерий оценки случайности последовательности

В качестве критерия случайности было использовано отношение средних арифметических четных и нечетных элементов друг к другу. Чем ближе коэффициент к 1, тем последовательность более случайна.