‘Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт прикладной математики и механики

**Кафедра «Информационная безопасность компьютерных систем»**

**ЛАБОРАТОРНАЯ РАБОТА № 1**

«**Изучения свойств линейного конгруэнтного генератора**»

по дисциплине «Структуры данных»

1. Выполнил студент гр.
2. 4831001/20003: Черникова В.М.

<*подпись*>

1. Преподаватель: Семьянов П.В.

<*подпись*>

1. Санкт-Петербург
2. 2023

Оглавление

[1. Цель работы 3](#_Toc145363624)

[2. Задачи 3](#_Toc145363625)

[3.Основная часть 3](#_Toc145363626)

[3.1 Хи-квадрат критерий 3](#_Toc145363627)

[4.2 Критерий перестановок 5](#_Toc145363628)

[5. Результаты 6](#_Toc145363629)

[5.1 Период. 6](#_Toc145363630)

[5.2 Разброс. 6](#_Toc145363631)

[5.3 Мощность. 6](#_Toc145363632)

[6. Заключение 6](#_Toc145363633)

# Цель работы

Изучение свойств линейного конгруэнтного генератора.

# 2. Задачи

1. Выбрать правильные параметры ЛКГ с учётом длинны машинного слова m = 32 бита.
2. На практике проверить мощность, разброс и период.
3. Реализовать метод проверки «Хи – квадрат»
4. Проверить генератор одним из тестов на случайность, представленных в книге Д.Э. Кнута “Искусство программирования”.

# 3.Основная часть

Суть линейного конгруэнтного метода заключается в вычислении последовательности случайных чисел, вычисляя каждый последующий член из предыдущего по формуле: Где m – модуль, a – множитель, c – приращение, – предыдущее значение.

Так как метод генерации основан на математической функции, со временем начинают образовываться повторы чисел. Такие циклы называются периодами. Обычно главной задачей при написании ЛКГ становиться выбор подходящих параметров a, c, m.

При выборе модуля m рассматривался следующий критерий: , где k – длина машинного слова, 0,01m<a<0,99m. Были выбраны параметры а=1103515245 и с=12345, удовлетворяющие данным критерия.

## 3.1 Хи-квадрат критерий

Для анализа выбранных констант и написанного ЛКГ были реализован критерий хи-квадрат.

Критерий «хи-квадрат» (х2-критерий) — это один из самых известных статистических критериев; он является основным методом, используемым в сочетании с другими критериями. Его работа рассматривается как фундамент современной математической статистики.

Для нашего случая проверка по критерию «хи-квадрат» позволит узнать, насколько созданный нами ЛКГ близок к эталону ЛКГ, то есть удовлетворяет ли он требованию равномерного распределения или нет. Для реализации хи-квадрат была реализована функция period(), определяющая период генератора. Это период делится на примерно равные интервалы, их получится k, в нашем случае – 16 интервалов. Далее наша программа запускает генерацию N количества случайных чисел и проверяет каждое на попадание в один из k отрезков. Для вычисления хи-квадрата находится разница между фактической, наблюдаемой вероятностью распределения чисел и ожидаемой вероятностью. Ожидаемая вероятность попадания считается по формуле:

Значение распределения величины в интервал хи-квадрат рассчитывается по формуле:

Далее это значение сравнивается с существующими значениями в таблице распределения Хи-квадрат, которые показаны на рисунке 1.

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 1

Всего проводится 100 тестов, после чего выводится процент удовлетворительных из них.

Тест можно считать удовлетворительным при попадании V в промежуток от 7.962 до 26.296. Программа выдала 90±2% тестов удовлетворительны, значит параметры генератора были подобраны правильно.

# 3.2 Критерий перестановок

Суть проверки заключается в том, что исходная последовательность разделяется на выходе на n групп по t элементов в каждой. Элементы в каждой группе можно упорядочивать t! различными способами. Подсчитывается число групп с любым возможным порядком и применяется критерий хи-квадрат с k=t! Возможными категориями и вероятностью 1/t! для каждой категории.

Было выбрано t=3, и поэтому существует 6 возможных категорий, на которые и разделяется последовательность для расчета.

Бралось 10000000 чисел. Из результатов теста можно сделать вывод, что параметры подобраны верно, так как распределение по промежуткам близко к теоретическому.

# 4. Результаты

### 4.1 Период.

В данной программе генерируются числа до того момента пока не попадется элемент равный первому. В результате проверки теоретический период совпал с полученным на практике, он равен 4294967296 =

# 4.2 Разброс.

Разброс - вероятность появления всех чисел из некоторого диапазона. Если все числа из сгенерированной псевдослучайной числовой последовательности встречаются с одинаковой вероятностью, то генератор имеет хороший разброс. Параметры были выбраны правильно, и период получился максимальной длины, т.е. равный модулю, следовательно полученные числа встречаются ровно по одному разу, встречаются с одинаковой вероятностью.

# 4.3 Мощность.

Мощность - такое наименьшее целое число s, что (a - 1)s ≡ 0 (mod m). Показывает, есть ли линейная зависимость между соседними членами последовательности. Если она маленькая, значит что есть связь, поэтому S>=5. Полученная мощность = 16, линейная зависимость между соседними членами последовательности отсутствует.

# 5. Заключение

В результате данной лабораторной работы были приобретены навыки создания ЛКГ и правильного подбора параметров для него. На практике проверены характеристики получившегося ЛКГ. Были изучены некоторые из критериев, позволяющие определить правильность работы алгоритма.

Данный генератор прошел проверку на различные критерии, полученные характеристики показывают, что генератор является хорошим и его можно использовать для генерации псевдослучайных чисел.