**Оглавление**

# Генераторы случайных чисел с равномерным законом распределения

Генерация случайных чисел слишком важна, чтобы оставлять ее на волю случая.

Роберт Кавью

1. **Цель работы:** разработка генераторов псевдослучайных чисел с равномерным законом распределения.
2. **Компьютерные средства:**

   Операционная среда: Windows 10/XP,
   программное средство: Visual Studio 2017.

3. **Требования к уровню подготовленности студента при выполнении лабораторной работы:**

Лабораторные работы проводятся после изучения студентами следующих дисциплин: *Информатика и основы программирования*, *Технологии программирования*.

Для успешного выполнения курса лабораторных работ обучающиеся должны:

- знать методы разработки программ для решения стандартных задач;

- знать основы информатики;

- знать алгоритмический язык программирования;

- знать информационные технологии, используемые при подготовке документов;

- уметь разрабатывать алгоритмы решения задач с использованием компьютера;

- владеть методами проверки правильности работы программы.

## 4. Краткая теория

Качественное решение задач теории информационных процессов требует использования хорошего генератора случайных чисел.

**Эталонный генератор случайных чисел** (ГСЧ) – это генератор, порождающий последовательность случайных чисел $\{r_i\}$, удовлетворяющую условиям:

- числа $r_i$ должны быть в диапазоне от 0 до 1;
- числа $r_i$ должны иметь равномерное распределение на отрезке $[0, 1]$ (математическое ожидание в этом случае $m_r = 0{,}5$, а среднеквадратичное отклонение $\sigma_r = \sqrt{\frac{1}{12}} \approx 0{,}2887$);
- числа $r_i$ должны быть статистически независимы.

Стандартный ГСЧ выдает одно случайное число при однократном обращении к нему. Повторяя запросы, можно получить последовательность случайных чисел.

ГСЧ по способу получения случайных чисел могут быть табличными, физическими и программными.

В данной работе будем рассматривать программные **генераторы псевдослучайных чисел** (ГПСЧ).

Программный генератор – это алгоритм, порождающий последовательность чисел, которая по своим характеристикам похожа на случайную. Для формирования очередного числа последовательности используются различные алгебраические преобразования.

Последовательность на выходе такого генератора подчиняется некоторому закону, где каждое сгенерированное число зависит от предыдущего. Такие числа называются псевдослучайными, а их генератор – ГПСЧ.

Начиная с некоторого значения, генерируемая последовательность повторяется, т.е. существует цикл, который может повторяться бесконечно. Такой цикл называется **периодом**. Чем больше период, тем качественней ГПСЧ.

Большинство используемых методов генерации псевдослучайных целых чисел состоит в выборе некоторой функции *f*, отображающей множество целых чисел в себя. При этом выбирается какое-нибудь начальное число $r_0$, а каждое последующее число порождается с помощью рекуррентного соотношения:

$r_{i+1} = f(r_i)$

Число $r_i$ называется зерном ГСЧ и полностью определяет текущее состояние ГСЧ и следующее генерируемое значение.

Вначале функции *f(r)* выбирались как можно более сложные и трудно понимаемые. Например, *f(r)* определялась как целое число, двоичное представление которого составляет средний 31 разряд 62-разрядного квадрата числа *r* (модификация метода средин квадратов).

Отсутствие теории по отношению к функции *f(r)* приводило к катастрофическим последствиям. Используя же теорию чисел, можно выбрать такую функцию *f(r)*, для которой заранее будет известен ее максимально возможный период.

Кроме того, использование теории чисел помогает предсказать характер последовательности псевдослучайных чисел.

На рис.1. приведены примеры генерации псевдослучайных чисел в диапазоне [0; 1] рекуррентным методом.

Требования к функции *y=f(r):*

1. Она должна быть определена на всем отрезке [0; 1] и иметь на нем непрерывную область значений [0; 1], в противном случае генерируемые числа будут составлять несобственное подмножество указанного отрезка.
2. Она должна иметь плотный и равномерный график, заполняющий область $r \in [0; 1]$, $y \in [0; 1]$.

Функция, приведенная на рис.1, а, удовлетворяет перечисленным выше требованиям, а функция на рис.1, б не удовлетворяет п.2, в результате чего соседние числа генерируемой последовательности будут иметь сильную корреляционную зависимость.

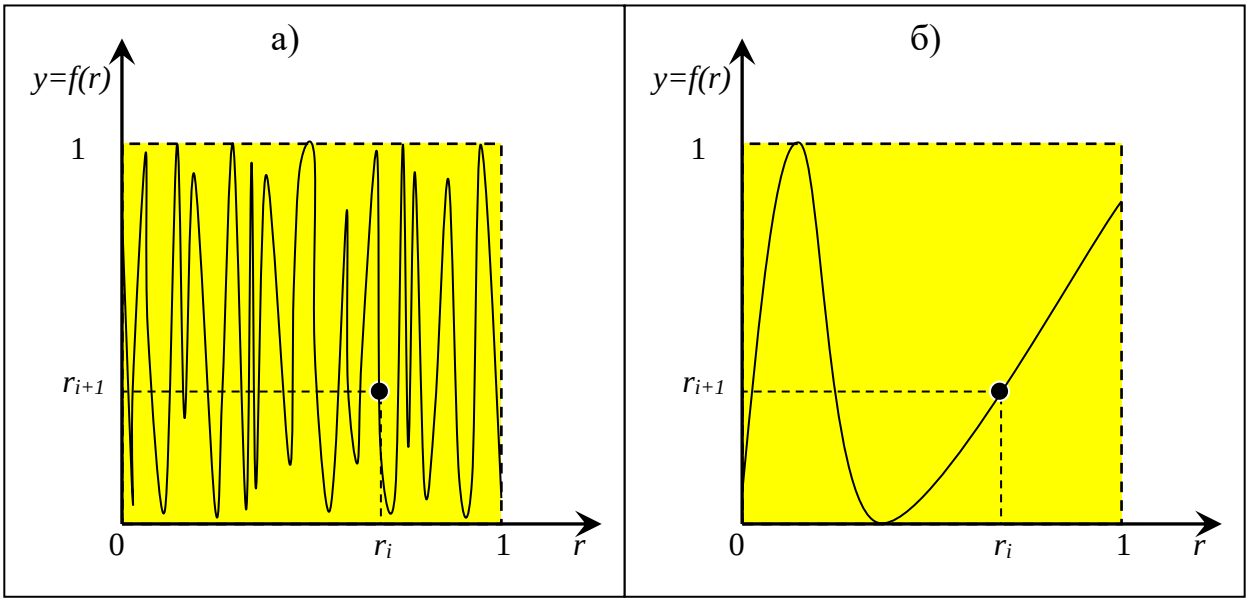


Рис.1. Примеры рекуррентной функции $y = f(r)$:
а) удачная функция, б) неудачная функция.

Рассмотрим следующие программные методы получения случайных чисел:

- метод срединных квадратов;
- метод срединных произведений;
- метод перемешивания;
- линейный конгруэнтный метод.

**Метод срединных квадратов**

Данный метод является одним из первых программных ГПСЧ, он был предложен в 1946 г. Дж. фон Нейманом.

На рис.2 приводится схема метода срединных квадратов.

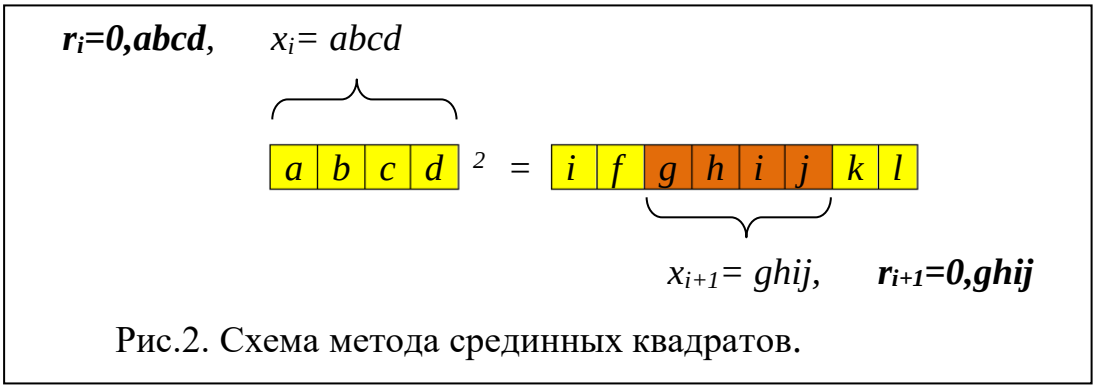


Рис.2. Схема метода срединных квадратов.

1. Выбрать некоторое (случайное) число $r_i$ ($i=0$), имеющее четную дробную разрядность, десятичные числа этого числа записать в $x_i$ ($i=0$);
2. Применить рекуррентную формулу: возвести $x_i$ в квадрат и взять середину полученного случайного числа:

   $x_{i+1} = Середина(x_i^2)$,

   используя $x_{i+1}$, составить случайные числа в диапазоне [0,1]:

   $r_{i+1} = 0, x_{i+1}$.

Таким образом, получаем последовательность $\{r_i\}$ равномерно распределенных случайных чисел из диапазона от 0 до 1.

Данный генератор имеет максимальный период:

$T = M^n$,

где $M$ – основание системы счисления, $n$ – разрядность числа $r_0$.

Например, если разрядность случайного числа равна 4, то для десятичной системы счисления период равен $T_{10}=10^4$, а для двоичной системы счисления $T_2=2^4=16$, т.е. уже через 16 шагов последовательность случайных чисел начнет повторяться. Если начальное число выбрано неудачно, то период может быть значительно меньше.

Недостаток метода: вырождается в случае, если очередное число последовательности станет равно нулю.

### Метод срединных произведений

1. Выбрать два случайных числа $r_i$ и $r_{i+1}$ ($i=0$), имеющих четную дробную разрядность $\Rightarrow$ записать десятичные значения в $x_i$ и $x_{i+1}$;
2. Применить рекуррентную формулу: найти произведение случайных чисел $x_i$ и $x_{i+1}$ и записать результат в новую переменную:

$x_{i+2} := x_i \cdot x_{i+1} \Rightarrow$

$r_i = r_{i+1}, \quad r_{i+1} = 0, x_{i+2}.$

На рис.3 приводится схема метода срединных квадратов.

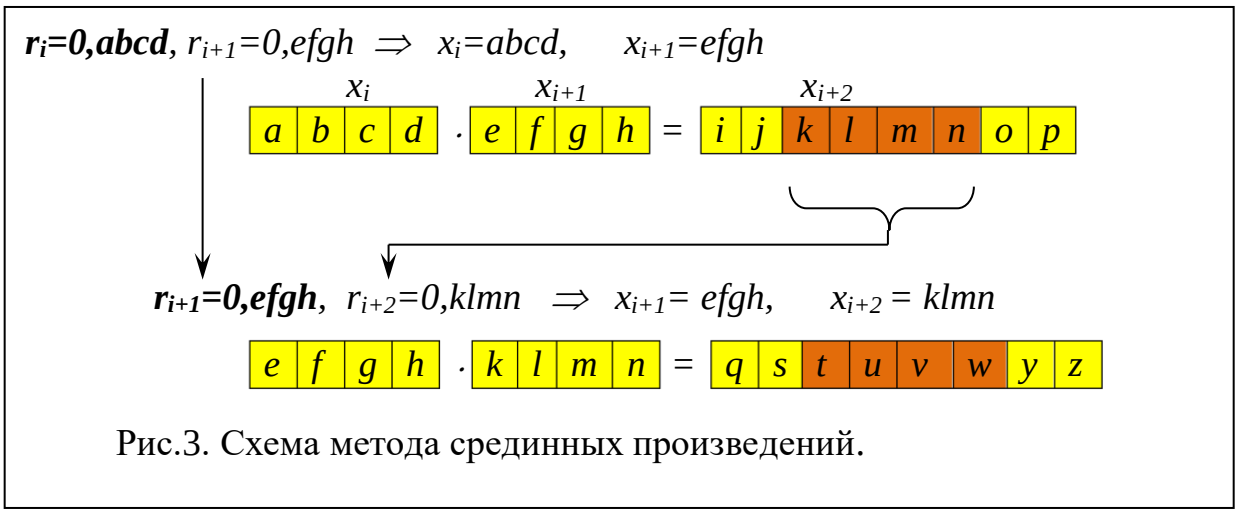


Рис.3. Схема метода срединных произведений.

**Метод перемешивания**

1. Выбрать некоторое случайное число $r_i$ ($i=0$), имеющее четную дробную разрядность, десятичные числа этого числа записываются в $x_i$ ($i=0$);
2. Циклически сдвинуть содержимое ячейки $x_i$ влево на ¼ длины ячейки, результат записать в $x1_i$;
3. Циклически сдвинуть содержимое ячейки $x_i$ вправо на ¼ длины ячейки, результат записать в $x2_i$.
4. Сложить полученные случайные числа: $x_{i+1}= x1_i + x2_i$.

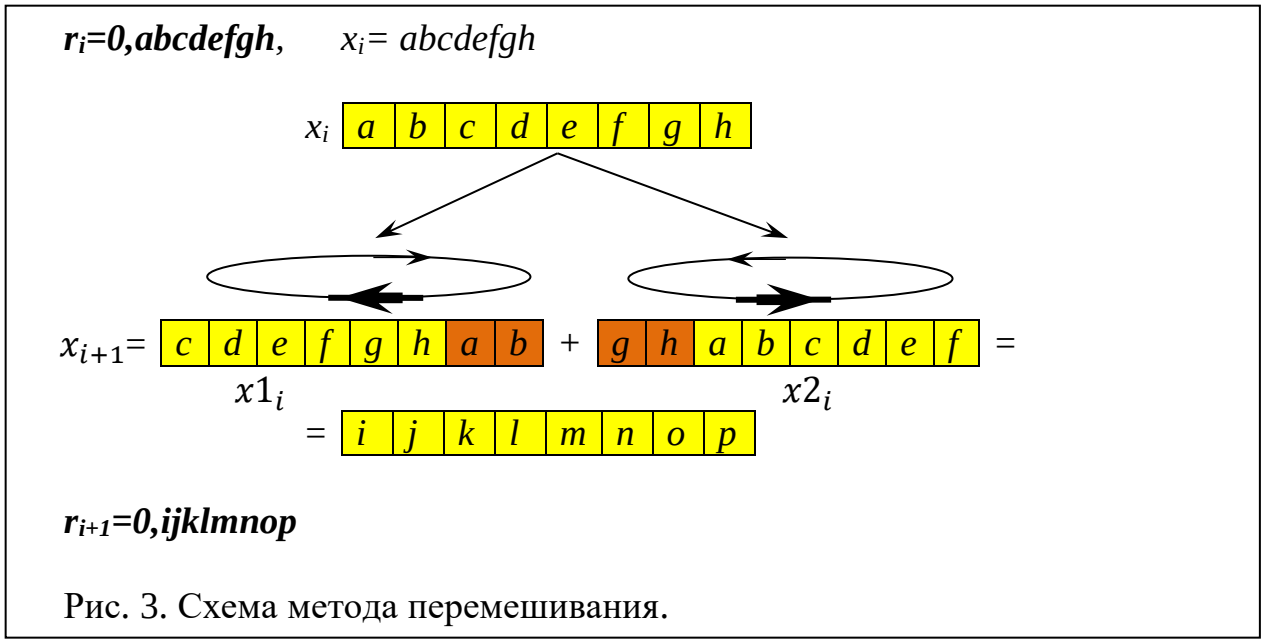


Рис. 3. Схема метода перемешивания.

*Примечание*:

Если результат сложения $x1_i + x2_i$ не вмещается в ячейку $x_{i+1}$, то крайний левый бит отбрасывается.

В Паскале, например, при переполнении ячейки тоже производится автоматическое урезание лишних битов в соответствии с типом переменной.

### Линейный конгруэнтный метод

В данном методе используется операция *mod(x,y)*, которая возвращает остаток от деления первого аргумента *x* на второй *y*.

1. Выбрать начальные значения $a$, $b$, $M$ и $r_i$;
2. Каждое последующее число рассчитывается по рекуррентной формуле:

$r_{i+1} = mod\ (ar_i+b, M)$.

Конгруэнтный ГСЧ выдает псевдослучайные целые числа в интервале (0, $M$). Параметры $r_0$, $a$ и $b$ – целые числа из этой области. Для качественного генератора требуется тщательно подобрать коэффициенты.

1. Параметр $M$ должен быть достаточно большим, так как период генерируемой последовательности не может быть больше $M$.

2. В качестве $r_0$ можно брать текущее время, преобразованное в число из интервала (0, $M$), что позволяет получить различные последовательности при различных запусках программы. Для проверки программы $r_0$ может быть выбрано произвольно, например, $r_0$=1.

3. Для двоичных машин в качестве числа $a$ следует выбирать число, удовлетворяющее следующим требованиям:

- $mod\ (a, 8) = 5$;
- $\frac{M}{100} < a < M - \sqrt{M}$ ;
- двоичные знаки $a$ не должны иметь очевидного шаблона.

4. В качестве числа $b$ следует выбирать нечетное число, такое, что

$$\frac{b}{M} \approx \frac{1}{2} - \frac{1}{6}\sqrt{3} \approx 0{,}21132\,.$$

Если $b=0$, то метод называется *мультипликативным конгруэнтным*.

Более подробные рекомендации по выбору параметров можно найти у Д. Кнута [1].

При использовании конгруэнтного метода следует помнить, что наименее значимые двоичные цифры $r_k$ будут «не очень случайными». Поэтому выбирают наиболее значимые разряды $r_k$, а не наименее значимые. Кроме

того, для повышения надежности созданного ГСЧ рекомендуется предварительно испытать полученные случайные числа на какой-либо задаче с известным ответом.

## 5. Задание

1. Изучите представленные выше методы построения ГПСЧ.
2. Напишите программу, реализующую работу описанных выше алгоритмов. Для выделения средней части следует использовать операции сдвига и преобразования типа (либо побитового «И»).
3. В результате работы программы на экран должен выводиться график, на котором изображена последовательности точек, где каждая точка, имеющая две координаты ($x$, $y$) – реализация двойного запуска ГПСЧ.
4. В программе должна быть реализована функция выбора длины псевдослучайной последовательности.
5. В программе должно быть реализовано графическое сравнение полученных результатов со встроенной функцией *random(x)* Результат должен быть схожим с написанными ГПСЧ при одинаковом размере выборки.

## 6. Отчетность по работе

По результатам выполнения лабораторной работы студент представляет отчет. Отчет должен содержать следующую информацию:

1. Цель работы.
2. Формулы генерации псевдослучайных чисел.
3. Код написанной студентом программы с комментариями.
4. Результат выполнения программы: скриншот графиков, позволяющих сравнить работу написанных функций *r(x)* со встроенной *random(x)*.
5. Изображения, содержащие не менее 25 чисел сгенерированных псевдослучайных последовательностей (в текстовом виде).

Материалы отчета располагаются в следующем порядке:

1. Титульный лист (образец в Приложении).
2. Цель работы, постановка задачи, краткая (!) теория.
3. Распечатка кода программы.
4. Результат работы программы: графики, таблицы.
5. Интерпретация результатов.
6. Выводы.

Подготовка отчета производится вне рамок времени, отведенного на выполнение лабораторной работы. Отчет сдается преподавателю, ведущему лекционный курс.

***Студент, не сдавший отчет по лабораторной работе, считается не выполнившим учебный план и к экзамену не допускается.***

## 7. Контрольные вопросы

1. Эталонный генератор случайных чисел, его свойства.
2. Требования, предъявляемые к ГСПЧ?
3. Требования к рекуррентным функциям ГПСЧ.
4. Метод срединных квадратов.
5. Метод срединных произведений.
6. Метод перемешивания.
7. Линейный конгруэнтный метод.

**Литература**


1. Кнут Д. Искусство программирования, том 2. Получисленные методы / Д. Кнут. М.: Изд. дом «Вильямс», 2007. 832 с.
2. Керниган Б. Язык программирования Си: Задачи по языку Си. / Б. Керниган, Д. Ритчи, А. Фьюэр М.: Финансы и статистика, 1985. – 192 с.
3. Керниган Б., Ритчи Д. Язык программирования Си. М.: Финансы и статистика, 1992. – 272 с.
4. Подбельский В.В., Фомин С.С. Программирование на языке Си. Учеб. пособие. М.: Финансы и статистика, 2004. 600 с.
5. Форсайт Дж. Машинные методы математических вычислений / Дж. Форсайт, М. Малькольм, К. Моулер. М.: Мир, 1980. – 279 с.
6. Каханер Д. Численные методы и математическое обеспечение: Пер. с англ. / Д. Каханер, К. Моулер, С. Нэш. М.: Мир, 1998. – 575 с., ил.
7. Зубинский А. В поисках случайности //А. Зубинский. Компьютерное обозрение №29, 2003.
8. Шарыгин, А.Г. Прикладные методы статистического модели рования / А.Г. Шарыгин, Ю.И. Палагин. – Л. : Машиностроение, 1986. – 320 с.
9. Галенко, Д.И. Моделирование псевдослучайных чисел на ЭВМ / Д.И. Галенко. – М. : Наука, 1982. – 224 с.
10. Ермаков, С.М. Курс статистического моделирования / С.М. Ермаков, Г.А. Михайлов. – М. : Физматлит, 1982. – 296 с.
11. Васильев, К.К. Математическое моделирование систем связи / К.К. Васильев, М.Н. Служивый. – Ульяновск : Изд-во УлГУ, 2008. – 170с.
12. Тюрин, Ю.Н. Статистический анализ данных на компьютере / Ю.Н. Тюрин, А.А. Макаров. – М. : ИНФРА-М, 1988. – 528 с.

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования

**«Дальневосточный федеральный университет»**

(ДВФУ)

**ШКОЛА ЕСТЕСТВЕННЫХ НАУК**

Теория информационных процессов и компьютерных систем

# ЛАБОРАТОРНАЯ РАБОТА №1

## Генераторы случайных чисел с равномерным законом распределения

Выполнил: студент гр. Б8318
Фамилия И.О.
Проверил: доцент каф. КС
Фамилия И.О.

2019