ЛАБОРАТОРНАЯ РАБОТА №1-2

Формирование последовательности случайных чисел с заданным законом распределения

Цель. Изучить основные способы создания последовательностей случайных чисел с заданными законами распределения вероятности.

Краткое теоретическое введение.

1. Алгоритм Лемера генерации равномерно распределенных случайных чисел.

Выраженный в символьном виде **алгоритм Лемера** представляет собой следующее выражение:

```
X(i) = a * X(i-1) mod m
```

«Новое случайное число является предыдущим случайным числом, умножаемым на константу a, после чего над результатом выполняется операция деления по модулю константы m». Например, предположим, что в некий момент текущее случайное число равно 104, a = 3 и m = 100. Тогда новое случайное число будет равно 3 * 104 mod 100 = 312 mod 100 = 12.

2. Метод серединных произведений.

Число *R*0 умножается на *R*1, из полученного результата *R*2 извлекается середина *R*2* (это очередное случайное число) и умножается на *R*1. По этой схеме вычисляются все последующие случайные числа (см. рис. 1).

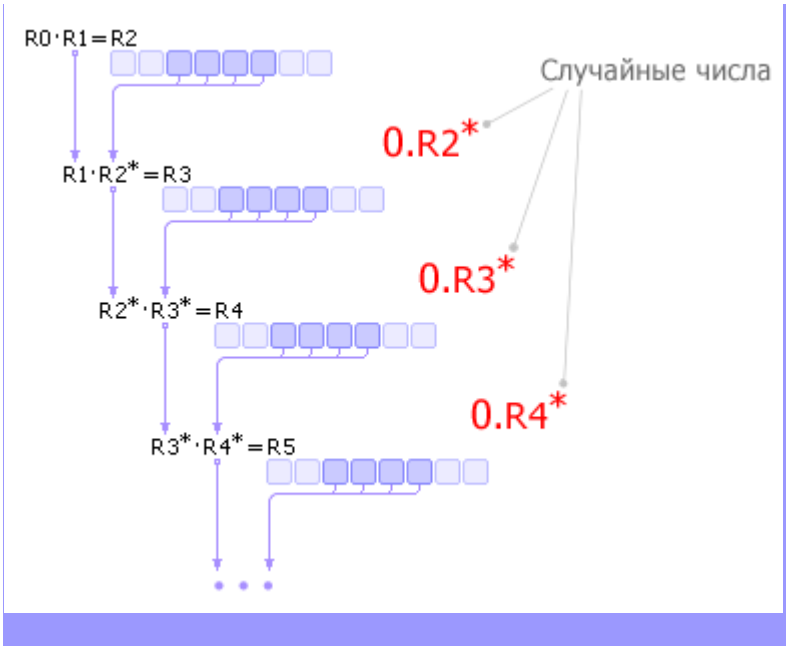

Рис. 1– Схема метода сер

3. Регистр с линейной обратной связью

В регистре сдвига с линейной обратной связью (РСЛОС) выделяют две части (модуля):

- собственно, регистр сдвига;
- схему (или подпрограмму) обратной связи, вычисляющую значение вдвигаемого бита.

Регистр состоит из функциональных ячеек памяти (битов одного или нескольких машинных слов), в каждой из которых хранится текущее состояние (значение) одного бита. Количество ячеек , называют длиной регистра. Биты (ячейки) обычно нумеруются числами , содержимое -й ячейки обозначается через . Значение нового бита определяется до сдвига битов в регистре и только после сдвига записывается в ячейку , а из ячейки извлекается очередной сгенерированный бит.

Функцией обратной связи для РСЛОС является линейная булева функция от значений всех или некоторых битов регистра. Функция выполняет умножение битов регистра на коэффициенты , где . Количество коэффициентов совпадает с количеством битов регистра . Коэффициенты принимают значения , причём последний коэффициент равен , так как РСЛОС задаётся характеристическим многочленом степени . Сложение по модулю 2 (операция «XOR», обозначаемая в формулах символом «») или её логическая инверсия «XNOR» являются линейными булевыми функциями и наиболее часто применяются в таких регистрах[2]. При этом биты, являющиеся переменными функции обратной связи, называются **отводами**, а сам регистр называется **конфигурацией Фибоначчи**[3].

Управление регистром в аппаратных реализациях производится подачей сдвигающего импульса (иначе называемого **тактовым** или **синхроимпульсом**) на все ячейки. Управление регистром в программных реализациях производится выполнением цикла. На каждой итерации цикла вычисляется функция обратной связи и выполняется битовый сдвиг в слове.