

ЛАБОРАТОРНАЯ РАБОТА №3

ВАРИАНТ 8

КРАЖЕВСКИЙ АЛЕКСЕЙ ИГОРЕВИЧ, 15 ГРУППА

Условие варианта:

8	$\begin{matrix} 10100 \\ x^5 + x^4 + x^2 + x + 1 \end{matrix}$	$\begin{matrix} 1011000 \\ x^7 + x^6 + x^5 + x^4 + 1 \end{matrix}$	$\begin{matrix} 01000110 \\ x^8 + x^6 + x^5 + x^2 + 1 \end{matrix}$
---	--	--	---

Шаг 1. Реализовать работу РСЛОС. На входе заданы число n – количество ячеек памяти, из которых состоит регистр, начальное состояние и характеристический многочлен.

На первом шаге необходимо реализовать 3 РСЛОС, заданные в вашем варианте. Для каждого регистра найти период выходной последовательности и сгенерировать последовательность до начала зацикливания.

Шаг 2. Сгенерировать выходную последовательность генератора Геффе длительностью $N = 10\,000$ элементов.

Шаг 3. Для сгенерированной на шаге 2 последовательности вычислить следующие статистики:

1) количество 0 и количество 1;

$$2) r_i = \sum_{j=1}^{10000-i} \tau(\gamma_j \oplus \gamma_{j+i}), \tau(x) = (-1)^x \text{ для } i \text{ от } 1 \text{ до } 5.$$

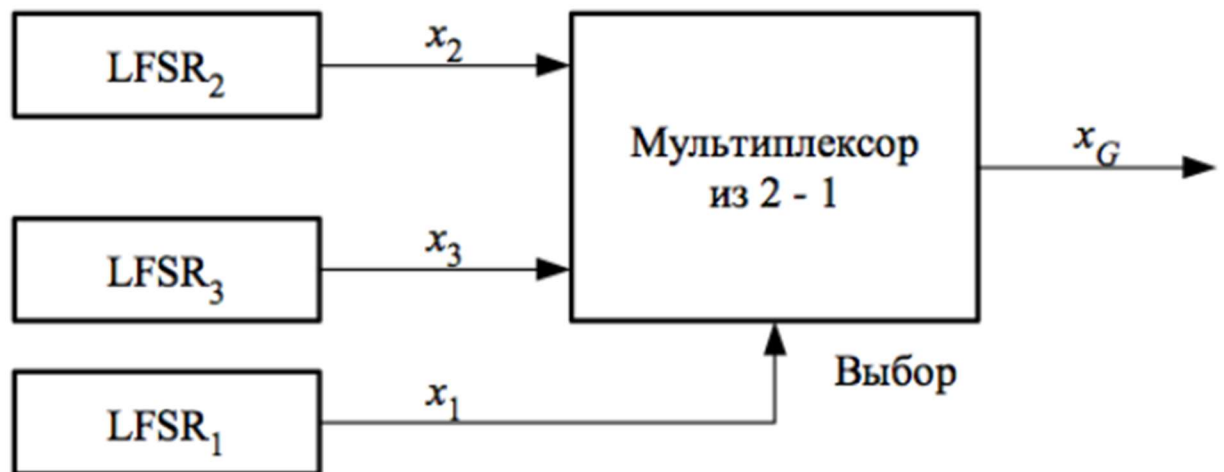
РСЛОС (LFSR) - регистр битовых слов, у которого значение входного бита равно линейной булевой функции от значений остальных битов регистра до сдвига.

Принцип работы LFSR:

В течение каждого такта сдвигового регистра с линейной обратной связью выполняет следующие операции:

- читается бит, расположенный в ячейке $L - 1$; этот бит является очередным битом выходной последовательности;
- функции обратной связи вычисляет новое значение для ячейки 0, используя текущие значения ячеек;
- содержимое каждой i -й ячейки перемещается в следующую ячейку $i + 1$, где $i = 0, 1, \dots, L - 2$;
- в ячейку 0 записывается бит, ранее вычисленный функцией обратной связи.

Генератор Геффе:



В этом генераторе используются три РСЛОС, объединённые нелинейным образом. Длины этих регистров попарно простые числа.

Нелинейную функцию для данного генератора можно записать следующим образом:

$$f(x_1, x_2, x_3) = x_1 x_2 \oplus (1 + x_2) x_3 = x_1 x_2 \oplus x_2 x_3 \oplus x_3.$$

Выполнение написанного кода:

Количество нулей и единиц:

```
4981 zeros
5019 ones
```

Периоды каждой последовательности:

```
[31, 127, 255] periods
```

Вывод r_i :

```
r_1: -161
r_2: -99
r_3: 57
r_4: -21
r_5: -121
```

Вывод:

По выводу r_i для генератора Геффе (i от 1 до 5) нельзя сказать о приблизительно одинаковом количестве нулей и единиц, но при увеличении

промежутка проверки мы сможем убедиться в том, что их на самом деле примерно одинаковое кол-во.

```
r_38: 9 r_39: 28 r_40: -19 r_41: -3 r_42: -10 r_43: -8 r_44: 5 r_45: 24 r_46: -9 r_47: -8 r_48: 40 r_49: 4
```

Вероятности получения единиц и нулей при использовании генератора случайных чисел практически одинаковы и примерно равны $\frac{1}{2}$.

Также периоды, полученные в результате выполнения программы соответствуют действительности:

5	$x^5 + x^3 + 1$	31
6	$x^6 + x^5 + 1$	63
7	$x^7 + x^6 + 1$	127
8	$x^8 + x^6 + x^5 + x^4 + 1$	255

Таким образом, мы удостоверились в правильности работы программы.