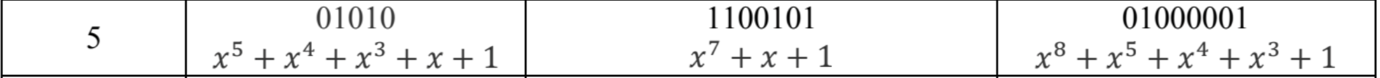
**Гончаренко Андрей Дмитриевич, 5 вариант**

**Описание работы РСЛОС**

Пусть изначально мы имеем некоторые значения на выходе регистра. Булева функция, исходя из этих значений, подает на вход регистра некоторое число. Затем, как только мы подаем тактовый сигнал, все значения сдвигаются на 1 вправо, в нулевой триггер попадает тот самый результат булевой функции.

**Описание работы генератора Геффе**

В генераторе Геффе используется три регистра с линейной обратной связью, объединённые нелинейным образом. Два регистра LFSR являются входами мультиплексора, а третий – управляет его выходом. Через  обозначены выходы трёх LFSR, выход генератора Геффе  описывается так:

На самом деле генератора Геффе плох, т.к. информаци о РСЛОС 1 и 3 содержится в его выходной последовательности и как следствие он поддается корреляционным атакам.

**Период каждой сгенерированной выходной последовательности**

Сгенерированная последовательность РСЛОС находится в файле **output2.txt**.

Сгенерированная последовательность при помощи генератора Геффе находится в файле **result.txt**.

**Количество нулей и единиц**

Количество нулей: 5053

Количество единиц: 4947

Результат также можно посмотреть в файле **resultOneZero.txt**.

**Значение**

При .

При .

При .

При .

При .

Результат также можно посмотреть в файле **resultPart3.txt**.

**Бонусные задания:**

1. Бинарный файл: **result.bin**, но я так понял, что там нужна Windows, но у меня MacOS, а виртуалки нету, но я интересовался, может все же какой-то дополнительный балл будет?)