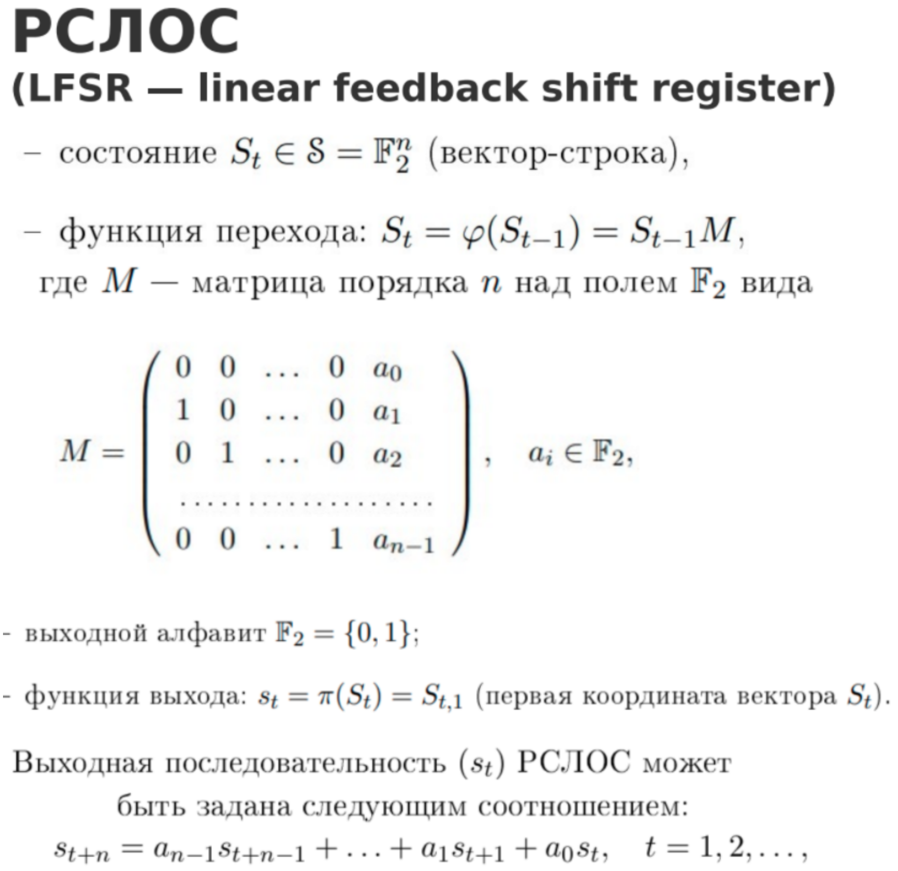
Ермолаева Екатерина Александровна, 14 группа, лабораторная №3, 2 вариант

РСЛОС №1 **(5)**	**РСЛОС №2** **(7)**	**РСЛОС №3** **(8)**
01001 $x^5 + x^3 + x^2 + x + 1$	0011100 $x^7 + x^5 + x^2 + x + 1$	10001011 $x^8 + x^4 + x^3 + x^2 + 1$

1)РСЛОС

Описание работы:



РСЛОС

(LFSR — linear feedback shift register)

– состояние $S_t \in \mathcal{S} = \mathbb{F}_2^n$ (вектор-строка),

– функция перехода: $S_t = \varphi(S_{t-1}) = S_{t-1}M$,
где M — матрица порядка n над полем $\mathbb{F}_2$ вида

$$M = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix}, \quad a_i \in \mathbb{F}_2,$$

- выходной алфавит $\mathbb{F}_2 = \{0, 1\}$;

- функция выхода: $s_t = \pi(S_t) = S_{t,1}$ (первая координата вектора S_t).

Выходная последовательность (s_t) РСЛОС может быть задана следующим соотношением:

$$s_{t+n} = a_{n-1}s_{t+n-1} + \ldots + a_1 s_{t+1} + a_0 s_t, \quad t = 1, 2, \ldots,$$

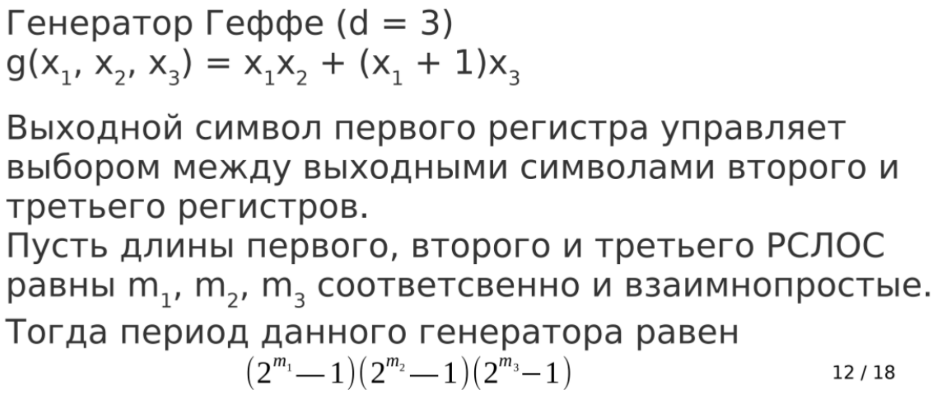
Период первой последовательности - 31

Период второй последовательности - 127

Период третьей последовательности - 255

2)Генератор Геффе

Определение:



Генератор Геффе (d = 3)

$g(x_1, x_2, x_3) = x_1x_2 + (x_1 + 1)x_3$

Выходной символ первого регистра управляет выбором между выходными символами второго и третьего регистров.

Пусть длины первого, второго и третьего РСЛОС равны m_1, m_2, m_3 соответсвенно и взаимнопростые.

Тогда период данного генератора равен

$$(2^{m_1}—1)(2^{m_2}—1)(2^{m_3}—1)$$

12 / 18

Количество нулей - 4975

Количество единиц - 5025

$r_1 =- 57$

$r_2 = 34$

$r_3 = 125$

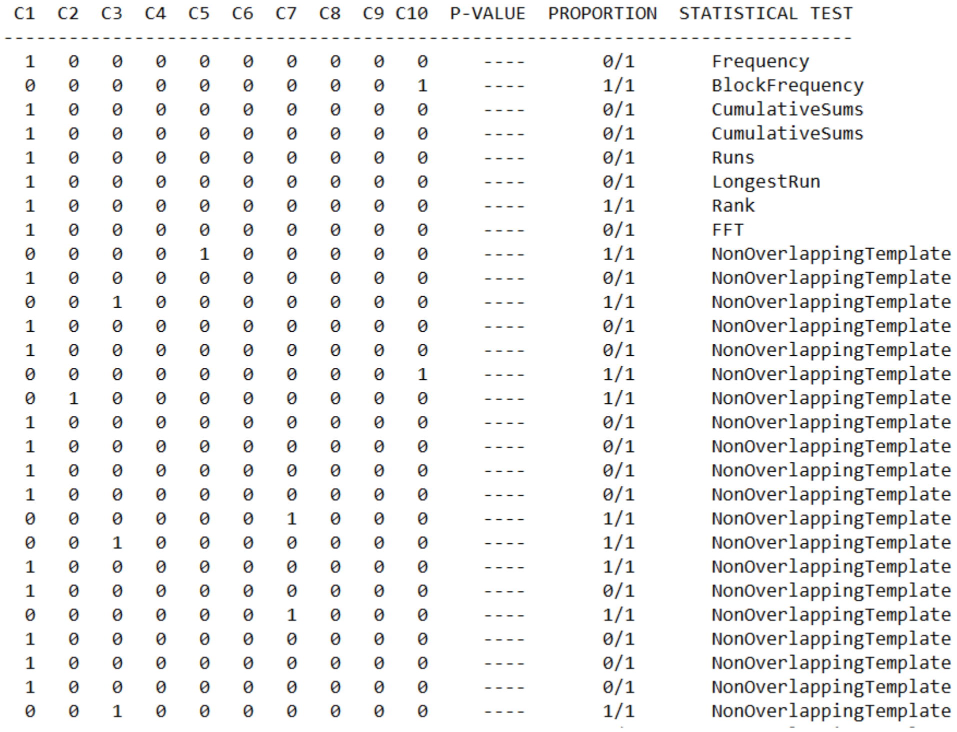
$r_4 =- 16$

$r_5 = 27$

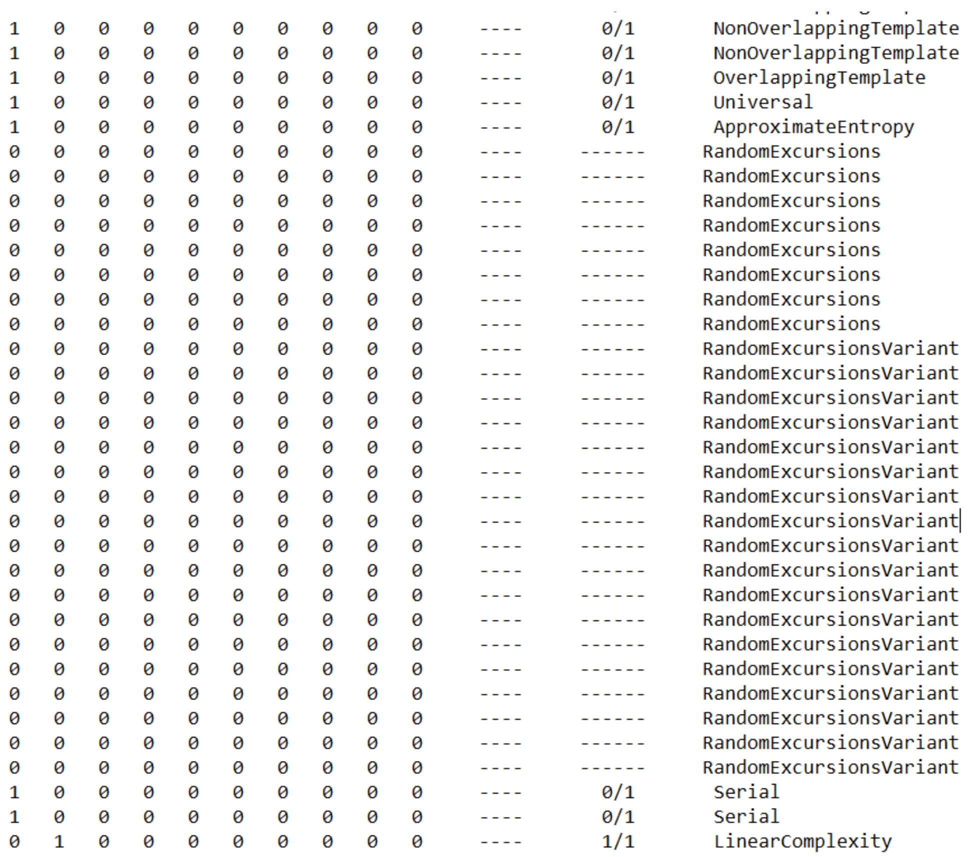
Количества единиц и нулей примерно равны.

Значения автокорреляционной функции не близки к нулю (значит, последовательность недостаточно случайная).

Бонусное задание 1)Результат тестирования последовательности:



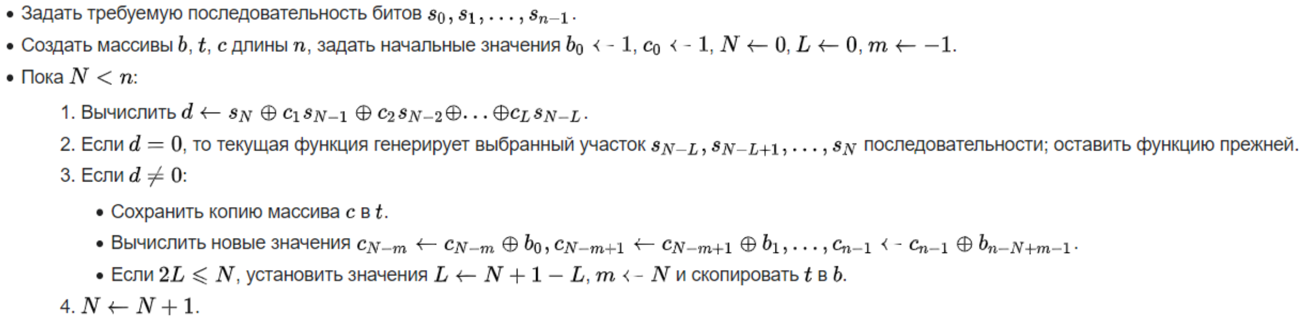
```
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
  1   0   0   0   0   0   0   0   0   0    ----       0/1      Frequency
  0   0   0   0   0   0   0   0   0   1    ----       1/1      BlockFrequency
  1   0   0   0   0   0   0   0   0   0    ----       0/1      CumulativeSums
  1   0   0   0   0   0   0   0   0   0    ----       0/1      CumulativeSums
  1   0   0   0   0   0   0   0   0   0    ----       0/1      Runs
  1   0   0   0   0   0   0   0   0   0    ----       0/1      LongestRun
  1   0   0   0   0   0   0   0   0   0    ----       1/1      Rank
  1   0   0   0   0   0   0   0   0   0    ----       0/1      FFT
  0   0   0   0   1   0   0   0   0   0    ----       1/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  0   0   1   0   0   0   0   0   0   0    ----       1/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  0   0   0   0   0   0   0   0   0   1    ----       1/1      NonOverlappingTemplate
  0   1   0   0   0   0   0   0   0   0    ----       1/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  0   0   0   0   0   0   1   0   0   0    ----       1/1      NonOverlappingTemplate
  0   0   1   0   0   0   0   0   0   0    ----       1/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       1/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  0   0   0   0   0   0   1   0   0   0    ----       1/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----       0/1      NonOverlappingTemplate
  0   0   1   0   0   0   0   0   0   0    ----       1/1      NonOverlappingTemplate
```



```
  1   0   0   0   0   0   0   0   0   0    ----      0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----      0/1      NonOverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----      0/1      OverlappingTemplate
  1   0   0   0   0   0   0   0   0   0    ----      0/1      Universal
  1   0   0   0   0   0   0   0   0   0    ----      0/1      ApproximateEntropy
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursions
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  0   0   0   0   0   0   0   0   0   0    ----    ------    RandomExcursionsVariant
  1   0   0   0   0   0   0   0   0   0    ----      0/1      Serial
  1   0   0   0   0   0   0   0   0   0    ----      0/1      Serial
  0   1   0   0   0   0   0   0   0   0    ----      1/1      LinearComplexity
```

По значениям в столбце Proportion можно увидеть, какие тесты последовательность прошла (1/1), а какие провалила (0/1).

Бонусное задание 2)Алгоритм:



- Задать требуемую последовательность битов $s_0, s_1, \ldots, s_{n-1}$.
- Создать массивы b, t, c длины n, задать начальные значения $b_0 \leftarrow 1$, $c_0 \leftarrow 1$, $N \leftarrow 0$, $L \leftarrow 0$, $m \leftarrow -1$.
- Пока $N < n$:
    1. Вычислить $d \leftarrow s_N \oplus c_1 s_{N-1} \oplus c_2 s_{N-2} \oplus \ldots \oplus c_L s_{N-L}$.
    2. Если $d = 0$, то текущая функция генерирует выбранный участок $s_{N-L}, s_{N-L+1}, \ldots, s_N$ последовательности; оставить функцию прежней.
    3. Если $d \neq 0$:
        - Сохранить копию массива c в t.
        - Вычислить новые значения $c_{N-m} \leftarrow c_{N-m} \oplus b_0, c_{N-m+1} \leftarrow c_{N-m+1} \oplus b_1, \ldots, c_{n-1} \leftarrow c_{n-1} \oplus b_{n-N+m-1}$.
        - Если $2L \leqslant N$, установить значения $L \leftarrow N + 1 - L$, $m \leftarrow N$ и скопировать t в b.
    4. $N \leftarrow N + 1$.