**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ**

**И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. Проф. М.А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра Защищенных систем связи

Дисциплина «Основы криптографии»

**Лабораторная работа № 9**

**Моделирование работы линейного рекуррентного регистра и исследование характеристик рекуррентной последовательности**

Выполнил: ст. гр. ИКТЗ-83 Урванцев Г.А.

Проверил: д.т.н., проф. Яковлев В. А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

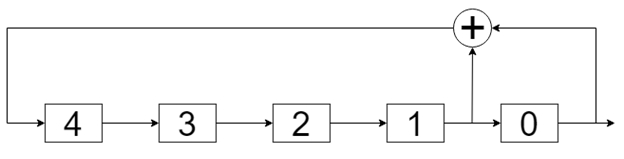
Цель лабораторной работы:

* Анализ работы ЛРР и исследование характеристик рекуррентной последовательности

**Выполнение работы:**

Построение ЛРР по заданному характеристическому многочлену *h(x)*

Вариант 26: 



Моделирование работа ЛРР, таблица смены его состояний

1-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Выход сдвига |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 2 | 1 | 1 | 1 | 1 | 0 | 0 |
| 3 | 1 | 1 | 1 | 1 | 1 | 1 |
| 4 | 0 | 1 | 1 | 1 | 1 | 1 |
| 5 | 0 | 0 | 1 | 1 | 1 | 1 |
| 6 | 0 | 0 | 0 | 1 | 1 | 1 |
| 7 | 0 | 0 | 0 | 0 | 1 | 1 |
| 8 | 1 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 1 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 1 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 1 | 0 | 0 |
| 12 | 1 | 0 | 0 | 0 | 1 | 1 |
| 13 | 1 | 1 | 0 | 0 | 0 | 0 |
| 14 | 0 | 1 | 1 | 0 | 0 | 0 |
| 15 | 0 | 0 | 1 | 1 | 0 | 0 |
| 16 | 1 | 0 | 0 | 1 | 1 | 1 |
| 17 | 0 | 1 | 0 | 0 | 1 | 1 |
| 18 | 1 | 0 | 1 | 0 | 0 | 0 |
| 19 | 0 | 1 | 0 | 1 | 0 | 0 |
| 20 | 1 | 0 | 1 | 0 | 1 | 1 |
| 21 | 1 | 1 | 0 | 1 | 0 | 0 |

Т.к. в шаге 21 последовательность повторяется заново, найдем другие последовательности. Для этого за первый шаг регистра возьмем такое состояние, которого не было раньше.

2-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Выход сдвига |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 2 | 1 | 1 | 0 | 0 | 1 | 1 |
| 3 | 1 | 1 | 1 | 0 | 0 | 0 |
| 4 | 0 | 1 | 1 | 1 | 0 | 0 |
| 5 | 1 | 0 | 1 | 1 | 1 | 1 |
| 6 | 0 | 1 | 0 | 1 | 1 | 1 |
| 7 | 0 | 0 | 1 | 0 | 1 | 1 |

3-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Выход сдвига |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 2 | 1 | 1 | 0 | 1 | 1 | 1 |
| 3 | 0 | 1 | 1 | 0 | 1 | 1 |

Общее число состояний – 31, моделирование работы регистра проведено верно.

Исследование линейной рекуррентной последовательности

* Период последовательности максимальной длины:
* Баланс единиц и нулей в ней: 47,62% единиц, 52,38% нулей

Вывод: свойство баланса не соблюдено

* Найти серии и подсчитать их количество:

Всего серий: 10

1(4 серии) + 2(2 серии) + 3(1 серия) + 4(1 серия) + 5(1 серия)

40% + 20% +10% +10% +10%

Вывод: свойство серий выполняется

* Проверить свойство «окна»:

11010100110001000011111010

11010

10101

01010

10100

01001

10011

00110

01100

11000

10001

00010

00100

01000

10000

00001

00011

00111

01111

11111

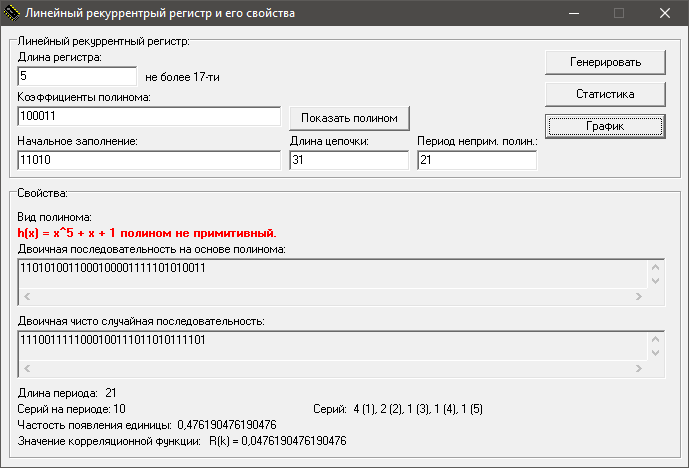
11110

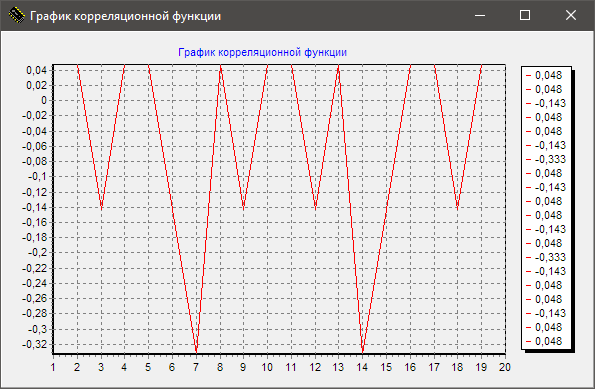
11101

11010

Вывод: свойство окна не действительно

Проверка на совпадение характеристик последовательности





Характеристики совпадают, проверка проведена верно.

Выводы:

* Данный полином не является примитивным, т. к. длина периода (21) не равна
* В данной работе были получены навыки по работе с линейным рекуррентным регистром
* В ходе моделирования работы ЛРР на компьютере, совпали все характеристики.
* Для данного регистра выполняется только свойство серий