**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 Громов А.А.

Проверил: д.т.н., проф. Яковлев В. А.

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

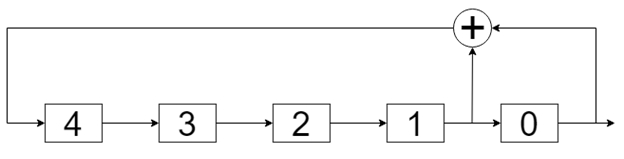
Цель лабораторной работы:

* Анализ работы ЛРР и исследование характеристик рекуррентной последовательности

**Выполнение работы:**

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

Вариант 4:



Моделирование работа ЛРР, таблица смены его состояний

1-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Сдвиг |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 2 | 0 | 1 | 0 | 0 | 1 | 1 |
| 3 | 0 | 0 | 1 | 0 | 0 | 0 |

Так как период не равен 31, найдем остальные периоды.

2-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Сдвиг |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 1 | 1 |
| 3 | 1 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 1 | 0 | 0 | 0 | 0 |
| 5 | 1 | 0 | 1 | 0 | 0 | 0 |
| 6 | 1 | 1 | 0 | 1 | 0 | 0 |
| 7 | 1 | 1 | 1 | 0 | 1 | 1 |
| 8 | 1 | 1 | 1 | 1 | 0 | 0 |
| 9 | 0 | 1 | 1 | 1 | 1 | 1 |
| 10 | 1 | 0 | 1 | 1 | 1 | 1 |
| 11 | 0 | 1 | 0 | 1 | 1 | 1 |
| 12 | 0 | 0 | 1 | 0 | 1 | 1 |

3-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Сдвиг |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| 2 | 1 | 1 | 0 | 0 | 0 | 0 |
| 3 | 1 | 1 | 1 | 0 | 0 | 0 |
| 4 | 0 | 1 | 1 | 1 | 0 | 0 |
| 5 | 0 | 0 | 1 | 1 | 1 | 1 |
| 6 | 0 | 0 | 0 | 1 | 1 | 1 |

4-я последовательность:

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

5-я последовательность:

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

6-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Сдвиг |
| 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 |

7-я последовательность:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Сдвиг |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 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: 50% единиц, 50% нулей

Вывод: свойство баланса не соблюдено

* Найти серии и подсчитать их количество:

Всего серий: 7

1(5 серии) + 3(1 серия) + 4(1 серия)

Вывод: свойство серий не выполняется

* Проверить свойство «окна»:

00101111010000101 11101000010111

00101

01011

10111

01111

11110

11101

11010

10100

01000

10000

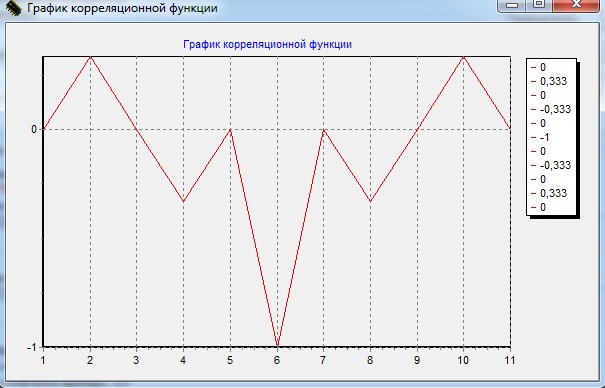
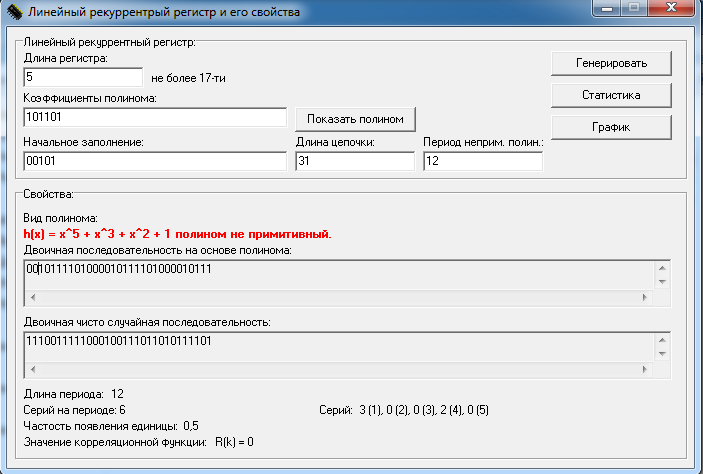
00001

00010

00101

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