**Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации**

**ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникации им. проф. М.А. Бонч-Бруевича»**

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

Факультет: ИКСС

Отчет по лабораторной работе №10

“ Моделирование работы формирователя случайной гаммы и исследование характеристик гаммы”

Выполнил: Громов А.А.

Группа: ИКТЗ-83

Проверил: Яковлев В.А.

Санкт-Петербург

2021 г.

1. Вариант 4 (530). Характеристический многочлен:
2. Схема линейного рекуррентного регистра

0

1

2

3

4

1. Таблица смены состояний

Начальное заполнение регистра S=NÅK

N = 00100 K = 01010 S = 01110

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | Сдвиг |
| 0 | 0 | **1** | **1** | **1** | 0 | 0 |
| 1 | **1** | 0 | **1** | **1** | **1** | **1** |
| 2 | **1** | **1** | 0 | **1** | **1** | **1** |
| 3 | 0 | **1** | **1** | 0 | **1** | **1** |
| 4 | 0 | 0 | **1** | **1** | 0 | 0 |
| 5 | 0 | 0 | 0 | **1** | **1** | **1** |
| 6 | **1** | 0 | 0 | 0 | **1** | **1** |
| 7 | **1** | **1** | 0 | 0 | 0 | 0 |
| 8 | **1** | **1** | **1** | 0 | 0 | 0 |
| 9 | **1** | **1** | **1** | **1** | 0 | 0 |
| 10 | **1** | **1** | **1** | **1** | **1** | **1** |
| 11 | 0 | **1** | **1** | **1** | **1** | **1** |
| 12 | 0 | 0 | **1** | **1** | **1** | **1** |
| 13 | **1** | 0 | 0 | **1** | **1** | **1** |
| 14 | **1** | **1** | 0 | 0 | **1** | **1** |
| 15 | 0 | **1** | **1** | 0 | 0 | 0 |
| 16 | **1** | 0 | **1** | **1** | 0 | 0 |
| 17 | 0 | **1** | 0 | **1** | **1** | **1** |
| 18 | 0 | 0 | **1** | 0 | **1** | **1** |
| 19 | **1** | 0 | 0 | **1** | 0 | 0 |
| 20 | 0 | **1** | 0 | 0 | **1** | **1** |
| 21 | 0 | 0 | **1** | 0 | 0 | 0 |
| 22 | 0 | 0 | 0 | **1** | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | **1** | **1** |
| 24 | **1** | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | **1** | 0 | 0 | 0 | 0 |
| 26 | **1** | 0 | **1** | 0 | 0 | 0 |
| 27 | 0 | **1** | 0 | **1** | 0 | 0 |
| 28 | **1** | 0 | **1** | 0 | **1** | **1** |
| 29 | **1** | **1** | 0 | **1** | 0 | 0 |
| 30 | **1** | **1** | **1** | 0 | **1** | **1** |
| 31 | 0 | **1** | **1** | **1** | 0 | 0 |

1. Исследуем полученную линейную рекуррентную последовательность

Период последовательности

*T=31*

Баланс единиц и нулей: 0111011000111110011010010000101

*Единиц – 16; Нулей – 15*

*Вывод: Свойство баланса выполняется. ЛРР содержит на полном периоде 2n-1 единиц и 2n-1-1 нуль.*

Серии:

*Всего 16: (1)=8; (2)=4; (3)=2; (4)=1; (5)=1*

*Вывод: Свойство серий выполняется. В любой выходной последовательности полного периода половина всех серий из нулей или из единиц имеет длину 1, четверть - длину 2, восьмая часть - длину 3*

Свойства “окна”:

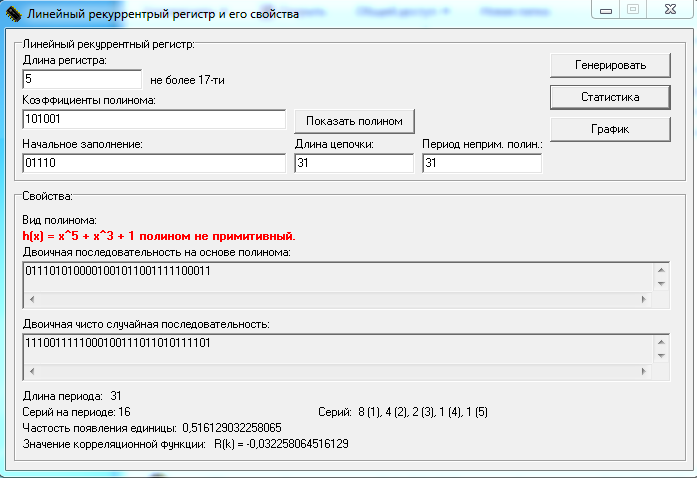
*n=5*

0111011000111110011010010000101

01110  
 11101  
 11011  
 10110  
 01100  
 11000  
 10001  
 00011  
 00111  
 01111  
 11111  
 11110  
 11100  
 11001  
 10011  
 10110  
 01101  
 11010  
 10100  
 01001  
 10010  
 00100  
 01000  
 10000  
 00001  
 00010  
 00101

*Вывод: Свойство «окна» выполняется. Каждая комбинация видна в окне ровно один раз. Всего комбинаций равно числу периоду = 31*

1. Проверка полученных результатов в программе



1. Моделирование работы формирователя случайной гаммы. Вариант 4.

0

1

2

3

4

И

ИЛИ

УЛ

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | 4 ячейка | 3 ячейка | 2 ячейка | 1 ячейка | 0 ячейка | или | и | ул |
| 0 | 0 | **1** | **1** | **1** | 0 | 1 | 0 | **1** |
| 1 | **1** | 0 | **1** | **1** | **1** | 1 | 1 | **1** |
| 2 | **1** | **1** | 0 | **1** | **1** | 1 | 1 | 0 |
| 3 | 0 | **1** | **1** | 0 | **1** | 1 | 0 | **1** |
| 4 | 0 | 0 | **1** | **1** | 0 | 0 | 0 | **1** |
| 5 | 0 | 0 | 0 | **1** | **1** | 0 | 1 | 0 |
| 6 | **1** | 0 | 0 | 0 | 1 | 1 | 0 | **1** |
| 7 | **1** | **1** | 0 | 0 | 0 | 1 | 0 | **1** |
| 8 | **1** | **1** | **1** | 0 | 0 | 1 | 0 | **1** |
| 9 | **1** | **1** | **1** | **1** | 0 | 1 | 0 | **1** |
| 10 | **1** | **1** | **1** | **1** | **1** | 1 | 1 | **1** |
| 11 | 0 | **1** | **1** | **1** | **1** | 1 | 1 | **1** |
| 12 | 0 | 0 | **1** | **1** | **1** | 0 | 1 | 0 |
| 13 | **1** | 0 | 0 | **1** | **1** | 1 | 1 | 0 |
| 14 | **1** | **1** | 0 | 0 | **1** | 1 | 0 | **1** |
| 15 | 0 | **1** | **1** | 0 | 0 | 1 | 0 | **1** |
| 16 | **1** | 0 | **1** | **1** | 0 | 1 | 0 | **1** |
| 17 | 0 | **1** | 0 | **1** | **1** | 1 | 1 | 0 |
| 18 | 0 | 0 | **1** | 0 | **1** | 0 | 0 | **1** |
| 19 | **1** | 0 | 0 | **1** | 0 | 1 | 0 | **1** |
| 20 | 0 | **1** | 0 | 0 | **1** | 1 | 0 | **1** |
| 21 | 0 | 0 | **1** | 0 | 0 | 0 | 0 | **1** |
| 22 | 0 | 0 | 0 | **1** | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | **1** | 0 | 0 | 0 |
| 24 | **1** | 0 | 0 | 0 | 0 | 1 | 0 | **1** |
| 25 | 0 | **1** | 0 | 0 | 0 | 1 | 0 | **1** |
| 26 | **1** | 0 | **1** | 0 | 0 | 1 | 0 | **1** |
| 27 | 0 | **1** | 0 | **1** | 0 | 1 | 0 | **1** |
| 28 | **1** | 0 | **1** | 0 | **1** | 1 | 0 | **1** |
| 29 | **1** | **1** | 0 | **1** | 0 | 1 | 0 | **1** |
| 30 | **1** | **1** | **1** | 0 | **1** | 1 | 0 | **1** |
| 31 | 0 | **1** | **1** | **1** | 0 | 1 | 0 | **1** |

ШГ: 1111111001111011100111111011011

1. Исследование полученной последовательности

Период последовательности

*T=31*

Баланс единиц и нулей: 1111111001111011100111111011011

*Единиц – 24; Нулей – 7*

*Вывод: Свойство баланса невыполняется*

Серии:

*Всего 11: (1)=3; (2)=3; (3)=1; (4)=1; (6)=1; (9)=1;*

*Вывод: Свойство серий не выполняется.*

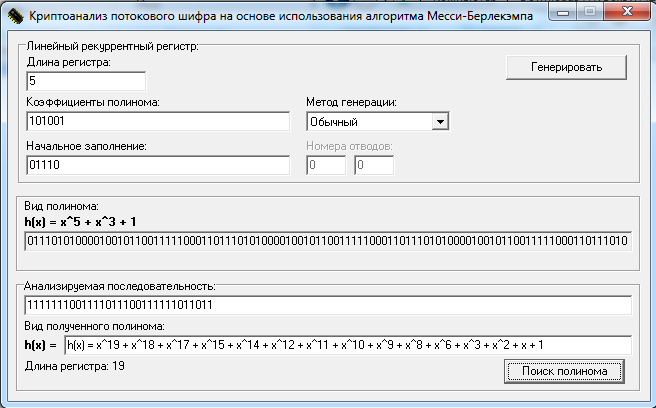
Свойства “окна”:

*n=5*

1111111001111011100111111011011

11111  
 11111  
*Вывод: Свойство «окна» не выполняется. Комбинации видны несколько раз.*

1. ЛЭС и построение регистра



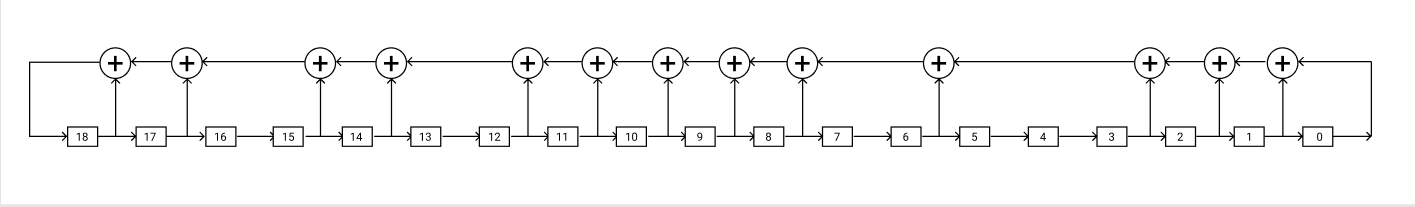
Поученный полином:

h(x) = x^19 + x^18 + x^17 + x^15 + x^14 + x^12 + x^11 + x^10 + x^9 + x^8 + x^6 + x^3 + x^2 + x + 1

Регистр: 11101101111101001111

Длина регистра = 19 => ЛЭС = 19

Схема регистра:



Вывод:

В ходе выполнения лабораторной работы мы построили линейно рекурсивный регистр по заданному многочлену, провели моделирование работы ЛРР, представив таблицу смены его состояний. Исследовали его свойства и проверили правильность выполнения в программе. Выполнили моделирование работы формирователя случайной гаммы, используя, в соответствие с вариантом, нелинейные узлы.

*Пригоден ли данный формирователь шифрующих гамм для шифрования?*

Вырабатываемая шифратором гамма, в данной работе, имеет малый период. Величина ЛЭС также мала. Регистр имеет короткую длину, по этой причине количество ключей шифратора будет небольшим. Я считаю, что такой формирователь шифрующих гаммне годится для шифрования.