СОДЕРЖАНИЕ

[1. Нахождение примитивных полиномов ГПСП 2](#_Toc200030367)

[2. Аналитическое деление заданного слова на полином делитель 2](#_Toc200030368)

[3. Имитационное моделирование получения обратной сигнатуры 4](#_Toc200030369)

1. Нахождение примитивных полиномов ГПСП

Для 5-разрядного ГПСП полином имеет вид

где коэффициенты a₁, a₂, a₃, a₄ ∈ {0, 1}. Константная 1 гарантирует выполнение условий непроводимости и примитивности. Имеется ровно   
2⁴ = 16 вариантов выбора коэффициентов.

Суть задачи сводится к следующему: для каждого из 16 кандидатов проверить, является ли соответствующий генератор максимального периода. Для 5ГПСП максимальный период равен **2⁵ – 1 = 31**. Если при инициализации генератора ненулевым состоянием (в нашем случае 11111) и последовательном применении схемы обратной связи состояние регистра возвращается к начальному только через 31 такт, то полином является примитивным.

В таблице 1 перечислены найденные примитивные полиномы. Результат подтверждается теоремой: количество примитивных полиномов равно

Таблица 1 – Примитивные полиномы 5-разрядного ГПСП

|  |  |
| --- | --- |
| № | Примитивный полином |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |

1. Аналитическое деление заданного слова на полином делитель

Рассмотрим аналитический способ деления полинома. За делитель (порождающий полином) возьмем примитивный полином из таблицы 1: . Заданное слово представлено шестнадцатиразрядным словом 1010 1111 0011 0011.

Это слово можно представить, как полином p(x) степени 15, где старший разряд соответствует x15. Распишем биты по позициям:

* Бит15 (x15): 1
* Бит14 (x14): 0
* Бит13 (x13): 1
* Бит12 (x12): 0
* Бит11 (x11): 1
* Бит10 (x10): 1
* Бит9 (x9): 1
* Бит8 (x8): 1
* Бит7 (x7): 0
* Бит6 (x6): 0
* Бит5 (x5): 1
* Бит4 (x4): 1
* Бит3 (x3): 0
* Бит2 (x2): 0
* Бит1 (x1): 1
* Бит0 (x0): 1

Таким образом:

Разделим полученный полином на порождающий аналитически:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |
|  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Воспроизведем с помощью программы Modius имитационное моделирование этой процедуры. Построим сигнатурный анализатор для порождающего полинома, показанный на рисунке 1.

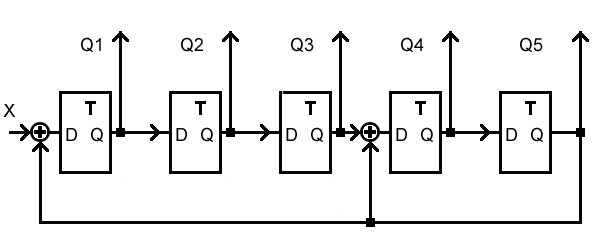


Рисунок 1 – Сигнатурный анализатор вида

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1100110011110101 |  | 0 | 0 | 0 | 0 | 0 |
| 1 | 110011001111010 |  | 1 | 0 | 0 | 0 | 0 |
| 2 | 11001100111101 |  | 1 | 1 | 0 | 0 | 0 |
| 3 | 1100110011110 |  | 0 | 1 | 1 | 0 | 0 |
| 4 | 110011001111 |  | 0 | 0 | 1 | 1 | 0 |
| 5 | 11001100111 |  | 1 | 0 | 0 | 1 | 1 |
| 6 | 1100110011 |  | 0 | 1 | 0 | 1 | 1 |
| 7 | 110011001 |  | 1 | 0 | 1 | 1 | 1 |
| 8 | 11001100 |  | 1 | 1 | 0 | 0 | 1 |
| 9 | 1100110 |  | 0 | 1 | 1 | 1 | 0 |
| 10 | 110011 |  | 1 | 1 | 1 | 0 | 1 |
| 11 | 11001 |  | 0 | 1 | 0 | 0 | 1 |
| 12 | 1100 |  | 0 | 0 | 1 | 1 | 0 |
| 13 | 110 |  | 0 | 0 | 0 | 1 | 1 |
| 14 | 11 |  | 0 | 0 | 0 | 1 | 1 |
| 15 | 1 |  | 1 | 0 | 0 | 1 | 1 |
|  |  |  | 0 | 1 | 0 | 1 | 1 |
|  |  |  |  |  |  |  |  |

Полученные аналитически и в результате моделирования сигнатуры совпадают.

1. Имитационное моделирование получения обратной сигнатуры

Для полинома найдем обратный полином:

С помощью имитационного моделирования найдем .

Матрица, составленная из коэффициентов полинома делителя , следующая:

Найдем :

Таким образом, моделирование выполнено верно.