**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

**Институт кибербезопасности и цифровых технологий**

**Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»**

Отчет по практической работе № 2

по дисциплине «Специальные разделы математики»

Тема: «Линейные регистры сдвига»

Выполнил: студент группы ББМО-01-25

\_\_\_Мухаметшин Александр Ринатович\_

Проверила:

Изотова Анастасия Андреевна

Москва, 2025

**ЗАДАНИЕ**

Задание 5. Реализация LFSR с другим многочленом и начальным состоянием

Условие:

Реализуйте LFSR длины 5 с многочленом обратной связи ( x^5 + x^2 + 1 ) (т.е. taps = [5, 2]) и начальным состоянием [0, 1, 0, 0, 1]. Сгенерируйте последовательность длиной 31 бит.

Задание 6. Определение периода LFSR с разными начальными состояниями

Условие:

Для LFSR с многочленом ( x^4 \u002B x \u002B 1 ) (taps = [4, 1]) найдите период для следующих начальных состояний:

• [1, 0, 0, 0]

• [0, 1, 0, 0]

• [1, 1, 1, 1]

Сравните полученные периоды и сделайте выводы.

Задание 7. Исследование влияния многочлена обратной связи на период для 3-битного LFSR

Условие:

Для регистра длины 3 сравните периоды LFSR с многочленами:

• ( x^3 + x + 1 ) (taps = [3, 1])

• ( x^3 + x^2 + 1 ) (taps = [3, 2])

Начальное состояние — [1, 0, 0].

Задание 8. Генерация псевдослучайных чисел с LFSR и анализ распределения

Условие:

Используя LFSR с многочленом ( x^6 + x + 1 ) (taps = [6, 1]) и начальным состоянием [1,0,0,0,0,0], сгенерируйте последовательность длиной 63 бита. Подсчитайте количество единиц и нулей и постройте гистограмму распределения (можно с помощью matplotlib).

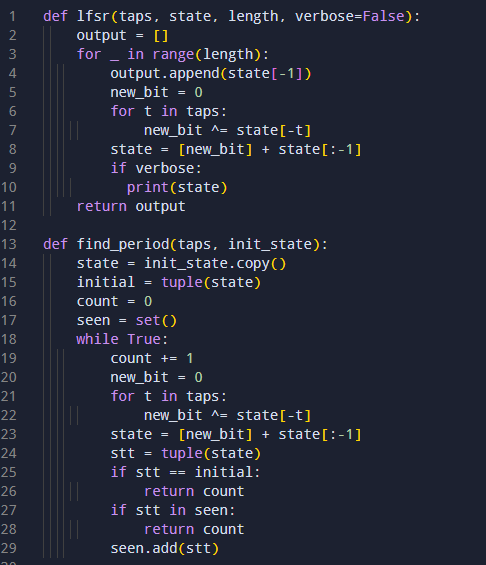
Задание 9. Реализация LFSR с обратной связью по нескольким битам и визуализация состояния

Условие:

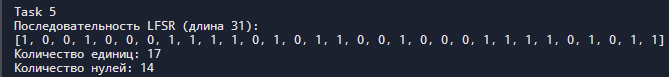
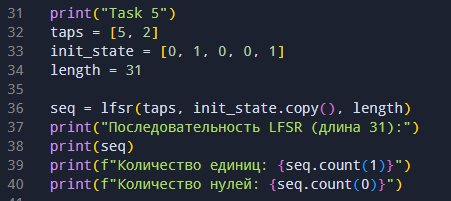
Реализуйте LFSR длины 4 с многочленом ( x^4 + x^3 + 1 ) (taps = [4, 3]) и начальным состоянием [1, 1, 0, 0]. Выведите в консоль состояние регистра на каждом шаге, а также итоговую последовательность длиной 15.

**ХОД РАБОТЫ**

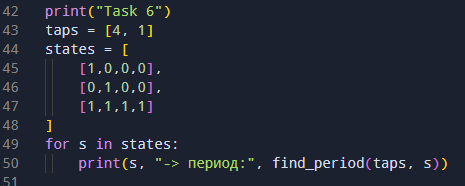
Основные функции, используемые для заданий



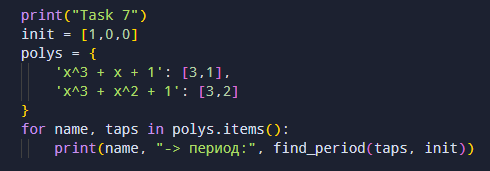
Реализация и вывод задания 5



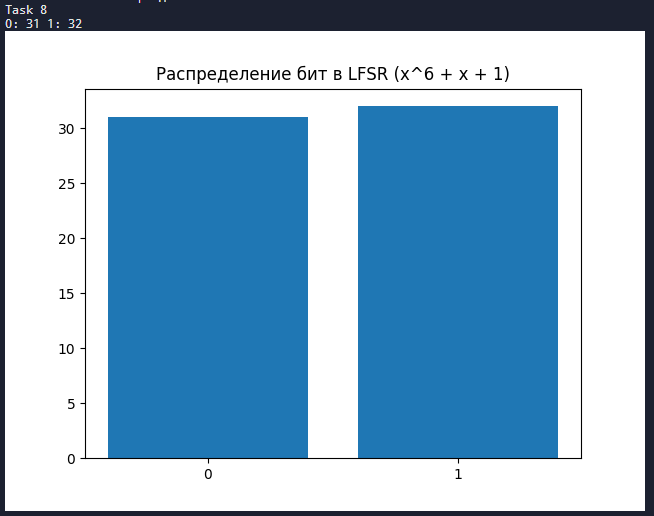
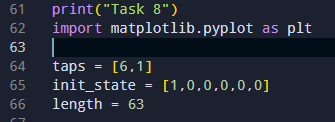
Реализация и вывод задания 6



Реализация и вывод задания 7



Реализация и вывод задания 8



Реализация и вывод задания 9

