1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ЛАБОРАТОРНАЯ РАБОТА № 4**

1. по дисциплине «Основы построения стойких криптопримитивов и псевдослучайных генераторов»
2. Выполнил
3. студент гр. 5151001/00201 Устюгов А.А.

<*подпись*>

1. Преподаватель д.ф.-м.н. Шенец Н.Н.

<*подпись*>

1. Санкт-Петербург
2. 2024

# Цель работы

Изучение свойств линейных рекуррентных последовательностей и методов оценивания их параметров.

# Задание

1. Получить у преподавателя вариант задания, содержащий характеристический многочлен линейной рекуррентной последовательности.
2. Написать программу П-1, которая по заданному вектору начального состояния S0 генерировать линейную рекуррентную последовательность заданной длины L. Последовательность должна записываться в бинарный файл.
3. Написать программу П-2, которая для заданного отрезка линейной рекуррентной последовательности оценивает снизу порядок л.р.п на основе ганкелевых определителей, а также определяет минимальный многочлен этой последовательности с помощью алгоритма Берлекэмпа-Мэсси по отрезку длины 2k. Параметры L и k должны вводиться пользователем, а последовательность – считываться из бинарного файла.
4. Выполнить задание, указанное в варианте.

# Ход работы

## Теоретические сведения

Линейная рекуррентная последовательность порядка *n* задается следующим соотношением:

При этом задается начальное состояние , которое определяется по ключу .

Линейная рекуррентная последовательность может быть записана в матричном виде: , где – первая компонента вектора , матрица имеет вид:

Характеристический многочлен матрицы имеет вид

Данный многочлен также называют характеристическим многочленом л.р.п., а матрицу – сопровождающей матрицей многочлена.

Минимальным многочленом называют такой многочлен, что всякий характеристический многочлен последовательности делится на . Степень минимального многочлена называют линейной сложностью последовательности. Л.р.п, заданная неприводимым многочленом является чисто периодической и ее минимальный период совпадает с порядком ее минимального многочлена.

## Исходные данные

Номер варианта – 6. Характеристический многочлен = 84163 = . Начальное заполнение 3855 = 0000 1111 0000 1111. L = 131 072, k = 32.

## Примеры работоспособности программы

Была написана П-1, генерирующая л.р.п. с заданным в варианте характеристическим многочленом и берущая с стандартного потока ввода начальное заполнение и длину последовательности. На рисунках 1 и 2 представлены результаты работы программы при L = 128, начальное заполнение на рисунке 1 - , на рисунке 2 - .

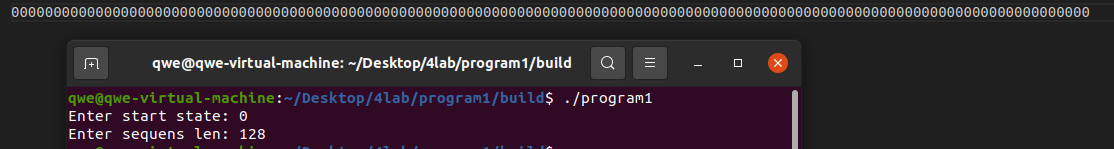


Рисунок 1 – сгенерированная последовательность при

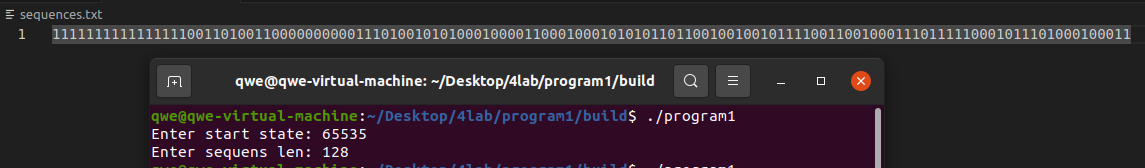
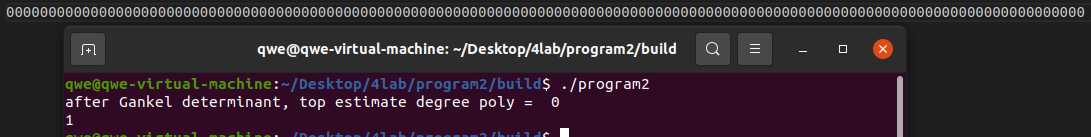


Рисунок 2 – сгенерированная последовательность при

Далее была протестирована программа П-2, берущая на вход L и k и читающая с файла последовательность. На вход были поданы нулевая последовательность, единичная последовательность и последовательность вида {1001}. L = 128, k = 8. Результаты, представленные на рисунках 3, 4, 5, были сравнены с выводом sagemath.



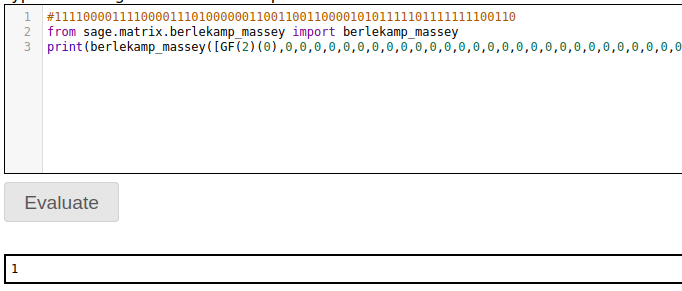
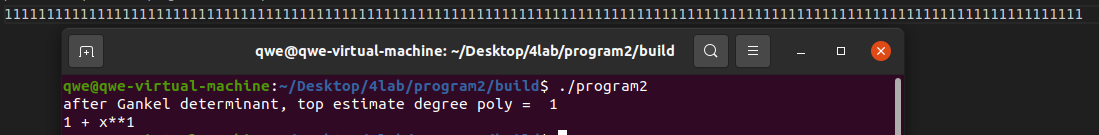


Рисунок 3 – минимальный многочлен нулевой последовательности



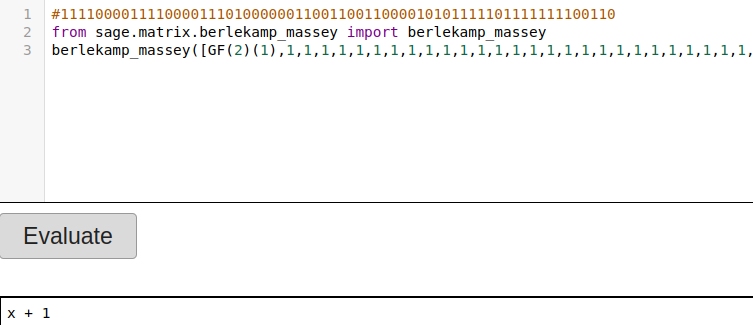
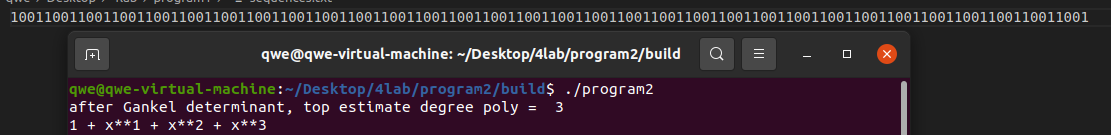


Рисунок 4 – минимальный многочлен единичной последовательности



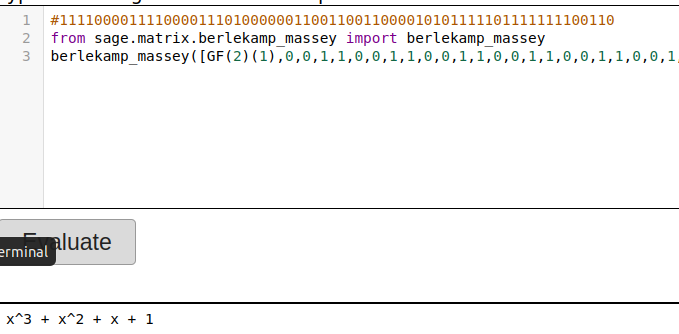
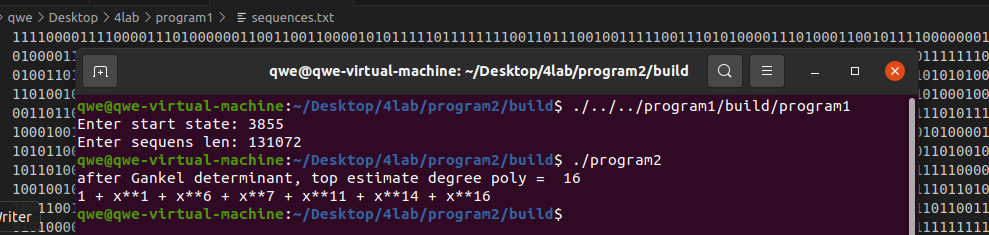


Рисунок 5 – минимальный многочлен последовательности вида {1001}

Далее, в соответствии с вариантом, П-1 сгенерировала последовательность с S0 = 3855 длины 131072. Эта последовательность была подана на вход П-2, которая ищет минимальный многочлен последовательности. На рисунке 6 представлен вывод П-2, а также проверка полученной от П-1 последовательности в sagemath.



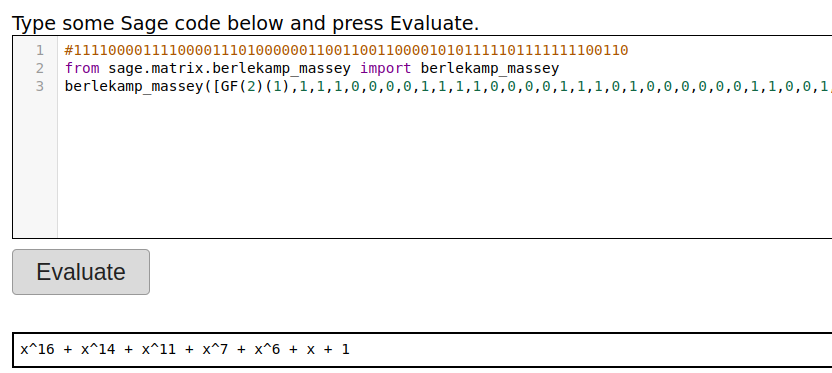


Рисунок 6 – минимальный многочлен последовательности, заданной в варианте

# Контрольные вопросы

1. *Что такое минимальный многочлен линейной рекуррентной последовательности?*

Минимальным многочленом m(x) называют такой многочлен, что всякий характеристический многочлен последовательности делится на m(x).

1. *Чему равен период л.р.п. порядка n, заданной над конечным полем и имеющей примитивный характеристический многочлен?*

Примитивный многочлен неприводим, поэтому период л.р.п совпадает с порядком примитивного характеристического многочлена.

1. *Что такое порядок многочлена?*

Порядком многочлена называется наименьшее число *e,* такое, что многочлен делится на .

1. *Докажите, что многочлен делит многочлен тогда и только тогда, когда порядок многочлена делит r.*

# Вывод

В результате данной работы были написаны две программы, одна из которых генерирует л.р.п по заданному характеристическому многочлену, а другая по полученной последовательности оценивает порядок и минимальный многочлен.