Доп. дисциплины

Магистры весна 2021

Занятие 9

ЛИНЕЙНЫЕ РЕГИСТРЫ СДВИГА

06.05.2021

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Рекуррентные последовательности

Определение. *Последовательность называется рекуррентной, если следующий ее член зависит от нескольких предыдущих.*

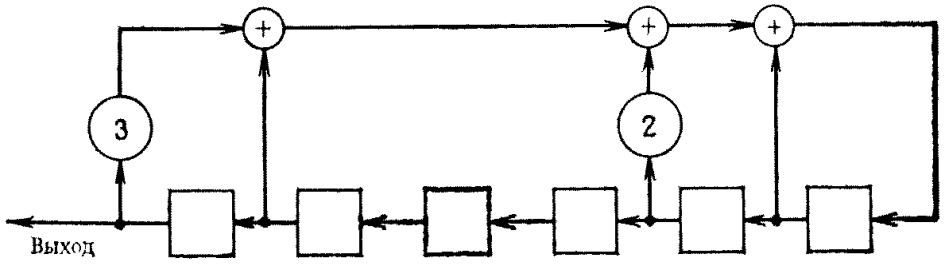
Определение. *Начальные значения* $\boldsymbol{s}_0 = (s_0, s_1, \ldots, sn)$ *называются вектором инициализации.*

Пример 1 *регистра сдвига над полем GF(5)* $S_{n+6} = S_{n+5} + 2S_{n+4} + S_{n+1} + 3S_n$, $n = 0, 1, 2,\ldots$ *и его схема*.

Решение. Для того чтобы в поле GF(5) получить линейную рекуррентную последовательность, удовлетворяющую однородному линейному рекуррентному соотношению

$$S_{n+6} = S_{n+5} + 2S_{n+4} + S_{n+1} + 3S_n,\ n = 0, 1, 2,\ldots$$

можно использовать регистр сдвига с обратной связью, изображенный ниже. Так как $a_2 = a_3 = 0$, соответствующие соединения не нужны.



Пример 2. *Поиск максимального период регистра сдвига вида*

$S_{N+2} = 2*S_{N+1} + 3*S_N$ *над полем GF(5).*

Решение. Поскольку регистр сдвига задается соотношением второго порядка, то его начальным вектором состояния (вектором инициализации) является вектор из двух элементов над полем GF(5).

Различных таких векторов всего $5^2 = 25$. Однако, для нулевого начального вектора (0,0), очевидно, выходная последовательность будет состоять из одних нулей. Следовательно, ее период будет равен 1. Поэтому нулевой начальный вектор можно не рассматривать.

Останется 24 ненулевых начальных векторов. В процессе работы регистра его начальный вектор $\mathbf{S_0} = (S_0, S_1)$ будет изменяться.

После первого такта он станет равен $\mathbf{S_1} = (S_1, S_2)$, после второго такта $\mathbf{S_2} = (S_2, S_3)$, и т.д.

После n-го такта появится n-й вектор $\mathbf{S_n} = (S_n, S_{n+1})$. Как только вновь возникший вектор внутреннего состояния совпадет с одним из предыдущих векторов состояний, процесс начнет повторяться.

Поскольку ненулевых векторов всего 24, то цикл не может иметь длину больше чем 24 такта.

Вычислим длину цикла (или, как чаще говорят, длину периода) псевдослучайной последовательности, задаваемой нашим регистром сдвига.

Так как период зависит от вектора инициализации, то зададим вектор начального состояния, дающий максимальный период. Как известно из теории, таким вектором является импульсная функция, вектор вида

(0, 0, 0,…, 0, 1), в нашем случае вектор $\mathbf{S_0} = (S_0, S_1) = (0, 1)$.

Первый способ. Прямое вычисление по формуле регистра сдвига.

Поскольку $S_{N+2} = 2*S_{N+1} + 3*S_N$, то при N = 0 мы получаем, что

$S_2 = 2*1 + 3*0 = 2 \pmod 5$.

Аналогично, $S_3 = 2*2+3*1 = 7 \pmod 5 = 2$.

Продолжая вычислять по формуле регистра сдвига, последовательно будем получать – выписываем сразу результат: 0, 1, 2, 2, 0, 1, 2, 2, 0, 1, …

Таким образом, период равен 4, что в 6 раз меньше максимально возможного. С криптографической точки зрения наш регистр сдвига весьма слаб.

Второй способ. Вычисление явной формулы через корни характеристического многочлена.

Характеристическим многочленом для данного регистра сдвига является многочлен второй степени $X^2 - 2*X - 3$ над полем GF(5).

Найдем его корни в поле GF(5). Найти корни можно прямой проверкой, подставляя все элементы поля

GF(5) = {0, 1, 2, 3, 4}.

Убеждаемся, что корнями являются элементы 3 и 4.

(Мы говорим элементы 3 и 4, а не числа 3 и 4, потому, что эти элементы похожи на числа 3 и 4 только по написанию, а свойства у них совершенно другие, чем у чисел. Например, у «нормальных» чисел сумма 3 + 4 равна 7, а у элементов 3 и 4 поля GF(5) сумма элементов 3 + 4 равна элементу 2. Поэтому символы 3 и 4 можно рассматривать просто как номера некоторых новых сущностей. В данном случае элементов поля GF(5))

Из теории известно, что если - различные корни характеристического многочлена регистра сдвига второй степени, то можно указать явный вид n-го (т.е. произвольного) члена последовательности, порождаемой данным регистром. А именно, этот n-й член будет иметь вид

$$s_n = a_1 3^n + a_2 4^n$$

где неизвестные коэффициенты a_1, a_2 можно вычислить, зная начальное наполнение ячеек регистра. В нашем случае начальное наполнение

$$(S_0, S_1) = (0, 1).$$

Используя это составляем систему двух линейных уравнений от двух неизвестных (a_1, a_2) над полем GF(5):

$$\begin{cases} 0 = a_1 * 3^0 + a_2 * 4^0 \\ 1 = a_1 * 3^1 + a_2 * 4^1 \end{cases} \Rightarrow \begin{cases} 0 = a_1 + a_2 \\ 1 = a_1 * 3 + a_2 * 4 \end{cases} \Rightarrow \begin{cases} a_2 = -a_1 \\ 1 = a_1 * 3 + -a_1 * 4 \end{cases} \Rightarrow \begin{cases} a_2 = 1 \\ a_1 = 4 \end{cases}$$

Таким образом, получаем явную формулу для n-го члена

$$S_n = 4 * 3^n + 4^n = (-1) * 3^n + (-1)^n, n = 0,1,...$$

т.к. в поле GF(5) имеет место равенство 4 = -1.

Определим, как ведут себя степени элемента 3 в поле GF(5). Просто возводим элемент 3 в различные степени, а результат приводим по модулю 5. Получаем

$3^1 = 3$, $3^2 = 4$, $3^3 = 2$, $3^4 = 1$, $3^5 = 3$ и т.д.

Используя эти наблюдения вычисляем члены последовательности S_0, S_1, S_2, … по формуле (1) и получаем

0, 1, 2, 2, 0, 1,

Видим, что опять период получился равным 4.

Третий способ. Представим формулу регистра сдвига в матричном виде. В этом случае период последовательности, задаваемой регистром, будет равен той степени матрицы, в которой она будет равна единичной матрице.

Напомним связь между регистром сдвига над полем P

$$S_{n+k} = a_{k-1} * S_{n+k-1} + a_{k-2} * S_{n+k-2} + ... + a_1 * S_{n+1} + a_0 * S_n$$

и его матрицей A размера $k \times k$ над тем же полем P:

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 1 & 0 & \dots & 0 & 0 & a_1 \\ 0 & 1 & \dots & 0 & 0 & a_2 \\ 0 & 0 & \dots & 0 & 0 & a_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & a_{k-3} \\ 0 & 0 & \dots & 1 & 0 & a_{k-2} \\ 0 & 0 & \dots & 0 & 1 & a_{k-1} \end{pmatrix}$$

В нашем случае, когда k = 2, а регистр сдвига задан формулой

$S_{N+2} = 2*S_{N+1} + 3*S_N$

над полем Галуа GF(5) мы получаем матрицу A размера 2 на 2

$$A = \begin{pmatrix} 0 & a_0 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}$$

Вычисляя степени матрицы A последовательно получаем

$$A = \begin{pmatrix} 0 & 3 \\ 1 & 2 \end{pmatrix}, A^2 = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}, A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Итак, матрица A в 4-й степени равна единичной матрице, значит период последовательности, при самом лучшем выборе начального вектора, равен 4.

Все три способа дали один и тот же ответ.

Пример 3. *Для регистра сдвига с обратной связью $S_{N+4} = S_{N+1} + S_N$. над полем GF(2) и импульсной функции (0,0,0,1) прямым вычислением найти период.*

Решение. Производим непосредственные вычисления по формуле

$$S_{N+4} = S_{N+1} + S_N.$$

Регистр сдвига имеет порядок 4, потому вектор инициализации будет 4-х мерным, именно такая импульсная функция (0, 0, 0, 1) нам и дана.

Таким образом, $S_0 = 0$, $S_1 = 0$, $S_2 = 0$, $S_3 = 1$. Так как поле GF(2) содержит всего 2 элемента, а вектора состояний 4-х мерные, максимально возможный период рекуррентной последовательности равен $2^4 - 1 = 15$.

Значит, нам нужно вычислить 15 членов последовательности, начиная с 4-го и заканчивая 18-м:

$S_4 = S_1 + S_0 = 0 + 0 = 0$; $S_5 = S_2 + S_1 = 0 + 0 = 0$; $S_6 = S_3 + S_2 = 1 + 0 = 1$;

$S_7 = S_4 + S_3 = 0 + 1 = 1$; $S_8 = S_5 + S_4 = 0 + 0 = 0$; $S_9 = S_6 + S_5 = 1 + 0 = 1$;

$S_{10} = S_7 + S_6 = 1 + 1 = 0$, $S_{11} = S_8 + S_7 = 0 + 1 = 1$; $S_{12} = S_9 + S_8 = 1 + 0 = 1$;

$S_{13} = S_{10} + S_9 = 0 + 1 = 1$; $S_{14} = S_{11} + S_{10} = 1 + 0 = 1$; $S_{15} = S_{12} + S_{11} = 1 + 1 = 0$;

$S_{16} = S_{13} + S_{12} = 1 + 1 = 0$; $S_{17} = S_{14} + S_{13} = 1 + 1 = 0$; $S_{18} = S_{15} + S_{14} = 0 + 1 = 1$.

Выпишем полученные элементы по порядку 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1. Чтобы было проще найти повторяющиеся вектора состояний, выпишем эти вектора-состояния:

(0,0,0,1); (0,0,1,0); (0,1,0,0); (1,0,0,1); (0,0,1,1); (0,1,1,0); (1,1,0,1); (1,0,1,0); (0,1,0,1); (1,0,1,1); (0,1,1,1); (1,1,1,1); (1,1,1,0); (1,1,0,0); (1,0,0,0); **(0,0,0,1).**

Одинаковые вектора состояний мы выделили жирным шрифтом. Таким образом, у нашей последовательности длина оказалась максимально возможной, равной 15.

Пример 4. *Найти матрицу регистра сдвига над полем GF(3)*

$S_{N+4} = S_{N+1} - S_N$. *и степень, в которой она равна единичной матрице.*

Решение. Согласно теории получается матрица размера 4 на 4 над полем GF(3)

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Теперь будем возводить матрицу в степени 2, 3, …

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} = A^2,$$

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 1 \end{pmatrix} = A^3.$$

На самом деле возводить в степень придется долго. Поскольку регистр сдвига имеет порядок 4, то вектор состояний 4-х мерный.

Так как поле содержит 3 элемента, то различных векторов состояний регистра ровно $3^4 = 81$, а ненулевых 80. Значит период последовательности, порожденной регистром сдвига, может быть любым числом, не превосходящим 80.

На самом деле, он будет равен 26. Что можно проверить, вычислив произведение $A^2 \cdot A^8 \cdot A^{16} = A^{26}$.

Каким же образом выяснить до вычислений, что период равен именно 26?

Для этого используем жорданову форму. Вначале найдем характеристический многочлен матрицы

$$\begin{vmatrix} \lambda & 0 & 0 & 1 \\ -1 & \lambda & 0 & -1 \\ 0 & -1 & \lambda & 0 \\ 0 & 0 & -1 & \lambda \end{vmatrix} = \lambda^4 - \lambda + 1 .$$

Обратим внимание, что характеристический матрицы рекуррентной последовательности совпал с характеристическим многочленом самой последовательности. И это не случайно, можно показать, что это верно для любого регистра сдвига над любым полем.

Поэтому при поиске жордановой формы можно не искать характеристический многочлен матрицы, а сразу воспользоваться характеристическим многочленом самой последовательности.

Характеристический многочлен разлагается над полем GF(3) на неприводимые множители $\lambda^4 - \lambda + 1 = (\lambda + 1)(\lambda^3 - \lambda^2 + \lambda + 1)$. Пусть α - корень многочлена $\lambda^3 - \lambda^2 + \lambda + 1$в поле Галуа GF($3^3$).

Т.к. многочлен $\lambda^3 - \lambda^2 + \lambda + 1$ неприводим, то из теории известно, что кроме элемента α его корнями также будут элементы α^3, α^9.

Поскольку в поле GF(3^3) ровно 26 ненулевых элементов, то примитивный элемент этого поля имеет порядок 26. Поскольку число 3 не делит 26, то все корни $\alpha, \alpha^3, \alpha^9$ неприводимого многочлена $\lambda^3 - \lambda^2 + \lambda + 1$ имеют один и тот же порядок.

Таким образом, характеристический многочлен $\lambda^4 - \lambda + 1$ имеет 4 корня $-1, \alpha, \alpha^3, \alpha^9$ и жордановы форма нашей матрицы выглядит так

$$L = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha^3 & 0 \\ 0 & 0 & 0 & \alpha^9 \end{pmatrix}.$$

Чтобы узнать порядок матрицы осталось узнать в какой степени корень альфа равен 1.

На самом деле – это примитивный элемент поля GF(27) и его порядок равен 26. Следовательно, и $A^{26} = E$, т.е. матрица A имеет порядок 26.

Примитивность проверим средствами языка программирования Julia 1.4.1 официальный сайт https://julialang.org/.

Только вместо символа альфа, которого нет на клавиатуре, используем символ z

```
julia> using Nemo
Welcome to Nemo version 0.17.4
Nemo comes with absolutely no warranty whatsoever

julia> T, t = PolynomialRing(ResidueRing(ZZ, 3), "t")
```

```
(Univariate Polynomial Ring in t over Integers modulo 3, t)
julia> U, z = FiniteField(t^3-t^2+t + 1, "z")
(Finite field of degree 3 over F_3, z)
```

Проверим является ли z примитивным элементом, т.е. $z^2 \neq 1, z^{13} \neq 1$. Имеем

```
julia> z^2
z^2
julia> z^13
2
```

Значит z – примитивный элемент, имеет порядок 26, а вместе с ним порядок 26 и матрицы. Пример закончен.

ЛИТЕРАТУРА

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2017. - URL: https://e.lanbook.com/reader/book/111097/
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/126718/