Доп. дисциплины

Магистры весна 2021

Занятие 10

ЛИНЕЙНЫЕ РЕГИСТРЫ СДВИГА

13.05.2020

ОСНОВНЫЕ СВОЙСТВА

Определение. *Пусть* $s_0, s_1, ..., s_n, ...$ *- последовательность элементов поля P, тогда зависимость вида*

$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + ... + a_1S_{n+1} + a_0S_n + a, n = 0,1,2,...,$$

называется линейным регистром сдвига с обратной связью порядка k. Если при этом a=0, то последовательность называется однородной.

При этом первые k значений последовательности могут принимать любые значения.

Определение. *Первые k элементов последовательности S называются вектором инициализации* $\overline{s_0} = (s_0, s_1, ..., s_{k-1})$. *Вектор инициализации может быть любым.*

Определение. *Вектор инициализации называется импульсной функцией, если он имеет вид* $\overline{s_0} = (0, 0, ..., 0, 1)$.

Определение. *Характеристическим многочленом однородной линейной рекуррентной последовательности называется многочлен k-й степени*

$$x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1x + a_0.$$

ТРУДНЫЙ ПРИМЕР

Изучить регистр сдвига $S_{n+3} = 2S_{n+1} + 3S_n$ над полем GF(5).

Характеристический многочлен. Данного регистра сдвига будет многочлен 3-й степени $x^3 = 2x + 3 \Rightarrow x^3 - 2x - 3 = 0$.

Прямая проверка показывает, подстановкой элементов $\{0,1,2,3,4\}$, что в поле GF(5) многочлен корней не имеет. Поэтому его корни нужно искать в расширении поля GF(5). Т.к. многочлен $x^3 - 2x - 3$ имеет третью степень и не имеет корней, то он неприводим. Поэтому расширение, в котором он будет иметь корни, может быть построено добавлением корня этого многочлена.

Пусть a - корень многочлена $x^3 - 2x - 3$, тогда $\alpha^3 = 2\alpha + 3$ и мы получаем поле GF(5^3). Поскольку многочлен $x^3 - 2x - 3$ неприводим, а в поле GF(5) элемент 5 = 0 (характеристика поля равна 5), то, по одной из теорем о полях Галуа. Корнями многочлена, будут элементы $\alpha, \alpha^5, \alpha^{25}$. Осталось записать их в виде многочленов степени не выше второй.

Вычисления средствами языка Julia. Подключаем пакет Nemo.

```
using Nemo
R, x = FiniteField(5, 3, "x")
```

И задаем стандартное для Julia поле $GF(5^3)$:

```
julia> using Nemo
Welcome to Nemo version 0.17.5
Nemo comes with absolutely no warranty whatsoever
julia> R, x = FiniteField(5, 3, "x")
(Finite field of degree 3 over F_5, x)
julia> x^3
2*x+2
```

Следовательно, поле задано, как поле разложения многочлена $x^3 - 2x - 2 = 0$. Наш многочлен другой, поэтому зададим поле $GF(5^3)$ явным образом

```
T, t = PolynomialRing(ResidueRing(ZZ, 5), "t")
F, a = FiniteField(t^3-2*t - 3, "a")
julia> T, t = PolynomialRing(ResidueRing(ZZ, 5), "t")
(Univariate Polynomial Ring in t over Integers modulo 5, t)
julia> F, a = FiniteField(t^3-2*t - 3, "a")
(Finite field of degree 3 over F_5, a)
julia> a^5
3*a^2+4*a+1
julia> a^25
2*a^2+4
```

Итак, получили три корня (`a, 3*a^2+4*a+1, 2*a^2+4`).

Матричный вариант. 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

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

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 = 3, а регистр сдвига задан формулой

$$S_{n+3} = 2S_{n+1} + 3S_n$$

над полем Галуа GF(5) мы получаем матрицу A размера 3 на 3

$$A = \begin{pmatrix} 0 & 0 & a_0 \\ 1 & 0 & a_1 \\ 0 & 1 & a_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

Вычисляем степени матрицы A, используя язык Julia

```
using LinearAlgebra
S = MatrixSpace(GF(5),3,3)
A= [0 0 3; 1 0 2; 0 1 0]
B=S(A)
```

Максимально возможный порядок матрицы 125-1 = 124. Проверяем

```
julia> using LinearAlgebra
julia> S = MatrixSpace(GF(5),3,3)
Matrix Space of 3 rows and 3 columns over Galois field with
characteristic 5
julia> A= [0 0 3; 1 0 2; 0 1 0]
3?3 Array{Int64,2}:
 0  0  3
 1  0  2
 0  1  0
julia> B=S(A)
[0  0  3]
[1  0  2]
[0  1  0]
julia> B^62
[4  0  0]
[0  4  0]
[0  0  4]
```

Поскольку 62-я степень матрицы не равна единичной матрице, значит ее порядок равен 124. Следовательно, и период последовательности равен 124. Вручную непосредственно его найти затруднительно.

Явная формула. Напомним теорию.

В случае, когда корни $\alpha_1, \alpha_2, ..., \alpha_k$ характеристического многочлена попарно различны для n-го члена рекуррентной последовательности можно указать явный вид.

$$s_n = \beta_1 \alpha_1{}^n + \beta_2 \alpha_2{}^n + ... + \beta_k \alpha_k{}^n, n = 0, 1, 2, ...,$$

где коэффициенты $\beta_1, \beta_2, ..., \beta_k \in P$ можно определить, зная значения вектора инициализации решив систему из k линейных уравнений от k неизвестных $\beta_1, \beta_2, ..., \beta_k$:

$$\begin{cases} \beta_1 \alpha_1{}^0 + \beta_2 \alpha_2{}^0 + ... + \beta_k \alpha_k{}^0 = s_0 \\ \beta_1 \alpha_1{}^1 + \beta_2 \alpha_2{}^1 + ... + \beta_k \alpha_k{}^1 = s_1 \\ ... \\ \beta_1 \alpha_1{}^{k-1} + \beta_2 \alpha_2{}^{k-1} + ... + \beta_k \alpha_k{}^{k-1} = s_{k-1} \end{cases}$$

В нашем случае, с импульсной функцией, и ранее вычисленными корнями характеристического многочлена, $\alpha_1 = a; \alpha_2 = 3a^2 + 4a + 1; \alpha_3 = 2a^2 + 4$, получаем

$$\begin{cases} \beta_1 + \beta_2 + \beta_3 = 0 \\ \beta_1 a + \beta_2 (3a^2 + 4a + 1) + \beta_3 (2a^2 + 4) = 0 \\ \beta_1 a^2 + \beta_2 (3a^2 + 4a + 1)^2 + \beta_3 (2a^2 + 4)^2 = 1 \end{cases}$$

Вычисления произведем в Julia

```
using Nemo
using LinearAlgebra
M, x = PolynomialRing(ResidueRing(ZZ, 5), "x")
F, a = FiniteField(x^3-2*x - 3, "a")
A = [1 1 1; a 3*a^2+4*a+1 2*a^2+4; a^2 (3*a^2+4*a+1)^2 (2*a^2+4)^2]
b = [0,0,1]
```

К сожалению, простое взятие обратной матрицы A^(-1) над не простым полем Галуа к успеху не приводит, Julia выдает ошибку. Приходится проявлять “чудеса” изобретательности. А именно, грубо задать цикл по вычислению все возрастающих степеней матрицы А. Через несколько сек. получаем A^7812 = E, значит A^7811 = A^(-1).

Итак

```
julia> B=A^7811
3?3 Array{Any,2}:
 a^2+4*a+4    2*a^2+2*a+4  3*a^2+2*a+1
 2*a^2+4*a+1  a^2+4*a+2    a^2+2*a+2
 2*a^2+2*a+1  2*a^2+4*a+4  a^2+a+2
julia> b = [0,0,1]
3-element Array{Int64,1}:
 0
 0
 1
```

```
julia> B*b
3-element Array{Any,1}:
 3*a^2+2*a+1
 a^2+2*a+2
 a^2+a+2
```

Получаем явную формулу для n-го члена

$$s_n = (3a^2+2a+1)a^n + (a^2+2a+2)(3a^2+4a+1)^n + (a^2+a+2)(2a^2+4)^n .$$

Проверим правильная это формула или нет и, заодно, явно вычислим первые 130 членов нашей последовательности:

```
julia> for n in 0:129
print((3*a^2+2*a+1)*a^n+(a^2+2*a+2)*(3*a^2+4*a+1)^n+(a^2+a+2)*(2*a^2+4)^n,",")
 end
```

```
0,0,1,0,2,3,4,2,2,1,0,3,3,1,0,1,3,2,4,3,4,3,2,3,3,2,0,3,1,1,1,0,0,3,0,1,4,2,1
,1,3,0,4,4,3,0,3,4,1,2,4,2,4,1,4,4,1,0,4,3,3,3,0,0,4,0,3,2,1,3,3,4,0,2,2,4,0,
4,2,3,1,2,1,2,3,2,2,3,0,2,4,4,4,0,0,2,0,4,1,3,4,4,2,0,1,1,2,0,2,1,4,3,1,3,1,4
,1,1,4,0,1,2,2,2,       0,0,1,0,2,3
```

Видно, что длина периода последовательности равна 124.

Глядя на явную формулу хочется воскликнуть как Тарас Бульба: “Что, сынку, помогли тебе твои ляхи?”

И искать ее трудно и вычислять по исходной рекуррентной формуле намного проще, потому, что в ней все происходит в поле GF(5), а не в громоздком поле GF(125).

Такова судьба многих явных формул - они больше для теории. Важен сам факт их существования.

ПРИМЕР ДОСТУПНЫЙ РУЧНОМУ ВЫЧИСЛЕНИЮ

Изучить регистр сдвига $S_{n+2} = S_{n+1} + S_n$ над полем GF(7) с импульсной функцией (0, 1). Это ряд Фибоначчи над полем из 7 элементов.

Его характеристический многочлен имеет вид $x^2 = x+1 \Rightarrow x^2 - x - 1$.

Легко проверить, что в GF(7) многочлен корней не имеет и, значит, неприводим.

Прямое вычисление. Вычисляем первые 48 членов ряда Фибоначчи, поскольку период не больше 48:

0,1,1,2,3,5,1,6,0,6,6,5,4,2,6,1,0,1,1

Очевидно, что период равен 16 и 48 членов вычислять ни к чему.

Вычисления по явной формуле. Воспользуемся средствами языка Julia, поскольку поле разложения многочлена $x^2 - x - 1$ содержит 49 элементов. Это немного, но хлопотно.

Как следует из теории многочлен имеет 2 корня - a и a^7.

```
julia> T, t = PolynomialRing(ResidueRing(ZZ, 7), "t")
(Univariate Polynomial Ring in t over Integers modulo 7, t)
julia> F, a = FiniteField(t^2-t-1, "a")
(Finite field of degree 2 over F_7, a)
julia> a^7
6*a+1
```

Итак, корни это {a, 6*a+1}.

Явная формула в нашем случае имеет вид $s_n = \beta_1 a^n + \beta_2 (1-a)^n$, а система по поиску коэффициентов такова

$$\begin{cases} \beta_1 + \beta_2 = 0 \\ \beta_1 a + \beta_2 (1-a) = 1 \end{cases} \Rightarrow \begin{cases} \beta_2 = -\beta_1 \\ \beta_1 (2a-1) = 1 \end{cases} \Rightarrow \begin{cases} \beta_2 = a+3 \\ \beta_1 = 6a+4 \end{cases},$$

поскольку

```
julia> (2*a-1)^(-1)
6*a+4.
```

Итог. Явная формула n-го члена последовательности имеет вид

$$s_n = (6a+4)a^n + (\mathrm{a}+3)(1-a)^n.$$

Опять от этой формулы на практике мало толку, но мы вычислим, используя эту формулу, с помощью Julia

```
julia> for n in 0:18
       print((4-a)*a^n+(a+3)*(1-a)^n,",")
       end
0,1,1,2,3,5,1,6,0,6,6,5,4,2,6,1,0,1,1
```

Получилась та же последовательности, что и при прямом вычислении.

Матричный метод. Матрица последовательности имеет вид

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Так как ее характеристический многочлен совпадает с характеристическим многочленом последовательности, то ее жорданова форма имеет вид

$$J(A) = \begin{pmatrix} a & 0 \\ 0 & a^7 \end{pmatrix}$$

Ее порядок, т.е. минимальная степень, в которой она равна единичной матрице, совпадает с порядком корня “a”. Кроме того, порядки “a” и “a^7” равны, т.к. нод(7,48) = 1. Итак, осталось найти порядок корня “a”. Имеем

```
julia> a^8
6
julia> a^16
1
```

Значит порядок корня “a” равен 16, поэтому порядок жордановой формы равен 16. А т.к. $A = T^{-1}J(\mathrm{A})\mathrm{T}$ для некоторой матрицы Т (матрицы перехода к жорданову базису), то и порядок матрицы А равен 16. Следовательно, и период последовательности равен 16.

Опять тот же ответ, что и выше.

Есть способ просто возводить матрицу А во все возрастающие степени, пока не получится единичная.

```
julia> S = MatrixSpace(GF(7),2,2)
Matrix Space of 2 rows and 2 columns over Galois field with
characteristic 7
julia> A=[0 1; 1 1]
2?2 Array{Int64,2}:
 0  1
 1  1
julia> B=S(A)
[0  1]
[1  1]
julia> B^8
[6  0]
[0  6]
julia> B^16
[1  0]
[0  1]
```

Опять период равен 16.

Самым простым оказался первый способ – прямое вычисление. Но это только потому, что число p=7 маленькое. Если бы p было 150-значное, как это принято в криптографии, первый способ, даже на самом мощном в мире суперкомпьютере был бы не осуществим.

Нужны были бы триллионы триллионов гигатонн бумаги, чтобы распечатать эту последовательность. Даже шрифтом 1 микрон и на бумаге тоньше человеческого волоса в миллион раз.

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/