7 Минимальный многочлен ЛРП. Алгоритм Берлекэмпа–Месси

7.1 Минимальный многочлен и линейная сложность ЛРП

ЛРП из элементов поля P, заданная некоторым рекуррентным соотношением, может удовлетворять и многим другим рекуррентным соотношениям. Так если t есть период ЛРП $< u >= u_0, u_1, \ldots$, то выполняются рекуррентные соотношения $u_{n+t} = u_n,\ n = 0, 1, \ldots$, $u_{n+2t} = u_n,\ n = 0, 1, \ldots$ и т.д. Подобные соотношения связаны между собой, как это определяет следующая теорема.

Теорема 7.1 *Пусть* $< u >= u_0, u_1, \ldots$ *– ЛРП над полем* P*. Тогда существует однозначно определяемый нормированный многочлен* $m(x)$ *над полем* P *такой, что любой нормированный многочлен* $f(x)$ *положительной степени над* P *является характеристическим многочленом этой последовательности* $< u >$ *тогда и только тогда, когда* $f(x)$ *делится на* $m(x)$.

Определяемый этой теоремой многочлен $m(x)$ является, очевидно характеристическим многочленом ЛРП $< u >$, имеющим наименьшую степень, он называется *минимальным* многочленом ЛРП, степень минимального многочлена определяет *линейную сложность* ЛРП.

Линейной сложностью $L(u^n)$ конечной последовательности $< u^n >= u_0, u_1, \ldots, u_{n-1}$ называется сложность бесконечной ЛРП

$$< u >= u_0, u_1, \ldots u_{n-1}, u_n \ldots,$$

имеющей минимальную линейную сложность.

Профилем линейной сложности ЛРП $< u >$ (или конечной последовательности $< u^n >$) называется последовательность

$$L(u^1), L(u^2), \ldots$$

линейных сложностей конечных подпоследовательностей

$$< u^1 >= u_0,\ < u^2 >= u_0, u_2,\ \ldots$$

(или последовательность $L(u^1), \ldots L(u^n)$).

Профиль линейной сложности обладает следующими свойствами

1. $i > j \to L(u^i) \geq L(u^j)$,
2. $L(u^{N+j}) > L(u^N)$ возможно только при $L^N \leq N/2$.
3. $L(u^{N+1}) > L(u^N) \to L(u^{N+1}) + L(u^N) = N + 1$.

Пример 7.1. Профиль линейной сложности периодической последовательности с циклом

$$1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0$$

следующий:

$1, 1, 1, 3, 3, 3, 3, 5, 5, 5, 6, 6, 6, 8, 8, 8, 9, 9, 10, 10, 11, 11, 11, 11, 14, 14, 14, 14, 15, 15, 15, 17,$
$17, 17, 18, 18, 19, 19, 19, 19, \ldots$

Близость профиля линейной сложности последовательности $< u >$ профилю линейной сложности случайной последовательности является необходимым, но недостаточным условием случайности последовательности $< u >$,

Пример 7.2. Профиль линейной сложности последовательности $< u >$, в которой

$$u_i = \begin{cases} 1, & \text{если } i = 2^j - 1 \text{ при некотором } j \geq 0, \\ 0 & \text{в остальных случаях,} \end{cases}$$

максимально примыкает к линии $L = N/2 : \forall N \geq 1\ L(u^N) = \lfloor (N+1)/2 \rfloor$.
Однако ясно, что последовательность $< u >$ не является случайной.

7.2 Алгебра степенных рядов

Произвольной последовательности $u_0, u_1, \ldots, u_n, \ldots$ из элементов поля P свяжем формальный степенной ряд от формальной переменной x.

$$G(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_n x^n + \cdots = \sum_{n=0}^{\infty} u_n x^n. \quad (7.1)$$

Степенной ряд последовательности иногда называют производящей функцией этой последовательности. Однако в данном случае ни область определения, на область значений "функции"не могут быть указаны. Рассматриваемая конструкция является лишь формальным символом, отражающим линейный порядок элементов последовательности. Элементы последовательности выступают в качестве коэффициентов формального степенного ряда.

Два формальных степенных ряда

$$B(x) = \sum_{n=0}^{\infty} b_n x^n \ \text{ и } C(x) = \sum_{n=0}^{\infty} c_n x^n$$

считаются равными, если $b_n = c_n,\ n = 0, 1, \ldots$.

Использование формальных степенных рядов позволяет рассматривать многочлен над полем P

$$p(x) = p_0 + p_1 x + \cdots + p_k x^k$$

также как формальный степенной ряд

$$p(x) = p_0 + p_1 x + \cdots + p_k x^k + 0 \cdot x^{k+1} + 0 \cdot x^{k+2} + \cdots.$$

На множестве степенных рядов определяют операции сложения и умножения по правилам, аналогичным правилам сложения и умножения многочленов:

$$B(x) + C(x) = \sum_{n=0}^{\infty} (b_n + c_n) x^n,$$

$$B(x)C(x) = \sum_{n=0}^{\infty} (d_n) x^n, \quad \text{где } d_n = \sum_{k=0}^{n} b_k c_{n-k},\ n = 0, 1, \ldots.$$

Если $B(x)$ и $C(x)$ – многочлены, то эти операции имеют обычный смысл сложения и умножения многочленов. В то же время, как видно, можно складывать и перемножать обычные многочлены и формальные степенные ряды смешанным образом (один операнд – многочлен, а другой – формальный степенной ряд).

Множество формальных степенных рядов с двумя рассмотренными операциями образует кольцо. Аддитивной единицей кольца является формальный ряд, соответствующий последовательности

$$< 0 >= 0, 0, \ldots$$

из аддитивных единиц 0 поля P, а мультипликативной единицей – формальный ряд, соответствующий последовательности

$$< 1 >= 1, 0, 0 \ldots,$$

начинающейся мультипликативной единицей 1 поля P и продолжающийся аддитивными единицами этого поля.

Теорема 7.2 *Формальный степенной ряд*

$$B(x) = \sum_{n=0}^{\infty} b_n x^n$$

имеет обратный относительно операции умножения элемент $B(x)^{-1}$ *тогда и только тогда, когда* $b_0 \neq 0$.

Доказательство. Пусть $C(x) = B(x)^{-1}$, то есть

$$B(x)C(x) =< 1 > .$$

в кольце степенных рядов. Тогда коэффициенты $c_0, c_1, \ldots,$ $b_0, b_1, \ldots$ степенных рядов $C(x)$ и $B(x)$ удовлетворяют соотношениям

$$\begin{aligned} &d_0 = b_0 c_0 = 1, \\ &d_1 = b_0 c_1 + b_1 c_0 = 0. \\ &\ldots \\ &d_n = b_0 + c_n + b_1 c_{n-1} + \ldots + b_n c_0 = 0. \ldots \end{aligned}$$

Из первого соотношения следует, что $b_0 \neq 0$, и c_0 однозначно определяется как b_0^{-1} в поле P. Остальные коэффициенты $c_i,\ i = 1, 2, \ldots$ при этом определяются однозначно по рекурсивной схеме.

Если $B(x)$ имеет обратный элемент, то можно определить операцию деления $\frac{A(x)}{B(x)} = A(x)B(x)^{-1}$. Формально результат можно получить делением "углом."

Пусть $u_0, u_1, \ldots$ линейная последовательность k-го порядка над полем P, удовлетворяющая рекуррентному соотношению

$$u_{n+k} = a_{k-1}u_{n+k-1} + a_{k-2}u_{n+k-2} + \cdots + a_0 u_n,\ n = 0, 1, \ldots.$$

Многочлен

$$f^*(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \cdots - a_0x^k$$

над полем P называется *возвратным, или двойственным многочленом* этой последовательности. Характеристический многочлен

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0$$

и возвратный характеристический многочлен последовательности порядка k связаны соотношением

$$f^*(x) = x^k f(x^{-1}).$$

Отсюда

$$f(x) = x^k f^*(x^{-1}).$$

7.3 Алгоритм Берлекэмпа–Месси

Коэффициенты минимального многочлена линейной рекуррентной последовательности порядка k при заданном ее отрезке из $2k$ элементов можно найти как решение матричного уравнения

$$\mathbf{u_n}A^k = \mathbf{u_{n+k}},$$

с неизвестными элементами $a_0, a_1, ..., a_{k-1}$ матрицы A. Сложность алгоритма решения может быть резко понижена,если учесть особенности строения матрицы A, что и предусматривается алгоритмом Берлекэмпа – Месси.

Пусть задан отрезок ЛРП с неизвестным минимальным многочленом степени не более k, содержащий не менее $2k$ элементов. Приведём одну из модификаций алгоритма Берлекэмпа-Месси построения минимального многочлена $m(x)$

Пусть $u_0, u_1, \ldots$ – последовательность над конечным полем P и $G(x) = \sum_{n=0}^{\infty} u_n x^n$ – представляющий эту последовательность формальный степенной ряд. Для $j = 0, 1, \ldots$ определим многочлены $g_j,\ h_j$ над полем P, целые числа m_j и элементы b_j из поля P следующим образом.

Положим

$$g_0(x) = 1,\ h_0(x) = x,\ m_0 = 0,\ b_0 = u_0.$$

Далее для $j = (0, 2k-1)$ выполнить

$$1.g_{j+1}(x) = g_j(x) - b_j h_i(x);$$

$$2.h_{j+1}(x) = \begin{cases} b_j^{-1}xg_j(x), & \text{если } b_j \neq 0,\ m_j \geq 0, \\ xh_j(x) & \text{в противном случае;} \end{cases}$$

$$3.m_{j+1} = \begin{cases} -m_j, & \text{если } b_j \neq 0,\ m_j \geq 0, \\ m_j + 1 & \text{в противном случае;} \end{cases}$$

4. Присвоить b_{j+1} значение коэффициента при x^{j+1} формального ряда $g_{j+1}(x)G(x)$.

Замечание. Поскольку в вычислениях используются только первые $2k$ членов последовательности, то вместо формального ряда $G(x)$ можно использовать многочлен

$$G_{2k-1}(x) = \sum_{n=0}^{2k-1} u_n x^n.$$

Если $u_0, u_1, \ldots$ – ЛРП с минимальным многочленом степени k, то после выполнения указанных действий получим многочлен $g_{2k}(x)$, равный возвратному минимальному многочлену. Искомый минимальный многочлен в этом случае может быть получен как

$$m(x) = g_0^{-1} x^k g_{2k}(1/x),$$

где g_0 свободный член многочлена $g_{2k}(x)$. Если же заранее известно лишь, что $\deg m(x) \leq k$, то минимальный многочлен определяется равенством

$$m(x) = x^r g_0^{-1} g_{2k}(1/x),$$

где $r = \lfloor k + 1/2 - m_{2k}/2 \rfloor$.

Пример 7.3. Пусть 8 членов ЛРП над полем $GF(3)$ порядка $k \leq 4$ образуют её начальный отрезок

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

тогда

$$G_7(x) = 2x + x^2 + x^4 + 2x^5 + x^6.$$

Работа алгоритма представлена в следующей таблице

j	$g_j(x)$	$h_j(x)$	m_j	b_j
0	1	x	0	0
1	1	x^2	1	2
2	$1 + x^2$	$2x$	-1	1
3	$1 + x + x^2$	$2x^2$	0	0
4	$1 + x + x^2$	$2x^3$	1	2
5	$1 + x + x^2 + 2x^3$	$2x + 2x^2 + 2x^3$	-1	2
6	$1 + x^3$	$2x^2 + 2x^3 + 2x^4$	0	1
7	$1 + x^2 + 2x^3 + x^4$	$x + x^4$	0	1
0	$1 + 2x + x^2 + 2x^3$		0	

В данном случае $r = \lfloor 4 + 1/2 - m_8/4 \rfloor = 4$. Поэтому

$$m(x) = x^4 + 2x^3 + x^2 + 2x.$$

Рекуррентное соотношение наименьшего порядка, которому удовлетворяет данная последовательность, имеет вид

$$u_{n+4} = u_{n+3} + 2u_{n+2} + u_{n+1}.\ n = 0, 1, \ldots.$$

Что касается многочлена $g_{2k} = 1+2x+x^2+2x^3$, то он является минимальным многочленом последовательности с начальным состоянием

$$0, 1, 2, 1, 0, 1, 2.$$

Это записанные в обратном порядке семь заключительных элементов начального отрезка исходной последовательности. Эта "возвратная"последовательность удовлетворяет рекуррентному соотношению

$$u_(n+3) = u_{n+2} + 2u_{n+1} + u_2.$$

Пример 7.4. Пусть первые 8 членов ЛРП над полем $GF(2)$ следующие:

$$1, 1, 0, 0, 1, 0, 1, 1.$$

Используем многочлен $G_7(x) = 1 + x + x^4 + x^6 + x^7$ над полем $GF(2)$ вместо формального степенного ряда $G(x)$ последовательности. Применим алгоритм Берлекэмпа–Мэсси, чтобы найти ЛРП наименьшего порядка, с указанными первыми элементами. Работу алгоритма представим в таблице:

j	$g_j(x)$	$h_j(x)$	m_j	b_j
0	1	x	0	1
1	$1+x$	x	0	0
2	$1+x$	x^2	1	1
3	$1+x+x^2$	$x+x^2$	-1	1
4	1	x^2+x^3	0	1
5	$1+x^2+x^3$	x	0	0
6	$1+x^2+x^3$	x^2	1	0
7	$1+x^2+x^3$	x^3	2	0
0	$1+x^2+x^3$		3	

В этом примере $r = \lfloor 4 + 1/2 - m_8/2 \rfloor = 3$ и, следовательно,

$$m(x) = x^3(1 + (1/x)^2 + (1/x)^3) = x^3 + x + 1.$$

Таким образом, заданные элементы образуют начальный отрезок ЛРП, удовлетворяющей рекуррентному соотношению

$$u_{n+3} = u_{n+1} + u_n, n = 0, 1, \ldots,$$

и не существует ЛРП меньшего порядка, имеющей тот же начальный отрезок.

Пример 7.5. Построим ЛРП над полем $GF(2)$ наименьшего порядка, не превышающего 5, первые 10 членов которой образуют отрезок

$$0, 0, 1, 1, 0, 1, 1, 1, 0, 1.$$

Используем многочлен

$$G_{10} = x^2 + x^3 + x^5 + x^6 + x^7 + x^9,$$

представляющий указанный отрезок. Работа алгоритма Берлекэмпа-Месси представлена в таблице

j	$g_j(x)$	$h_j(x)$	m_j	b_j
0	1	x	0	0
1	1	x^2	1	0
2	1	x^3	2	1
3	$1+x^3$	x	-2	1
4	$1+x+x^3$	x^2	-1	1
5	$1+x+x^2+x^3$	x^3	0	1
6	$1+x+x^2$	$x+x^2+x^3+x^4$	0	0
7	$1+x+x^2$	$x^2+x^3+x^4+x^5$	1	1
0	$1+x+x^3+x^4+x^5$	$x+x^2+x^3$	0	1
9	$1+x^2+x^4+x^5$	$x^2+x^3+x^4$	0	1
10	$1+x^3+x^5$	$x+x^3+x^5+x^6$	0	0

В данном случае $r = \lfloor 5 + 1/2 + m_{10}/2 \rfloor = \lfloor 5 + 1/2 + 0 \rfloor = 5$. Следовательно,

$$m(x) = x^5(1 + (x^{-1})^3 + (x^{-1})^5) = x^5 + x^2 + 1.$$

Указанный отрезок является начальным отрезком ЛРП, определяемой рекуррентным соотношением

$$u_{n+5} = u_{n+2} + u_n.$$

Литература

1.Р.Лидл, Г.Нидеррайтер. Конечные поля. Том 2. М.: Мир, 1988.

2. А.П.Алфёров, А.Ю.Зубоа, А.С.Кузимин, А.В.Черёмушкин. Основы криптографии. М.:Гелиос АРВ. 2001.

3. Menezes A.J., van Oorschoft, Vanstone S.A. handbook of Applied Cryptography. – CRC Press, Boca Raton, New York, London, Tokio, 1997.