6 Линейные рекуррентные последовательности (ЛРП)

6.1 ЛРП и ее характеристический многочлен

Будем рассматривать бесконечные последовательности над простым конечным полем F_p

$$< u >= u_0, u_1, \ldots, u_n, \ldots,$$

то есть функции $u : N_0 \to F_p$ на множестве N_0 целых неотрицательных чисел, принимающие значения в поле F_p.

Последовательность $< u >$ называется *линейной рекуррентной последовательностью* (ЛРП) *порядка k над полем F_p*, если существуют константы $a_0, \ldots, a_{k-1} \in F_p$ такие, что

$$u_{n+k} = \sum_{j=0}^{k-1} a_j \cdot u_{n+j} + a, \; n \geq 0. \qquad (6.1)$$

Замечание. Ниже будем изучать только *однородные* ЛРП, определяемые рекуррентным соотношением вида

$$u_{n+k} = \sum_{j=0}^{k-1} a_j \cdot u_{n+j}, \; n \geq 0,$$

то есть соотношением (6.1), в котором свободный член $a = 0$.

Это равенство, выражающее зависимость между членами последовательности, называется *законом рекурсии,* а определяющий этот закон многочлен

$$f(x) = x^k - \sum_{j=0}^{k-1} a_j \cdot x^j \qquad (6.2)$$

называется *характеристическим многочленом* ЛРП. Вектор

$$\mathbf{u}_0 = (u_0, \ldots, u_{k-1})$$

называется *начальным вектором* ЛРП.

Периодом ЛРП $< u >$ называется наименьшее натуральное число t такое, что при некотором неотрицательном числе η для всех $i \geq 0$ выполняется равенство

$$u_{\eta+i+t} = u_{\eta+i}.$$

Если η может быть равно 0, то последовательность называется *строго периодической.* Последовательность строго периодическая тогда и только тогда, когда коэффициент a_0 ее характеристического многочлена не равен 0. В этом случае многочлен называется несингулярным. (Если $a_0 = 0$, то характеристический многочлен называется *сингулярным*).

6.2 Автоматная интерпретация ЛРП. Линейные регистры сдвига (ЛРС)

Линейные рекуррентные последовательность удобно изучать (и практически использовать) как последовательности выходных сигналов *линейных регстров сдвига* (ЛРС).

ЛРС, формирующий ЛРП порядка k над полем F_p представляется как автономный структурный автомат

$$V = (\emptyset, F_p^k, F_p, \varphi, \psi),$$

представляемый функциональной схемой с памятью. Функциональная схема содержит k элементов задержки

$$g_0,\ g_1,\ \dots,\ g_{k-1},$$

с начальными состояниями

$$\mathbf{q(0)} = (q_0(0) = u_0,\ q_1(0) = u_1,\ \dots,\ q_{k-1}(0) = u_{k-1}).$$

Функционирование автомата описывается следующей канонической системой:

$$q_{k-1}(t+1) = \sum_{i=0}^{k-1} a_i \cdot q_i(t),$$
$$q_i(t+1) = q_{i+1}(t),\ i = (0, k-2),$$
$$y(t) = q_0(t).$$

Нетрудно видеть, что последовательность $< y >$ выходных сигналов такого автомата в точности совпадает с ЛРП $< u >$ с начальным вектором, совпадающим с вектором начальных состояний автомата, то есть ЛРС. Из автоматной интерпретации ЛРП порядка k следует, что ее период не превышает $p^k - 1$, где p – порядок поля P. Действительно, автомат имеет $p^k - 1$ ненулевых состояний и в процессе функционирования через не более чем $p^k - 1$ моментов времени автомат перейдет в одно из состояний, в котором он уже находился.

Если при этом окажется, что период равен $p^k - 1$, то ЛРП порядка k называется *последовательностью максимального периода*, или просто *максимальной* ЛРП.

Автоматная интерпретация подсказывает понятие *состояния ЛРП* как вектора $\mathbf{u}_n = (u_n, u_{n+1}, \dots, n_{n+k-1})$, определяющего состояние $\mathbf{q(n)}$ структурного автомата в момент n дискретного времени. При этом начальный вектор $\mathbf{u}_0 = (u_0, \dots u_{k-1})$ (он же вектор начального состояния $\mathbf{q(0)}$ конечного автомата) ЛРП рассматривается как ее начальное состояние.

Нетрудно видеть, что векторы $\mathbf{u}_{n+1}$ и$\mathbf{u}_n$ соседних состояний ЛРП как векторы соседних состояний конечного автомата удовлетворяют матричному уравнению

$$\mathbf{u}_{n+1} = \mathbf{u}_n A,$$

где A есть матрица над полем F_p размера $k \times k$ следующего вида

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

Лемма 6.1. *Для векторов состояний* $\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_n, \dots$ *ЛРП справедливо равенство*

$$\mathbf{u}_n = \mathbf{u}_0 A^n, \ n = 0, 1, \dots \ .$$

Если характеристический многочлен несингулярный, то матрица A обратима. Можно показать, что обратной матрицей является матрица

$$A^{-1} = \begin{pmatrix} a^*_{k-1} & 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ a^*_{k-2} & 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ a^*_2 & 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ a^*_1 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ a^*_0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

Здесь a^*_i – коэффициенты *возвратного* многочлена

$$f^*(X) = X^n \times a_0^{-1} \times f(\frac{1}{X}).$$

Пример 6.1. Возьмем многочлен $f(X) = X^3 + X + 1$ над полем F_2, тогда $f^*(X) = X^3 + X^2 + 1$. Матрицы A и A^{-1} имеют вид

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Все обратимые матрицы размере $k \times k$ над полем F_p образуют *общую линейную группу* $GL(k, F_p)$.

Теорема 6.1 *Период ЛРП делит порядок матрицы* A, *рассматриваемой как элемент группы* $GL(k, F_p)$.

По лемме 6.1 начальное состояние $\mathbf{u}_0$ ЛРП можно вычислить, если известно состояние $\mathbf{u}_n$:

$$\mathbf{u}_0 = \mathbf{u}_n (A^n)^{-1}.$$

6.3 Статистические свойства ЛРП

Важным свойством ЛРП максимального периода является то, что мультиграммы на ее периоде распределены почти равномерно.

Теорема 6.2 *Пусть* $< u >$ *– ЛРП максимального периода* $2^k - 1$ *над полем* F_p *и* $\nu(s_1 s_2 \dots s_m)$ *– число появлений мультиграммы*

$$s_1 s_2 \dots s_m$$

на периоде последовательности $< u >$. *Тогда любая ненулевая мультиграмма*

$$s_1 s_2 \dots s_m, \ m = 1, 2, \dots, k,$$

встречается на периоде ЛРП $< u >$ *ровно*

$$T_{1m} = \nu(s_1 s_2 \dots s_m) = p^{k-m}$$

раз. Число T_{0m} *появлений нулевой мультиграммы длины* m – *на единицу меньше.*

Доказательство. Пусть $i = k - m, \ i = 0, 1, 2, \dots k - 1$ то есть $m = k - i$. При $i = 0$ $T_{1m} = T_{1k} = 1 = p^i = 1, \ T_{0m} = T_{0k} = 0$ (период ненулевой рекуррентной последовательности не содержит нулевой мультиграммы длины k, а каждая ненулевая мультиграмма длины k имеется в периоде в одном экземпляре). Предположим, что каждая ненулевая мультиграмма

$$s_1 s_2 \dots s_m$$

входит в период последовательности $p^{k-m} = p^i$ раз, а нулевая мультиграмма длины m входит в период $p^i - 1$ раз. Тогда каждая ненулевая мультиграмма

$$s_1 s_2 \dots s_{m-1}$$

является начальным отрезком p мультиграмм длины m, причем начальные отрезки конкретных присутствующих в последовательности экземпляров мультиграмм длины m не совмещаются. Таким образом, число вхождений ненулевых мультиграмм длины $m-1$ в p раз больше числа вхождений ненулевых мультиграмм длины m :

$$\nu(s_1 s_2 \dots s_{m-1}) = \nu(s_1 s_2 \dots s_m) \cdot p = p^i \cdot p = p^{i+1} = p^{k-m+1}.$$

С другой стороны, нулевая мультиграмма длины $m-1$ может быть начальным отрезком ненулевой мультиграммы длины m с единственным ненулевым элементом $s_m \in \{1, 2, \dots p-1\}$ или начальным отрезком нулевой мультиграммы длины m. Число вхождений каждой ненулевой мультграммы длины m указанного вида, по предположению, есть p^i, а число вхождений нулевой мультиграммы есть $p^i - 1$. Подсчитаем число вхождений нулевой мультиграммы длины $m-1$:

$$\nu(s_1 \dots s_{m-1}) = \nu(0 \dots 0) = (p-1)p^i + p^i - 1 = p^{i+1} - 1 = p^{k-m+1} - 1.$$

Теоремы доказана, таким образом, индукцией по i.

7 Формула общего члена ЛРП

7.1 След элемента конечного поля

Пусть $P = F_p$ – простое поле, $K = F_{p^k}$ – его расширение степени k, порожденное присоединением корня $\alpha \in K$ некоторого неприводимого многочлена $f(X)$ над F_p. значение функции *след* $tr(a)$ элемента a, $a \in K$ из поля K в поле P определяется равенством

$$tr(a) = a + a^p + a^{p^2} + \ldots + a^{p^{k-1}}.$$

Пример 7.1. Пусть $P = F = GF(2),\ K = GF(2^2), f(X) = 1 + X + X^2$. Тогда

$$tr(0) = 0.$$

$$tr_K(1) = 1 + 1 = 0,$$
$$tr(a) = \alpha + \alpha^2 = 1,$$
$$tr(1 + \alpha) = (1 + \alpha) + (1 + \alpha)^2 = 1.$$

Каждый элемент x поля K является корнем единственного неприводимого многочлена $\varphi(X)$ степени $d, d|k$ – так называемого минимального многочлена элемента x. Корнями многочлена $\varphi(X)$ являются элементы

$$x, x^p, x^{p^2}, \ldots, x^{p^{d-1}}.$$

Многочлен $g(X) = \varphi(X)^{k/d}$ называется *характеристическим* многочленом элемента x.

Корнями многочлена $g(X)$ в поле K, порожденном неприводимым многочленом $\varphi(X)$ являются те же элементы, взятые с кратностью k/d.

Отсюда

$$g(X) = X^k + a_{k-1}X^{k-1} + \ldots + a_1X_1 + a_0 =$$
$$= ((X - x)(X - x^p) \ldots (X - x^{p^{d-1}}))^{k/d} =$$
$$= (X - x)^{k/d}(X - x^p)^{k/d} \ldots (X - x^{p^{d-1}})^{k/d}.$$

Рассматривая эти вычисления в поле, порожденном многочленом $f(X)$ и сравнивая коэффициенты, получаем, что что $tr(x) = a_{k-1}$, то есть след $tr(x)$ всегда является элементом поля P.

Свойства операций конечного поля влекут следующие свойства функции след:

$$tr(a \cdot x + b \cdot y) = a \cdot tr(x) + b \cdot tr(y),\ a, b \in P;$$

$$tr(x) = tr(x^p) = (tr(x))^p.$$

7.2 Формула общего члена ЛРП

Выведем формулу общего члена ЛРП, заданной характеристическим многочленом $f(x)$ степени k. Пусть K – порождаемое корнем этого многочлена расширение степени k простого поля $P = F_p$.

Лемма 7.1. *Для любого ненулевого $\alpha \in K$ и любого $b \in P$ число N_b решений уравнения $tr(\alpha \cdot x) = b$ равно p^{k-1}.*

Доказательство: $N_b \leq p^{k-1}$, т.к. p^{k-1} – степень уравнения. Но $\sum_{b \in P} N_b = p^k$, так как при любом x $tr(\alpha \cdot x) \in P$. Отсюда $N_b = p^{k-1}$.

Лемма 7.2. *Для ЛРП $< u >$, определяемой примитивным характеристическим многочленом*

$$f(X) = X^k - \sum_{j=0}^{k-1} a_j \cdot X^j \qquad (7.1)$$

с корнем λ в поле K существует единственная константа $\alpha \in K$ такая, что

$$u_n = tr(\alpha \cdot \lambda^n), \; n \geq 0. \qquad (7.2)$$

Доказательство. Прежде всего заметим, что эта последовательность является линейной рекуррентной последовательностью

$$u_{n+k} = \sum_{j=0}^{k-1} a_j \cdot u_{n+j}, \; n \geq 0,$$

определяемой указанным характеристическим многочленом:

$$\sum_{j=0}^{k-1} a_j \cdot u_{n+j} = \sum_{j=0}^{k-1} a_j \cdot tr(\alpha \cdot \lambda^{n+j}) = tr\left(\alpha \cdot \lambda^n \cdot \sum_{j=0}^{k-1} a_j \cdot \lambda^j\right) =$$
$$tr(\alpha \cdot \lambda^n \cdot \lambda^k) = tr(\alpha \cdot \lambda^{n+k}) = u_{n+k}).$$

Здесь $\sum_{j=0}^{k-1} a_j \cdot \lambda^j = \lambda^k$, так как λ есть корень многочлена (7.1).

Далее покажем, что различным константам соответствуют разные последовательности.

Заметим, что векторы

$$\mathbf{u}_{\lambda^0} = (tr(1\lambda^0), tr(1\lambda^1), \ldots, tr(1\lambda^{k-1})),$$
$$\mathbf{u}_{\lambda^1} = (tr(\lambda\lambda^0), tr(\lambda\lambda^1), \ldots, tr(\lambda\lambda^{k-1})),$$
$$\ldots$$
$$\mathbf{u}_{\lambda^{k-1}} = (tr((\lambda^{k-1}\lambda^0), tr(\lambda^{k-1}\lambda^1), \ldots, tr(\lambda^{k-1}\lambda^{k-1})),$$

определяют начальные состояния

$$\mathbf{u}_{\lambda^0}, \mathbf{u}_{\lambda^1}, \ldots \mathbf{u}_{\lambda^{k-1}}$$

последовательностей, соответствующих линейно независимым значениям

$$1, \lambda, \ldots, \lambda^{k-1} \qquad (7.3)$$

константы α.

Множество этих начальных состояний также линейно независимо. Допустим, что это не так, тогда покажем, что линейно зависимо множество констант (7.3), составляющих полиномиальный базис поля K.

Допустим, что некоторая линейная комбинация указанных начальных состояний равна нулю:

$$c_0\mathbf{u}_1 + c_1\mathbf{u}_\lambda + \ldots + c_{k-1}\mathbf{u}_{\lambda^{k-1}} = 0.$$

Тогда линейной комбинации базисных констант

$$\beta = c_0 + c_1\lambda + \cdots + c_{k-1}\lambda^{k-1}$$

соответствует нулевое начальное состояние последовательности и, следовательно, нулевая последовательность:

$$tr(\beta \cdot \lambda^i) = tr((c_0 + c_1\lambda + \cdots + c_{k-1}\lambda^{k-1}) \cdot \lambda^i) = 0, i = 0, 1, \ldots.$$

Если λ есть корень примитивного, многочлена, то уравнение

$$tr(\beta \cdot x) = 0, \quad (7.4)$$

удовлетворяется при любом x, то есть имеет $p^k > p^{k-1}$ корней (0 и $p^k - 1$ степеней корня λ), что при

$$((c_0 + a_1\lambda + \cdots + c_{k-1}\lambda^{k-1}) \neq 0$$

противоречит лемме 7.2.

Таким образом, имеется взаимно однозначное соответствие между множеством возможных значений констант α и начальных состояний последовательностей.

Теорема 7.1 *Для ЛРП $< u >$, определяемой неприводимым характеристическим многочленом* (7.1) *с корнем λ в поле K существует единственная константа $\alpha \in K$ такая, что*

$$u_n = tr(\alpha \cdot \lambda^n), \ n \geq 0. \qquad (7.5)$$

Если λ есть корень примитивного многочлена, то теорема верна в силу только что доказанной леммы.

Если λ есть корень многочлена, не являющегося примитивным, он является степенью некоторого примитивного элемента и мы можем представим его через примитивный элемент θ поля K :

$$\lambda = \theta^m.$$

Формула общего члена рекуррентной последовательности, порождаемой примитивным характеристическим многочленом с корнем θ позволяет получить

Таблица 1:

i	θ^i	$tr(\theta^i \cdot \theta^j) = \theta^{i+j}, j = 0, \dots 63)$
0	100000	000001000011000101001111010001110010010110111011001101010111111
1	010000	000010000110001010011110100011100100101101110110011010101111110
2	001000	000100001100010100111101000111001001011011101100110101011111100
3	000100	001000011000101001111010001110010010110111011001101010111111000
4	000010	010000110001010011110100011100100101101110110011010101111110000
5	000001	100001100010100111101000111001001011011101100110101011111100000

Таблица 2:

i	θ^i	$tr(\theta^i \cdot \lambda^j) = tr(\theta^i \cdot \theta^{3j}) = tr(\theta^{i+3j}), j = 0 \dots 21)$
0	100000	000001010010011001011
1	010000	000100011011111100111
2	001000	010101110100001111011
3	0001000	000010100100110010110
4	000010	001000110111111001110
5	000001	101011101000011110110

формулу общего члена последовательности, порождаемой неприводимым характеристическим многочленом с корнем λ : Пусть $< u >$ – последовательность, порождаемая корнем θ примитивного многочлена, а $< \tilde{u} >$ – последовательность, порождаемая корнем $\lambda = \theta^m$ некоторого неприводимого многочлена той же степени. Тогда

$$\tilde{u}_s = u_{ms} = tr(a \cdot \theta^{ms}) = tr(a \cdot \lambda^s),$$

при некоторой однозначно определяемой константе

$$a = \sum_{i=0}^{k-1} a_i \theta^i.$$

Как видим, и в этом случае формула общего члена верна. При этом в ней присутствует константа из формулы для последовательности, порождаемой корнем примитивного многочлена, степенью корня θ которого является используемый в ней корень λ.

Пример 7.2. Пусть θ есть корень примитивного многочлена $1 + x + x^6$, а $\lambda = \theta^3$ - корень неприводимого многочлена $1 + x + x^2 + x^4 + x^6$.

Соответствие базовых констант и порождаемых ими последовательностей представлено в Табл. 1,2.

Пример 7.3. Пусть $k = 2$, λ – корень многочлена $X^2 + X + 1$ над полем $GF(2)$. Константам 1 и λ соответствуют базисные начальные состояния

$$\mathbf{u}_1 = (tr(1\lambda^0), tr(1\lambda^1) = (tr(1), tr(\lambda)) = (1 + 1, \lambda + \lambda^2) = (0, 1);$$

$$\mathbf{u}_\lambda = (tr(\lambda)\lambda^0), tr(\lambda\lambda^1) = (tr(\lambda), tr(\lambda^2)) = (1,1),$$

Отсюда получаем, что константам (0,0) и (1,1) соответствуют начальные состояния

$$\mathbf{u}_0 = (0,0) \text{ rm и } \mathbf{u}_1 = (1,0).$$

Упражнение. Сформулируйте алгоритм вычисления начального вектора ЛРП, определяемой известным неприводимым многочленом, по ее отрезку из k элементов.

Указание. Сначала следует найти элемент

$$\alpha = \alpha_0 + \alpha_1\lambda + \cdots + \alpha_{k-1}\lambda^{k-1},$$

упоминаемый в формулировке теоремы. Для этого с использованием заданных k элементов $u_n, u_{n+1}, \ldots, u_{n+k-1}$ составить и решить систему из k линейных относительно коэффициентов этого элемента уравнений

$$u_{n+j} = tr\left((\alpha_0 + \alpha_1\lambda + \cdots + \alpha_{k-1}\lambda^{k-1})\lambda^{n+j}\right),\ j = 0, 1 \ldots, k-1.$$

После того, как элемент α найден, k начальных элементов последовательности вычисляются по формуле

$$u_j = tr(\alpha_0 + \alpha_1\lambda + \cdots + \alpha_{k-1}\lambda^{k-1})\lambda^j,\ j = 0, 1 \ldots, k-1.$$

Пример 7.4. Пусть $k = 2$, λ есть корень многочлена $X^2 + X + 1$. Даны элементы $u_2 = 0$, $u_3 = 1$ последовательности

$$< u >= u_0, u_1, u_2, u_3, \ldots,$$

характеристическим многочленом которой является $X^2 + X + 1$.

Составим два уравнения

$$u_2 = tr((\alpha_0 + \alpha_1\lambda)\lambda^2) = tr(\alpha_0\lambda^2 + \alpha_1 tr(\lambda^3)) =$$

$$= tr(a_0 + a_0\lambda + a_1) = a_0 + a_0^2 + a_0 + a_0\lambda + a_1 + a_1^2 = a_0 + a_0\lambda = 0 \to a_0 = 0,$$

$$u_3 = tr((\alpha_0 + \alpha_1\lambda)\lambda^3) = \alpha_0 + \alpha_1 tr(\lambda^4) = \alpha_0 + \alpha_1 tr(\lambda) = \alpha_0 + \alpha_1 \cdot 1 = 1.$$

Из этих уравнений получим $\alpha_0 = 0, \alpha_1 = 1$, то есть $\alpha = (0,1)$.

Теперь можно определить u_0 и u_1 :

$$u_0 = tr(a\lambda^0) = tr((0 + \lambda) = \lambda + \lambda^2 = \lambda + \lambda + 1 = 1,$$

$$u_1 = tr(a\lambda^1) = tr((0 + \lambda)\lambda) = tr(\lambda^2) = tr(\lambda) = \lambda + \lambda^2 = 1.$$

Следствие 7.1. *Период линейной рекуррентной последовательности равен порядку корня λ ее характеристического многочлена и она является последовательностью максимального периода тогда и только тогда, когда ее характеристический многочлен примитивен.*

Литература

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

2. А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин, А.В.Черемушкин. Основы криптографии. М.:Гелиос АРВ. 2001.