ЛИНЕЙНЫЕ РЕКУРРЕНТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ (ЛРП)

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

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

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 (1), в котором свободный член $a = 0$.

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

$$f(x) = x^k - \sum_{j=0}^{k-1} a_j \cdot x^j \tag{2}$$

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*).

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

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

с начальными состояниями

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

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 $\mathbf{u}_n = (u_n, u_{n+1}, \ldots, n_{n+k-1})$, определяющего состояние $\mathbf{q}(\mathbf{n})$ структурного автомата в момент n дискретного времени. При этом начальный вектор $\mathbf{u}_0 = (u_0, \ldots u_{k-1})$ (он же вектор начального состояния $\mathbf{q}(\mathbf{0})$ 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

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

Лемма 1. *Для векторов состояний* $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_n, \ldots$ *ЛРП справедливо равенство*

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

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

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

Здесь a^*_i – коэффициенты *возвратного* многочлена

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

Пример 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 1. *Период ЛРП делит порядок матрицы A, рассматриваемой как элемент группы $GL(k, F_p)$.*

По лемме (3) начальное состояние $\mathbf{u}_0$ ЛРП можно вычислить, если известно состояние $\mathbf{u}_n$:

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

3. Статистические свойства ЛРП

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

Теорема 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 $i = k - m,\ i = 0, 1, 2, \ldots k-1$ 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

$$s_1 s_2 \ldots s_m$$

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

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

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 :

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

С другой стороны, нулевая мультиграмма длины $m-1$ может быть начальным отрезком ненулевой мультиграммы длины m с единственным ненулевым элементом $s_m \in \{1, 2, \ldots p-1\}$ 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 $m-1$:

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

Теоремы доказана, таким образом, индукцией по i.

4.Формула общего члена ЛРП

Выведем формулу общего члена ЛРП, заданной характеристическим многочленом $f(x)$ степени k. При этом будем использовать функцию $tr_P^Q : Q \to P$ следа из расширения $Q = GF(p^k)$ поля $P = GF(p) = F_p$ в простое поле $P = F_p$:

$$tr_P^Q(x) = x + x^p + x^{p^2} + \cdots + x^{p^{k-1}}.$$

Сокращенно эту функцию будем обозначать tr. Свойства операций конечного поля влекут следующие свойства функции след:

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

$$tr(x) = tr(x^{p^k}) = (tr(x))^{p^k}.$$

Лемма 2. *Для любого ненулевого $\alpha \in Q$ 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 3. *Для ЛРП $< u >$, определяемой примитивным характеристическим многочленом (6.2) с корнем λ в поле Q существует единственная константа $\alpha \in Q$ такая, что*

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

Доказательство. Прежде всего заметим, что последовательность (reflrp) является линейной рекуррентной последовательностью (6.1), определяемой характеристическим многочленом (2),

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

Здесь $\sum_{j=1}^{k-1} a_j \cdot \lambda^j = \lambda^k$, так как λ есть корень многочлена 2).

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

$$1, \lambda, \ldots, \lambda^{k-1}$$

константы α.

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

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

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

Тогда линейной комбинации базисных констант

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

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

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

Если λ есть корень примитивного, многочлена, то уравнение

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

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 3.

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

Теорема 3. *Для ЛРП* $< u >$, *определяемой неприводимым характеристическим многочленом (2) с корнем* λ *в поле* Q *существует единственная константа* $\alpha \in Q$ *такая, что*

$$u_n = tr(\alpha \cdot \lambda^n), \ n \geq 0. \tag{3}$$

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 Q :

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

Формула общего члена рекуррентной последовательности, порождаемой примитивным характеристическим многочленом с корнем θ позволяет получить 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 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 3. Пусть $k = 2,\ \lambda$ – корень многочлена $X^2 + X + 1$ над полем $GF(2)$. Константам 1 и λ соответствуют базисные начальные состояния

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

.

Таблица 1:

i	θ^i	$tr(\theta^i \cdot \theta^j = \theta^{i+j}, j = 0, \ldots 63)$
0	100000	**0**000**0**10000**0**110001010**0**011111010001110**0**10**0**10110111**0**110011010**1**0111111
1	010000	**0**000**1**00001**1**00010**1**00111101000111001001011011101100**1**10101111110
2	001000	**0**001000011000**1**01001111010001110010010**1**10111011001101010**1**11111100
3	000100	**0**010000**1**10001010011110100011100**1**0010**1**10111**0**110011010**1**0111111**0**00
4	000010	**0**100**0**01100**1**0**1**0100111101000111001001011011101100**1**10101011111**0**0**0**00
5	000001	**1**00**0**011000**1**0100111101000111001**0**010**1**10111011001101010111111000**0**0

.

Таблица 2:

i	$\lambda^i = \theta^{3i}$	$tr(\lambda^i \cdot \lambda^j) = tr(\theta^{3i} \cdot \theta^{3j} = tr(\theta^{3(i+j)}), j = 0 \ldots 21)$
0	100000	0000010100100110010 11
1	000100	0001000110111111001 11
2	110000	0101011101000011110 11
3	000110	0000101001001100101 10
4	101000	0010001101111110011 10
5	000101	1010111010000111101 10

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

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 $u_n, u_{n+1}, \ldots, u_{k-1}$ 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 4. Пусть $k = 2,\ \lambda$ 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

$$u_2 = tr((\alpha_0 + \alpha_1\lambda)\lambda^2) = \alpha_0 + \alpha_1 tr(\lambda^3) = \alpha_0 + \alpha_1 \cdot 0 = 0,$$

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

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

5. 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 4. *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 характеристический 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.

Линейная сложность имеет свойства:

1) $1 \le L(u^n) \le n$;

2)$L(u^n) = 0 \iff u^n = 0, 0, 0, 0, \ldots, 0$;

3)$L(u^n) = n \iff u^n = 0, 0, 0, 0, \ldots, 0, 1$;

4) если u имеет период N, то $L(u) \le N$;

5)$L(u \oplus t) \le L(u) + L(t)$.

6)если закон рекурсии последовательности определяется неприводимым многочленом степени n, то $L(u) = n$.

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 5. 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:
$1, 1, 1, 3, 3, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 7, 7, 10, 10, 11, 11, 11, 11, 14, 14, 14, 14, 15, 15, 15, 17,$
$17, 17, 18, 18, 19, 19, 19, 19, \ldots$

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

Пример 6. 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.

6. 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.

$$G(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_n x^n + \cdots = \sum_{n=0}^{\infty} u_n x^n. \quad (0.1)$$

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 5. *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

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

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

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

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. Алгоритм 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

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

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

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

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

$$m(x) = x^k g_{2k}(1/x).$$

Если же заранее известно лишь, что $\deg m(x) \leq k$, то минимальный многочлен определяется равенством

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

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

Пример 7. 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

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

Пример 8. 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 9. 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

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

8. Усложнение рекуррентных последовательностей

Необходимые криптографические свойства рекуррентных последовательностей (РП). Используемые в криптографии (как правило для получения псевдослучайных ключевых последовательностей) РП должны иметь достаточно большой период, высокую линейную сложность и хорошие статистические свойства.

Как было показано выше, применительно к ЛРП эти свойства обеспечиваются, если последовательность вырабатывается линейным регистром сдвига с обратной связью, определяемой примитивным многочленом, степень которого равна длине регистра.

Эти необходимые свойства не являются достаточными, чтобы считать последовательность криптографически стойкой.

Действительно, по любому её отрезку длина которого не менее $2k$, где k линейных сложности позволяет восстановить рекуррентное соотношение, а по отрезку длины k можно определить любое состояние последовательности (или, что то же, формирующего её ЛРС).

Известные приемы усложнения генераторов ЛРП не устраняют принципиально этих возможностей их вскрытия, а лишь затрудняют работу соответствующих алгоритмов, поскольку лишь увеличивают период ЛРП и её линейную сложность.

Введение нелинейности в обратную связь, как это будет показано в следующем разделе, позволяет обеспечить равномерное распределение всех без исключения мультиграмм длины не более k. (Это, однако, практически не затрудняет вычисление закона рекурсии или начального состояния ЛРС.)

Использование нелинейных логических фильтров к ЛРС затрудняет вычисление закона рекурсии или начального состояния ЛРС.

Увеличение периода и линейной сложности ЛРП достигаются следующими приемами:

– Нелинейная композиция нескольких ЛРП: использование нескольких ЛРП взаимно простой длины (здесь и ниже предполагается, что используются ЛРП максимальной длины) с подключением их выходов ко входам выходного функционального элемента, реализующего нелинейную функцию алгебры логики.

– Последовательное соединение двух или более ЛРС.

– Использование выходов одного или нескольких ЛРС для управления подвижками ("часам") других ЛРС генератора ЛРП.

Регистры сдвига с нелинейной обратной связью. Многочлен (2) можно записать в виде

$$f(x) = x^k + \varphi(x^0, x^1, x^2, \cdots, x^{k-2}, x^{k-1}), \tag{4}$$

с использованием линейной функции алгебры логики

$$\varphi(x_0, x_1, x_2, \ldots x_{k-1}) = a_0 x_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{k-2} x_{k-2} \oplus a_{k-1} x_{k-1}.$$

(выражение x^i формально рассматривается как значение переменной x_i, при функционировании регистра эти выражения принимают бинарные значения).

В общем случае обратная связь может соответствовать функции алгебры логики

$$\varphi(x_0, x_1, x_2, \ldots x_{k-1})$$

общего вида, не обязательно линейной. Такие регистры называются просто регистрами сдвига с обратной связью (РСОС).

При заданном начальном состоянии $u_0, u_1, \ldots, u_{k-1}$ РСОС формирует выходную последовательность

$$u_0, u_1, u_2, \ldots, u_{k-1}, u_k, \ldots u_j, \ldots$$

где элементы $u_j = u_{n+k},\ j \geq k$ определяются в соответствии с рекуррентным соотношением

$$u_{n+k} = \varphi(u_n, u_{n+1}, \ldots, u_{n+k-1}).$$

РСОС называется несингулярным, если при любом начальном состоянии его выходная последовательность строго периодическая.

Можно показать, что РСОС несингулярен тогда и только тогда, когда рекуррентное соотношение имеет вид

$$u_{n+k} = u_n \oplus \psi(u_{n+1}, u_{n+2}, \ldots, u_{n+k-1}),$$

где ψ есть некоторая функция алгебры логики, то есть если функция обратной связи представляется как

$$\varphi(x_0, x_1, x_2, \ldots x_{k-1}) = x_0 \oplus \psi(x_1, x_2, \ldots, x_{k-1}).$$

Период выходной последовательности РСОС не превышает 2^k. Если длина периода равна 2^k, то РСОС называется РСОС де Брейна, а его выходная последовательность является последовательностью де Брейна (полным циклом).

Пример 10. РСОС с функцией обратной связи

$$\varphi(x_0, x_1, x_2) = 1 \oplus x_0 \oplus x_1 \oplus x_1 x_2$$

и начальным состоянием $(0, 0, 0)$ формирует последовательность де Брейна с периодом

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

образуемую первыми двоичными символами кодов $(u_0 + i, u_1 + i, u_2 + i),\ i = 0, 1, 2, 3, 4, 5, 6, 7.$ состояний этой рекуррентной последовательности:

$$(\mathbf{0}, 0, 0), (\mathbf{0}, 0, 1), (\mathbf{0}, 1, 1), (\mathbf{1}, 1, 1), (\mathbf{1}, 1, 0), (\mathbf{1}, 0, 1), (\mathbf{0}, 1, 0), (\mathbf{1}, 0, 0).$$

Статистические свойства последовательности де Брейна, формируемой РСОС определяет следующая теорема.

Теорема 6. *Каждая мультиграмма длины* $s,\ s \leq k$ *встречается в любом отрезке длины* $2^k + k - 1$ *выходной последовательности* k*-разрядного РСОС де Брейна ровно* 2^{k-s} *раз.*

Регистр сдвига с линейной обратной связью, определяемой линейной функцией алгебры логики

$$\varphi(x_0, x_1, x_2, \ldots x_{k-1}) = a_{k-1}x_{k-1} \oplus \cdots \oplus a_1 x_1 \oplus a_0 x_0.$$

формирующий выходную последовательность максимального периода, может быть преобразован в РСОС де Брейна заменой этой функции функцией

$$\varphi'(x_0, x_1, x_2, \ldots x_{k-1}) = \varphi(x_0, x_1, x_2, \ldots x_{k-1}) \oplus \bar{x}_1 \bar{x}_2 \ldots \bar{x}_{k-1}.$$

Формируемая таким РСОС последовательность отличается от выходной последовательности исходного регистра тем, что мультиграммы, состоящие из $k-1$ символов 0 заменяются мультиграммами из k символов 0.

Пример 11. *Пусть* $\varphi(x_0, x_1, x_2) = x_0 + x_1,\ k = 3$. *(Соответствует неприводимому многочлену* $1 + X + X^3$*). Образуем функцию* $\varphi'(x_0, x_1, x_2) = x_0 \oplus x_1 \oplus \bar{x}_1 \bar{x}_2 = 1 \oplus x_2 \oplus x_1 x_2$. *регистр сдвига при начальном состоянии* $(0, 0, 0)$ *сформирует последоватльность де Брейна*

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

Нелинейные комбинирующие генераторы. Пусть имеются n линейных регистров сдвига ЛРС1, ..., ЛРСn, формирующие ЛРП $< s_1 >, \cdots < s_n >, < s_i >= s_{i0}, s_{i1}, \ldots s_{ik}, \ldots,\ i = 1, \ldots n.$

Подключим их выходы ко входам функционального элемента, реализующего нелинейную функцию алгебры логики $f(x_1, \ldots, x_n)$. Тогда на выходе этого элемента будет формироваться последовательность

$$< u >= u_0, u_1, u_2, \ldots, u_k, \cdots =$$

$$f(s_{1,0},\ldots,s_{n,0}), f(s_{1,1},\ldots,s_{n,1}),\ldots, f(s_{1,k},\ldots,s_{n,k}),\ldots.$$

Как известно, всякая функция алгебры логики представима многочленом Жегалкина (алгебраической нормальной формой). Порядком нелинейности функции называется максимальный ранг элементарных конъюнкций, являющихся слагаемыми многочлена. Например, порядок нелинейности функции

$$f(x_1,x_2,x_3,x_4,x_5) = 1 \oplus x_1x_2 \oplus x_2x_3x_4x_5$$

равен 4.

Известно, что если описанным образом образом объединить n ЛРС максимальной длины, длины которых $k_1, k_2, \ldots k_n$ попарно просты и превышают 2, то линейная сложность выходной последовательности определяется арифметическим выражением, которое получается из многочлена Жегалкина функции f заменой операций конъюнкции операциями арифметического умножения, операций сложения по модулю два операциями арифметического сложения и подстановкой чисел $k_1,\ldots,k_n$ вместо переменных $x_1,\ldots,x_n$. Условно эту схему вычислений можно обозначить как $f(k_1,\ldots,k_n)$.

Пример 12. (Генератор Жеффи). Три ЛРС максимальной длины, такие, что их длины k_1, k_2 и k_3 взаимно просты, объединяются на выходе схемой, реализующей нелинейную функцию алгебры логики

$$f(x_1,x_2,x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3.$$

Выходная последовательность имеет период $(2^{k_1}-1)\cdot(2^{k_2}-1)\cdot(2^{k_3}-1)$. Её линейная сложность k вычисляется как $k = k_1k_2 + k_2k_3 + k_3$.

9. Контрольные вопросы

1. Как по характеристическому многочлену записать закон рекурсии линейной рекуррентной последовательности?

2. Чем ограничен период линейной рекуррентной последовательности?

3. Как определить i-е состояние ЛРП при заданном j-м ее состоянии, зная ее характеристический многочлен над полем F_p и используя матричную алгебру над этим полем?

4. Каковы статистические свойства ЛПР максимального периода.

5.Как вычислить i-й элемент ЛРП, заданной своим начальным состоянием и характеристическим многочленом, не используя матричной алгебры?

6. Как определить закон рекурсии ЛРП порядка k, зная $2k$ ее последовательных элемента.

7. Перечислите три необходимые свойства ЛРП, применяемых в криптографии. Почему ЛРП нельзя применять в системах вычисления псевдослучайных ключевых последовательностей без их предварительного усложнения.

8. Какие способы усложнения ЛРП применяют для получения рекуррентных последовательностей, применяемых для вычисления псевдослучайных ключевых последовательностей?

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.