14 Усложнение л.р.п.

14.1 Минимальный многочлен

Пусть $\gamma = \gamma_1, \gamma_2, \ldots$ — произвольная периодическая последовательность с минимальным периодом r и предпериодом t_0. Такая последовательность удовлетворяет рекуррентному соотношению

$$\gamma_{t+r+t_0} = \gamma_{t+t_0}, \quad t = 1, 2, \ldots,$$

т. е. является л.р.п. с характеристическим многочленом $f(x) = x^{r+t_0} + x^{t_0}$. Последовательность γ удовлетворяет также рекуррентному соотношению

$$\gamma_{t+2r+t_0} = \gamma_{t+t_0}, \quad t = 1, 2, \ldots,$$

с характеристическим многочленом $g(x) = x^{2r+t_0} + x^{t_0}$ и видимо еще многим рекуррентным соотношениям с соответствующими характеристическими многочленами. Поставим вопрос о соотношении между данными многочленами.

Пусть

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_2[x]$$

— произвольный многочлен. Определим операцию произведения f на последовательность γ:

$$f(x)\gamma = w_1, w_2, \ldots, \quad w_t = \sum_{i=0}^{n} a_i \gamma_{t+i}.$$

Удобно интерпретировать данное произведение следующим образом: формальная переменная x отождествляется со сдвигом последовательности γ на одну позицию влево (соответственно, x^i — сдвиг на i позиций). Нетрудно понять, что умножение многочлена gf на γ состоит в умножении f на γ и последующем умножении g на полученную последовательность.

Определение 14.1. Ненулевой многочлен $f(x) \in \mathbb{F}_2[x]$ называется *аннулирующим многочленом* периодической последовательности γ, если $f(x)\gamma$ есть нулевая последовательность. Аннулирующий многочлен наименьшей степени называется *минимальным.* □

Ясно, что характеристический многочлен л.р.п. является аннулирующим, но не обязательно является минимальным.

Упражнение 14.1. Найти минимальный многочлен нулевой последовательности. □

Теорема 14.1 (основное свойство минимального многочлена). Всякий аннулирующий многочлен л.р.п. делится на минимальный.

Доказательство. Пусть γ — искомая ненулевая л.р.п., g — ее аннулирующий многочлен, f — минимальный. Выполним деление:

$$g = hf + r, \quad \deg r < \deg f.$$

Последовательности $g\gamma$ и $f\gamma$ являются нулевыми, следовательно, $r\gamma$ также нулевая последовательность. Но это значит, что $r = 0$, т. е. $f \mid g$. □

В 1969 Мэсси адаптировал алгоритм Берлекэмпа факторизации многочленов и предложил способ определения минимального многочлена f л.р.п. γ (алгоритм Берлекэмпа-Мэсси). Если $\deg f = n$, то для определения многочлена требуется располагать произвольным отрезком $\gamma_t, \gamma_{t+1}, \ldots, \gamma_{t+2n-1}$ длины $2n$.

Пример 14.1 (недостатки РСЛОС). Рассмотрим n-разрядный РСЛОС, который вырабатывает л.р.п. (s_t) порядка n с характеристическим многочленом f. Мы выяснили, что если f примитивен и начальное состояние S_0 РСЛОС не является нулевым, то выходная последовательность (s_t) обладает многими замечательными свойствами, а именно:

– высокий период;

– равная частота встречаемости 0 и 1;

– отсутствие значимых корреляций.

Кажется, что для построения поточной криптосистемы можно по ключу $K = (S_0, f)$ выработать л.р.п. (s_t) и использовать ее для наложения на открытый текст или шифртекст. Однако, Виктор по отрезку $(s_t, s_{t+1}, \dots, s_{t+2n-1})$ может определить f и сопровождающую его матрицу A, затем определить состояние $S_t = (s_t, s_{t+1}, \dots, s_{t+n-1})$ и вычислить $S_0 = S_t A^{-t}$. □

Пример означает, что использование л.р.п. в чистом виде не обеспечивает криптографическую стойкость. Далее мы рассмотрим некоторые подходы по усложнению л.р.п.

14.2 Генераторы на базе РСЛОС

Пусть имеется один или несколько РСЛОС. Всюду далее будем предполагать, что в регистрах используются ненулевые начальные состояния и характерестические многочлены являются примитивными, т. е. РСЛОС выдают m-последовательности.

Будем нумеровать регистры от 1 до d и при $d > 1$ помечать элементы i-го РСЛОС верхним индексом (напр., $(s_t^{(i)})$ — выходная л.р.п. соответствующего регистра).

Фильтрующий генератор ($d = 1$). Пусть $g \in \mathcal{F}_n$ — произвольная булева функция. Правило определения выходного символа

$$s_t = S_{t,1}, \quad t = 1, 2, \dots$$

заменяется на правило

$$\gamma_t = g(S_t).$$

Комбинирующий генератор (d — произвольно). Выходные последовательности РСЛОС обрабатываются функцией $g \in \mathcal{F}_d$:

$$\gamma_t = g(s_t^{(1)}, \dots, s_t^{(d)}), \quad t = 1, 2, \dots.$$

Пример 14.2 (генератор Геффе). В комбинирующем генераторе Геффе $d = 3$ и $f(x_1, x_2, x_3) = x_1x_2 + (x_1+1)x_3$: выходной символ первого регистра управляет выбором между выходными символами второго или третьего регистров.□

Неравномерное движение. В этом случае выходные символы РСЛОС$^{(i)}$ управляют выполнением преобразований на РСЛОС$^{(j)}$ — автомат РСЛОС$^{(j)}$ может либо выполнять стандартное рекуррентное преобразование (умножение вектора состояния $S_t^{(j)}$ на сопровождающую матрицу характеристического многочлена $A^{(j)}$, *шаг*), либо простаивать ($S_{t+1}^{(j)} = S_t^{(j)}$, *стоп*).

Пример 14.3 (поточная криптосистема `A5/1`). Для защиты голосовых данных в сетях GSM используется поточная криптосистема `A5/1`. Криптосистема построена на базе трех РСЛОС с использованием техники неравномерного движения. Регистры сдвига — 19-, 22- и 23-разрядные. Начальное заполнение регистров определяется на основании ключа $K \in \mathbb{F}_2^{64}$, $64 = 19 + 22 + 23$.

Используется отображение $F\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$. Значения $(y_1, y_2, y_3) = F(x_1, x_2, x_3)$ определяются по следующей таблице:

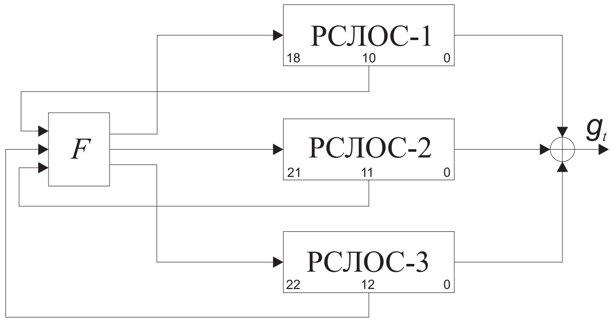
x_1	x_2	x_3	y_1	y_2	y_3
0	0	0	1	1	1
0	0	1	1	1	0
0	1	0	1	0	1
0	1	1	0	1	1
1	0	0	0	1	1
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

Действие F можно интерпретировать следующим образом: если в векторе (x_1, x_2, x_3) совпадают все координаты, то $y_1 = y_2 = y_3 = 1$. Если же $x_i = x_j \neq x_k$, то $y_i = y_j = 1$, $y_k = 0$ (правило большинства).

В фиксированных разрядах каждого РСЛОС снимаются биты x_1, x_2, x_3, которые подаются на вход функции F. Выходные биты y_1, y_2, y_3 определяют шаг или простой соответствующих РСЛОС.

Выходной символ определяется по правилу:

$$\gamma_t = S_{t,1}^{(1)} + S_{t,1}^{(3)} + S_{t,1}^{(3)}, \quad t = 1, 2, \ldots.$$



□

Сжимающий генератор ($d = 2$). Выходная последовательность РСЛОС$^{(1)}$ управляет выбором выходных символов РСЛОС$^{(2)}$:

$$\gamma_t = s_{\tau_t}^{(2)},$$

где τ_t — номер t-й единицы в последовательности $s_1^{(1)}, s_2^{(1)}, \ldots$.

Самосжимающий генератор ($d = 1$). Выходная последовательность разбивается на пары

$$(s_1, s_2), (s_3, s_4), \ldots.$$

Пары $(0, a)$ игнорируются, а по паре $(1, a)$ формируется очередной выходной символ $\gamma_t = a$.

14.3 Линейная сложность

Определение 14.2. *Линейной сложностью* $l(\gamma)$ периодической последовательности γ называется степень ее минимального многочлена. □

Одна из целей описанного выше усложнения л.р.п. состоит в повышении линейной сложности выходных последовательностей. Для практически используемых в криптографии конечных автоматов получение оценок для линейной сложности является достаточно сложной теоретической задачей. Мы рассмотрим только одну оценку.

Теорема 14.2 (линейная сложность самосжимающего генератора). Пусть γ — выходная последовательность самосжимающего генератора, результат усложнения m-последовательности (s_t) порядка n. Тогда справедлива следующая оценка для линейной сложности:

$$l(\gamma) > 2^{\lfloor n/2 \rfloor - 1}.$$

Доказательство. Доказательство проведем в три этапа.

1. Пусть r — минимальный период γ. Докажем, что $r \mid 2^{n-1}$. Рассмотрим пары

$$(s_1, s_2), (s_3, s_4), \ldots, (s_{2^n-1}, s_1), (s_2, s_3), \ldots (s_{2^n-2}, s_{2^n-1}), (s_1, s_2), \ldots$$

Как видим, последовательность пар является чисто периодической с периодом $2^n - 1$.

Из доказательства постулатов Голомба для m-последовательностей следует, что среди первых $2^n - 1$ пар встретятся пары:

(i) $(0, 0)$ — $2^{n-2} - 1$ раз (такие пары отбрасываются при самосжимании);

(ii) $(0, 1)$ — 2^{n-2} раз (отбрасываются);

(iii) $(1, 0)$ — 2^{n-2} раз (выдается 0);

(iv) $(1, 1)$ — 2^{n-2} раз (выдается 1).

Таким образом, по 2^n-1 парам будет построено 2^{n-1} выходных символов γ и 2^{n-1} — период γ. Минимальный период последовательности обязан делить всякий другой период (проверить!), т. е. $r \mid 2^{n-1}$.

2. Докажем, что $r \geqslant 2^{\lfloor n/2 \rfloor}$. Пусть сначала n — четное, $n = 2m$. Векторы состояний $S_1, \dots, S_{2^n-1}$ базового РСЛОС пробегают все ненулевые векторы из $\mathbb{F}_2^n$, в том числе все векторы вида

$$(1, a_1, 1, a_2, \dots, 1, a_m).$$

Но таким векторам соответствуют m-граммы $(a_1, a_2, \dots, a_m)$ в последовательности γ. Число различных m-грамм не может быть меньше периода выходной последовательности, т. е. $r \geqslant 2^m$.

Случай n — нечетное, $n = 2m+1$, рассматривается аналогично. Используется тот факт, что векторы $S_1, \dots, S_{2^n-1}$ пробегают каждый из шаблонов

$$(1, a_1, 1, a_2, \dots, 1, a_m, b),$$

ровно по одному разу.

3. Из 1 и 2 следует, что $r = 2^d$, $d \geqslant \lfloor n/2 \rfloor$. Пусть $f(x)$ — искомый минимальный многочлен γ. Многочлен $f(x)$ должен делить $x^r - 1 = (x-1)^{2^d}$, т. е.

$$f(x) = (x-1)^l,$$

где l и есть искомая линейная сложность. Остается доказать, что $l > 2^{d-1}$.

От противного, пусть $l \leqslant 2^{d-1}$. Тогда

$$f(x) \mid (x-1)^{2^{d-1}} = x^{2^{d-1}} - 1$$

и выходная последовательность обязана удовлетворять рекуррентному соотношению $\gamma_{t+2^{d-1}} = \gamma_t$. Но тогда ее период меньше r, противоречие. □

Пример 14.4 (линейная сложность комбинирующего генератора). Если $G^{(i)}$ – генераторы m-последовательностей порядка n_i, $i = 1, \dots, d$, то линейную сложность последовательности $g_0, g_1, \dots$ можно определить, вычислив значение многочлена Жегалкина $g(x_1, \dots, x_d)$ при значениях n_i переменных x_i, выполняя умножение и сложение в кольце $\mathbb{Z}$, а не в поле $\mathbb{F}_2$. Например, линейная сложность выходных последовательностей генератора Геффе равняется $n_1 n_2 + n_1 n_3 + n_3$. □