УДК 681.3.067

АЛГОРИТМ И СРЕДСТВА ГЕНЕРАЦИИ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

МЕЛЬНИКОВА О.А., ОЛЕШКО О.И., ГОЛОВАШИЧ С.А.

Рассматриваются вопросы построения примитивных образующих полиномов для линейных рекуррентных регистров, применяемых для генерации линейных рекуррентных последовательностей максимального периода. Предложен алгоритм проверки трёхчленных многочленов на неприводимость и принципы построения на их основе примитивных полиномов.

Линейные рекуррентные последовательности максимального периода (ЛРПМ) применяются в системах связи со сложными сигналами, а также в системах криптографической защиты информации. Их применение в системах связи объясняется хорошими корреляционными свойствами, а применение в системах защиты информации — заведомо известным периодом повторения, идеальными свойствами псевдослучайности.

Для формирования ЛРПМ применяются линейные рекуррентные регистры (ЛРР). Работа ЛРР по формированию ЛРПМ полностью определяется характеристическим многочленом:

$$f(X) = A_0X^n + A_1X^{n-1} + \ldots + A_{n-1}X + A_n \ , \quad (1)$$

где $A_0, A_1, \ldots, A_n$ — коэффициенты многочлена над полем $GF(P)$.

В названных приложениях наибольшее применение нашли двоичные ЛРПМ ($P=2$). Основные свойства двоичных ЛРПМ: длина ЛРПМ равна 2^n-1, где n – число разрядов ЛРР; число единиц в ЛРПМ на одну больше, чем нулей; сложение по модулю 2 любой ЛРПМ с другой ЛРПМ, полученной из данной путем циклического сдвига, также является ЛРПМ, которая представляет собой циклический сдвиг исходной ЛРПМ на другое число позиций; каждое возможное состояние линейного рекуррентного регистра за время формирования полной ЛРПМ возникает в некоторый момент времени только один раз; для определения закона функционирования ЛРПМ необходимо получить $2n$ безошибочных бит. Состояние ЛРР, при котором все разряды содержат нули – запрещено.

ЛРПМ обладает свойством псевдослучайности, т. е. в ней $1/2$ всех серий подряд расположенных одинаковых символов имеет длину 1, $(1/2)^2$ длину 2, $(1/2)^3$ длину 3.

1. Линейные рекуррентные регистры

Пусть необходимо построить ЛРР, вырабатывающий двоичную ЛРПМ длиной 2^n-1, работа которого определяется характеристическим многочленом (1). Структурная схема ЛРР представлена на рис.

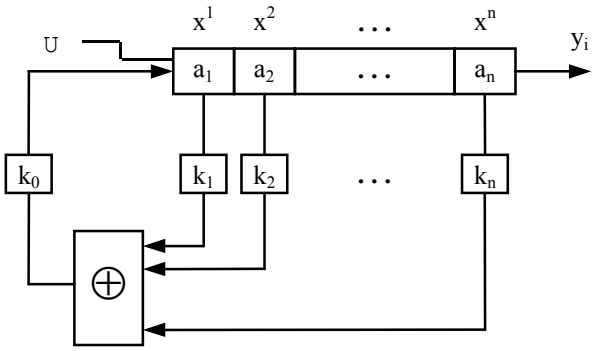

Рис. Структура линейного регистра

Вектор $(a_1, a_2, \ldots, a_n)_i$ определяет текущее состояние регистра (или его исходное состояние перед началом работы), а вектор $(k_0, k_1, \ldots, k_n)$ определяет необходимые обратные связи. При подаче на ЛРР тактовой сдвигающей частоты регистр входит в рабочее состояние.

На каждом такте i содержимое последней ячейки (a_n) считывается на выход (y_i), тем самым дополняя создаваемую ЛРПМ очередным символом. В то же время значения всех ячеек умножаются на соответствующие коэффициенты k и поступают на вход общего сумматора. Результат суммирования умножается на k_0 и поступает на вход регистра (ячейка a_1). На этом работа ЛРР в очередном такте заканчивается. Так как ЛРПМ имеет период 2^n-1, то после 2^n-1 тактов работы регистр принимает исходное состояние. В нашем случае необходимо получить двоичную последовательность, поэтому вектор $(a_1, a_2, \ldots, a_n)$ является двоичным, и в сумматоре выполняется сложение по модулю 2. Отметим, что нулевое состояние регистра является запрещенным, так как оно приводит к нулевой последовательности; при корректном выборе характеристического многочлена, правильном синтезе регистра и выборе ненулевого вектора $(a_1, a_2, \ldots, a_n)$ оно не может возникнуть.

2. Принцип построения примитивных полиномов

Для определения структуры ЛРР разрядности n необходимо знать характеристический многочлен степени n, причем многочлен $f(X)$ степени n должен быть неприводимым к виду произведения многочленов меньших степеней и примитивным относительно двучлена X^N-1, где $N=2^n-1$, т. е. должен делить его без остатка. Поскольку ЛРПМ широко применяются, то их свойства и многочлены были изучены основательно [1].

Проверка примитивности выбранного характеристического многочлена небольших степеней проводится с помощью построения функций автокорреляции и взаимокорреляции.

Значение корреляционных функций определяется как разность между числом совпадений и числом несовпадений при посимвольном сравнении кодовой последовательности или последовательностей в случае определения взаимной корреляции. При построении корреляционной функции происходит сравнение двух ЛРПМ, причем сравнение проводится после каждого сдвига одной последовательности относительно другой на один символ на протяжении всего периода ЛРПМ. Естественно, что периоды сравниваемых последовательностей должны быть равны. Функция автокорреляции (в сравнении участвует одна последовательность) для примитивного характеристического многочлена равна -1 при всех значениях сдвига, кроме нулевого. В случае нулевого сдвига (условие полной синхронизации) ненормированное значение функции автокорреляции равно 2^n-1. Функция взаимной корреляции, когда в качестве сравниваемых последовательностей выступают две ЛРПМ, построенные на основе примитивных мно-

гочленов, при малой амплитуде разбросов говорит о хороших корреляционных свойствах ЛРПМ. Таким образом, для проверки характеристического многочлена малой степени на примитивность достаточно проанализировать свойства построенной на его основе ЛРПМ. Известны таблицы, в которых приведены некоторые примитивные многочлены до степени 34 [1]. Проверить примитивность многочленов степеней, больших 34, весьма сложно. Эта задача сводится к нахождению трехчленных многочленов степени n вида

$$f(X) = X^n + X^r + 1 \qquad (2)$$

над полем из двух элементов, причем $r < (n+1)/2$.

Основой для нахождения таких многочленов является утверждение [3]: поскольку 0 и 1 не могут быть корнями многочлена (2) ($X+X^2$ и (2) взаимопросты), то трехчлен неприводим если

$$X^{2^n} = X \ (mod\ (X^n + X^r + 1)). \qquad (3)$$

Воспользовавшись тем, что для любого многочлена $g(X)$ над полем P верно равенство [5]:

$$(g(X))^2 = g(X^2), \qquad (4)$$

построим цепочки сравнения вида

$$X^{2^k} = g_k(X) \ (mod\ (X^n + X^r + 1)), \qquad (5)$$

где $g_k(X)$ — многочлен степени, меньшей n.

Посредством последовательного нахождения остатков можно реализовать эффективный способ проверки трехчленных многочленов на примитивность и с его помощью выявить необходимое множество примитивных многочленов. Проведенный анализ показал, что по известному неприводимому многочлену степени n, имеющему вид

$$f(X) = X^n + C_1X^{n-1} + \ldots + C_{n-1}X + C_n, \qquad (6)$$

строится неприводимый многочлен степени n вида

$$g(X) = X^n + t_1X^{n-1} + \ldots + t_{n-1}X + t_n \qquad (7)$$

такой, что при элементе N (примитивном по модулю 2^n-1) вектор коэффициентов $(t_1, t_2, \ldots, t_n)$ является функцией от вектора коэффициентов $(C_1, C_2, \ldots, C_n)$ и, если A — корень неприводимого многочлена $f(X)$, то корнем многочлена $g(X)$ является A^N.

3. Алгоритм построения примитивных трехчленов

Если n — простое число, то число неприводимых многочленов степени n над полем P находится по [4]:

$$Y(n) = (P^n - P) / n, \qquad (8)$$

а число примитивных многочленов, при $P = 2$, как

$$\Phi(2^n-1) / n, \qquad (9)$$

где $\Phi(X)$ — функция Эйлера [2].

Допустим, что 2^n-1 — простое число, тогда $\Phi(2^n-1) = 2^n-2$, поэтому число примитивных многочленов над полем 2 равно $(2^n-2)/n$. Следовательно, при простых n и 2^n-1 любой неприводимый многочлен степени n над полем из двух элементов является примитивным. Заметим, что это свойство выполняется только для характеристики поля $P = 2$.

Рассмотрим задачу нахождения неприводимых трёхчленных многочленов степени n над полем из двух элементов вида (2). Будем предполагать, что n — простое число (n не равно 2), а также что $r < (n+1)/2$, чтобы исключить "зеркально симметричные" многочлены. Многочлен неприводим тогда и только тогда, когда выполняется тождество (3).

Если найдено сравнение

$$X^{2^k} = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1X + a_0 \ (mod f(X)), \qquad (10)$$

то $X^{2^{k+1}} = (a^{2^k})^2 = a_{n-1}X^{2(n-1)} + a_{n-2}X^{2(n-2)} + \ldots$

$$+ a_1X^2 + a_0 \ (mod f(X)). \qquad (11)$$

Чтобы получить из X^{2^k} сравнение $X^{2^{k+1}}$, следует каждую степень X^{2m} $(m=1,2, \ldots, n-1)$ заменить сравнимым с ней многочленом степени, меньшей n, по модулю $f(X)$. Известно, что $X^n = X^r + 1 \ (mod f(X))$. Обозначим $n=2S+1$. Степени X^{2i} $(i \le S)$ заменять не следует, поскольку в этом случае $2i<n$:

$$X^{2S+i} = X^{n+i-1} = X^{r+i-1} + X^{i-1}. \qquad (12)$$

Возьмем $1 \le i \le n-r$, тогда правая часть сравнения (12) имеет степень, меньшую n. Если $i > n-r$, то

$$X^{2S+i} = X^{n-1+(r+i-n)} + X^{i-1} = X^{2S+(r+i-n)} + X^{i-1}. \qquad (13)$$

Используя для первого слагаемого (12), получим:

$$X^{2S+i} = X^{2r+i-n-1} + X^{r+i-n-1} + X^{i-1}. \qquad (14)$$

При $2S=n-1$ имеем $X^{2S} = X^{n-1}$, поэтому окончательно формулы будут иметь вид

$$X^{n+i-1} = X^{r+i-1} + X^{i-1} \quad \text{при } 1 \le i \le n-r; \qquad (15)$$

$$X^{n+i-1} = X^{2r+i-n-1} + X^{r+i-n-1} + X^{i-1} \quad \text{при } n-r+1 \le i \le n-1. \qquad (16)$$

Формулы дают возможность составить алгоритм проверки трёхчленов (2) на неприводимость, который опишем на примере степени $n=89$. Будем искать неприводимый многочлен степени 89 среди

$$f(X) = X^{89} + X^r + 1, \text{ при } 1 \le r \le 44. \qquad (17)$$

Требуется проверить сравнение

$$X^{2^{89}} = X \ (mod f(X)). \qquad (18)$$

По (15) и (16) при $X^{89} = X^r + 1 \ (mod f(X))$ получим:

$$X^{88+i} = X^{r+i-1} + X^{i-1}, \text{ при } 1 \le i \le 89-r; \qquad (19)$$

$$X^{88+i} = X^{2r+i-90} + X^{r+i-90} + X^{i-1}, \text{ при } 89-r \le i \le 88. \qquad (20)$$

Например, по (19) $X^{2^7} = X^{128} = X^{39+r} + X^{39}$. Последовательно найдем остатки от деления на $f(X)$ для $(X^{2^8}, \ldots, X^{2^{89}})$. Например, $X^{2^8} = (X^{2^7})^2 = X^{128} = (X^{39+r} + X^{39})^2 = X^{78+2r} + X^{78}$, а дальше применяем (19) или (20) в зависимости от r. Если связать с каждым остатком от деления на $f(X)$ многочлен

$$f(X) = A_0 + A_1X + \ldots + A_{88}X^{88} \qquad (21)$$

или вектор $A=(A_0, A_1, \ldots, A_{88})$, то остатку от деления X^{2^7} на $f(X)$ соответствует вектор, где лишь $A_{39+r} = A_{39} = 1$, остальные координаты равны 0.

Опишем, как по вектору $A=(A_0, A_1, \ldots, A_{88})$, соответствующему остатку от деления X^{2^n} на $f(X)$, строится вектор $B=(B_0, B_1, \ldots, B_{88})$, соответствующий остатку от деления $X^{2^{(n+1)}}$ на $f(X)$:

1. Если $A_k = 1$ $(0 \le k \le 88)$, то вычисляем $2k$.
2. Если $2k \le 88$, то $B_{2k} = 1$.
3. Если $2k > 89$, то $i = 2k-88$.
4. Если $1 \le i \le 89-r$, то $B_{r+i-1} = B_{i-1} = 1$ по (19).
5. Если $89-r < i \le 88$, то $B_{i-1} = B_{2r+i-90} = B_{r+i-90} = 1$, согласно (20).
6. $A_k = B_k$ $(0 \le k \le 88)$.

Все присваивания выполняются по модулю 2.

Шаги 1-6 повторяются 82 раза, начиная с X^{2^7}. Если по окончании цикла получим вектор B с $B_1 = 1$ (остаток равен X), то $f(X)$ — неприводимый и, следовательно, примитивный трёхчлен, так как 89 и $2^{89}-1$ простые числа. Теперь изложим основные теоретические выкладки, позволяющие предположить, что по известному неприводимому многочлену степени n можно построить другой неприводимый многочлен той же степени.

Предположим, что найден неприводимый примитивный многочлен степени n. Если n и 2^n-1 — простые, то любой неприводимый многочлен сте-

пени n примитивен. Пусть $C_1, C_2, \ldots, C_n$ — элементарные симметрические функции n переменных:

$$C_1(X_1, X_2, \ldots, X_n) = X_1 + X_2 + \ldots + X_n,$$
$$C_2(X_1, X_2, \ldots, X_n) = X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n, \quad (22)$$
$$\ldots\ldots$$
$$C_n(X_1, X_2, \ldots, X_n) = X_1X_2 \ldots X_n.$$

Тогда через C_i^f обозначим значения симметрических многочленов в точке $(a_1, a_2, \ldots, a_n)$, где a — корни многочлена $f(X)$. Корни примитивного многочлена $f(X)$ равны: $a, a^2, a^{2^2}, \ldots, a^{2^{n-1}}$ (a — фиксированный корень многочлена $f(X)$). Пусть N не является степенью двойки $(3 \leq N < 2^{n-1})$, тогда a^N — примитивный элемент, корень примитивного многочлена $g(X)$ степени n, отличного от $f(X)$. Остальные его корни имеют вид: $a^{N*2}, a^{N*2^2}, \ldots, a^{N*2^{n-1}}$, т.е. корни многочлена $g(x)$ являются N-ми степенями корней многочлена $f(X)$. Следовательно,

$$C_i^g = C_i(a_1^N, a_2^N, \ldots, a_n^N). \quad (23)$$

Если выразить C_i^g через C_i^f, то можно найти коэффициенты многочлена $g(X)$. Обозначим:

$$S_k = S(X_1^k) = X_1^k + X_2^k + \ldots + X_n^k; \quad (24)$$

$$t_k = S(X_1^N, X_2^N, \ldots, X_k^N) = C_k(X_1^N, X_2^N, \ldots, X_n^N). \quad (25)$$

Будем искать коэффициенты $g(X)$ в следующем порядке: через коэффициенты $f(X)$ найдем S_k, а через S_k выразим t_k. Для S_k известны рекуррентные формулы Ньютона, которые запишем с учетом двоичной характеристики поля:

$$S_k = S_{k-1}C_1 + S_{k-2}C_2 + \ldots + S_1C_{k-1} + kC_k, \text{ для } k \leq n; \quad (26)$$

$$S_k = S_{k-1}C_1 + S_{k-2}C_2 + \ldots + S_{k-n}C_n, \text{ для } k > n. \quad (27)$$

Для экономии вычислений нужно учитывать, что $S_{2k}^2 = S_k$. Формулы (26) и (27) позволяют, зная $C_1, C_2, \ldots, C_n$ и начиная с $S_1 = C_1$, последовательно вычислять $S_1, S_2, \ldots, S_k$ для любого k.

По стандартной процедуре выражения симметрического многочлена через элементарные симметрические многочлены найдем, что

$$t_1 = S(X_1^N) = C_1^3 + C_1C_2 + C_3; \quad (28)$$

$$t_2 = S(X_1^N X_2^N) = C_2^3 + C_1^2C_4 + C_2C_4 + C_1C_5 + C_6. \quad (29)$$

По индукции получится формула

$$t_k = t_{k-1}S_{N*1} + t_{k-2}S_{N*2} + \ldots + t_1S_{N*(k-1)} + S_{N*k}, \quad (30)$$

или все коэффициенты нового неприводимого многочлена для $k \leq 3$. Приняв их за начальные, после повторения той же процедуры получаем коэффициенты следующего неприводимого многочлена. Таким образом, мы сможем получить все неприводимые многочлены степени n, причем за первые $(2^n-2)/n$ шагов, но только в том случае, если N является первообразным корнем сравнения:

$$X^{2^{N-2}} = 1 \pmod{2^N-1}. \quad (31)$$

4. Анализ основных приложений

Основными приложениями решения задач построения примитивных полиномов являются системы защиты информации и системы кодирования. Необходимость знания примитивных полиномов с различными базами вплоть до 1024 связана с потребностью создания средств исходных последовательностей. Дело в том, что требуемое качество скрытия смыслового содержания может быть достигнуто, если период последовательности составляет порядка 10^{40}–10^{300} символов. При этом указанный период должен быть гарантирован, что обеспечивается использованием линейных автоматов типа ЛРР, в которых обратные логические связи реализуются в соответствии с выбранным примитивным полиномом. При этом в системах защиты различного назначения длины периодов последовательностей могут быть различными, что вызывает необходимость построения примитивных полиномов для различных длин. Кроме того, качество защиты информации может быть улучшено за счет смены законов формирования последовательностей в динамическом режиме, непосредственно в процессе работы системы. Для этого необходимо знать не только один полином, а уже все используемое множество изоморфизмов примитивных полиномов.

Вторым приложением работы является формирование сложных фазоманипулированных сигналов с расширением спектра. Применение для этих целей рассматриваемых рекуррентных последовательностей обеспечивает быстрый поиск сигналов и их прием на фоне мощных помех. Сложные сигналы, сформированные на основе линейных последовательностей, обладают идеальными автокорреляционными и хорошими взаимокорреляционными свойствами. В табл. приведены некоторые неприводимые трехчлены от 35 до 257 степени.

Таблица

Степень n	Варианты степени r	Степень n	Варианты степени r
35	2	142	21
44	5	150	53,73
49	9,12,15,22	159	31,34,40
57	4,7,22,25	167	6,35,59,77
63	1,5,11,28,31	174	13,57
68	9,33	183	56
76	21	194	87
86	21	202	55
90	27	210	7,21,63
94	21	217	45,64,66,82,85
98	11,27	222	105
103	9,13,30,31	228	63,113
108	17,27,31,33,45	234	31,103
111	10,49	239	36,81
118	33,45	244	111
123	2	249	35,86
129	5,31,46	253	46

Литература: 1. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир.– 1976.– 594 с. 2. *Виноградов И.М.* Основы теории чисел. М.: Наука, Главная редакция физико-математической литературы.– 1981.– 176 с. 3. *Завало С.Т., Костарчук В.Н., Хощет Б.И.* Алгебра и теория чисел. Киев: В. шк. Головн. Изд-во.– 1980.– 408 с. 4. *Долгов В.И., Горбенко И.Д., Снытkин И.И.* Теория дискретных сигналов. Часть 1. Оптимальные дискретные сигналы с одно- и двухуровневой ПФАК. МО СССР, 1983.– 142 с. 5. *Жальников В.* Криптография от папируса до компьютера.– М.: ABF.– 1996.– 336 с.

Поступила в редколлегию 12.10.97

Мельникова Оксана Анатольевна, аспирантка кафедры ЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: 310726, Украина, Харьков, пр.Ленина, 14, тел. 30-24-50.

Олешко Олег Иванович, аспирант кафедры ПО ЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: 310726, Украина, Харьков, пр.Ленина, 14, тел. 30-24-50.

Головашич Сергей Александрович, стажер-исследователь кафедры ЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: 310726, Харьков, пр.Ленина, 14, тел. 30-24-50.