С. Ш. ОГАНЕСЯН, В. Г. ЯГДЖЯН

НАХОЖДЕНИЕ ЦИКЛИЧЕСКИХ ПРЕДСТАВИТЕЛЕЙ В БИНАРНЫХ ЦИКЛИЧЕСКИХ АЛФАВИТАХ

Для исследования корректирующих возможностей циклических алфавитов (циклических кодов) в большинстве случаев необходимо знание весового спектра алфавита.

Весовым спектром алфавита называется множество чисел $\{A(0), A(1), \cdots A(s), \cdots A(n)\}$, где n — блоковая длина алфавита, $A(s)$ — число букв в алфавите с s количеством единиц.

Вычисление спектра на ЦВМ требует огромного машинного времени из-за большого количества букв. Так как буквы, принадлежащие к одному и тому же циклу, имеют одинаковый вес, то для вычисления спектра алфавита достаточно определение весов букв, которые являются представителями различных циклов алфавита. Таким образом, сокращается необходимое машинное время для вычисления спектра.

Бинарные циклические алфавиты, как известно, можно рассматривать как множество полиномов из кольца полиномов R_n по модулю $(X^n - 1)$ над полем $GF(2)$, которые делятся на фиксированный полином $g(x)$. Такое множество полиномов называется идеалом, а $g(x)$ — порождающим полиномом этого идеала.

Минимальным идеалом называется идеал, который не содержит в себе ненулевых идеалов. Можно показать, что идеал, порожденный полиномом $g(x) = (X^n - 1)/h(x)$, где $h(x)$ — неприводимый полином, а n нечетно, является минимальным.

Метод нахождения циклических представителей для алфавитов, являющихся минимальными идеалами, дан в работе [1]; кроме того, в работе [2] дан метод нахождения циклических представителей алфавита, являющегося объединением двух минимальных идеалов.

В настоящей работе описан метод нахождения циклических представителей для любого циклического алфавита.

* * *

Циклические представители минимального идеала U_i, порожденного полиномом $g_i(x) = (x^n - 1)/h_i(x)$, имеют вид $\{0, \alpha_i^0(x) \cdot \varepsilon_i(x), \alpha_i^1(x) \cdot \varepsilon_i(x), \cdots, \alpha_i^{m_i - 1}(x) \cdot \varepsilon_i(x)\}$, где $\alpha_i(x)$ — примитивный элемент поля

$GF(2^{k_i})$ по модулю полинома $h_i(x)$, $h_i(x)$ — неприводимый полином степени k_i над полем $GF(2)$, показатель которого e_i, $\varepsilon_i(x)$ — идемпотент*) U_i, $m_i = (2^{k_i}-1)/e_i$ — количество циклических представителей идеала U_i, $i = 1, 2, \cdots t$.

В данной статье дается метод нахождения циклических представителей идеала $U = U_1 \cup U_2 \cup \cdots \cup U_i \cdots \cup U_t$, порожденного полиномом $g(x) = (x^n-1)/h_1(x) \cdots h_i(x) \cdots h_t(x)$. Имеет место следующая теорема.

Циклические представители идеала U имеют вид

$$a_1 X^{d_1+d_2+\cdots+d_j+\cdots+d_{t-1}} + \cdots + a_i X^{d_i+d_{i+1}+\cdots+d_j+\cdots+d_{t-1}} + \cdots + a_t, \quad (1)$$

где $d_j \in D_j$, $a_i \in A_i$, A_i — множество циклических представителей идеала U_i, D_j — множество чисел $\{0, 1, \cdots (\text{H.O.D.}(\text{H.O.K.}(b_1, b_2, \cdots \cdots b_j), b_{j+1}-1)\}$,

$$b_i = \begin{cases} 1, \text{ если из множества } A_i \text{ выбран } 0 \\ e_i \text{ в остальных случаях.} \end{cases}$$

Период циклического представителя равен H.O.K.$(b_1, b_2, \cdots b_j, \cdots \cdots b_t)$. В дальнейшем H.O.D. $(r_1, r_2, \cdots r_k)$ будем обозначать через $(r_1, r_2, \cdots r_k)$, а H.O.K. $(r_1, r_2, \cdots r_k)$ соответственно $[r_1, r_2, \cdots r_k]$.

Доказательство. Найдем период, т. е. наименьшее натуральное T, когда выполняется следующее равенство:

$$(a_1 X^{d_1+d_2+\cdots+d_{t-1}} + \cdots + a_t)\, X^T = a_1 X^{d_1+d_2+\cdots+d_{t-1}} + \cdots + a_t. \quad (2)$$

Ввиду того, что U является прямой суммой минимальных идеалов, равенство (2) распадается на следующие сравнения:

$$\begin{aligned} T &\equiv 0 \mod (b_1) \\ &\cdots\cdots\cdots \\ T &\equiv 0 \mod (b_i) \\ &\cdots\cdots\cdots \\ T &\equiv 0 \mod (b_t). \end{aligned}$$

Отсюда очевидно, что

$$T = [b_1, b_2, \cdots b_i, \cdots b_t]. \quad (3)$$

Для дальнейшего достаточно показать, что:

1. Все элементы вида (1) принадлежат различным циклам, т. е.

$$a_1 X^{d_1+\cdots+d_j+\cdots+d_{t-1}} + \cdots + a_t = X^{\mu}(a_1' X^{d_1'+\cdots+d_j'+\cdots+d_{t-1}'} + \cdots + a_t') \quad (4)$$

только в случае, когда $a_i = a_i'$, $d_j = d_j'$, где $i = 1, 2, \cdots, t$, $j = 0, 1, 2, \cdots, (t-1)$, μ — любое целое число.

---

*) Идемпотент имеет следующие два свойства:

1. $\varepsilon_i(x) = \varepsilon_i^2(x)$; 2. $\varepsilon_i(x) \cdot R_n = U_i$.

2. Количество элементов вида (1) равно числу циклов идеала U.

Доказательство 1-го пункта разбивается на две части:

а) Необходимое условие выполнения равенства

$$a_1 X^{\mu_1} + \cdots + a_i X^{\mu_i} + \cdots + a_t X^{\mu_t} = a_1' X^{\mu_1'} + \cdots + a_{i'}' X^{\mu_{i'}'} + \\ + \cdots + a_{t'}' X^{\mu_{t'}'} \qquad (5)$$

при любых значениях μ_i и $\mu_{i'}'$, где i, i' пробегают $1, 2, \cdots t$, является $a_i = a_{i'}'$.

В работе [2] показано, что идеал U есть прямая сумма минимальных идеалов U_i, т. е. $U = U_1 + U_2 + \cdots + U_i + \cdots + U_t$, поэтому для выполнения равенства (5) необходимо, чтобы $a_i X^{\mu_i} = a_{i'}' X^{\mu_{i'}'}$, а так как циклы не пересекаются, то $a_i = a_{i'}'$.

После доказательства (а) равенство (4) принимает следующий вид:

$$a_1 X^{d_1 + \cdots + d_j + \cdots + d_{t-1}} + \cdots + a_t = X^{\mu} (a_1 X^{d_1' + \cdots + d_{t-1}'} + \cdots + a_t). \qquad (6)$$

б) Необходимое условие выполнения равенства (6) есть $d_j = d_j'$, где j пробегает $1, 2, \cdots (t-1)$.

Представим $a_1 X^{d_1 + \cdots + d_{t-1}} + \cdots + a_t$ в следующем виде:

$$((\cdots(\cdots(a_1 X^{d_1} + a_2) X^{d_2} + \cdots) X^{d_j} + \cdots) X^{d_{t-1}} + a_t).$$

Введем обозначения

$$\Gamma_j = ((\cdots (a_1 X^{d_1} + a_2) X^{d_2} + \cdots) X^{d_{j-1}} + a_j),$$

$$\Gamma_j' = ((\cdots (a_1 X^{d_1'} + a_2) X^{d_2'} + \cdots) X^{d_{j-1}'} + a_j).$$

Тогда равенство (6) примет вид $\Gamma_t = \Gamma_t' X^{\mu_t}$

Выражая Γ_t через Γ_{t-1}, получим

$$\Gamma_{t-1} X^{d_{t-1}} + a_t = (\Gamma_{t-1}' X^{d_{t-1}'} + a_t) X^{\mu_t}, \quad \text{откуда} \quad \Gamma_{t-1} = \Gamma_{t-1}' X^{\mu_{t-1}},$$

где $\mu_{j-1} = \mu_j' + d_{j-1}' - d_{j-1}$, $\mu_t = \mu$.

Используя метод полной математической индукции и условие, что U есть прямая сумма минимальных идеалов, получим

$$\Gamma_j = \Gamma_j' X^{\mu_j}, \qquad (7)$$

где $j = 2, 3, \cdots t$, для $j = 2$ получим $a_1 X^{d_1} + a_2 = (a_1 X^{d_1'} + a_2) X^{\mu_2}$.

Последнее равенство распадается на следующие два сравнения:

$$d_1 - d_1' \equiv \mu_2 \mod (b_1)$$

$$0 \equiv \mu_2 \mod (b_2).$$

Решая их совместно, получим $d_1 - d_1' \equiv c b_2 \mod (b_1)$, где c — любое целое число. Так как $(b_1, b_2) > d_1 - d_1'$, то $d_1 = d_1'$, откуда $\Gamma_2 = \Gamma_2'$.

Предположим, $\Gamma_j = \Gamma_j'$, $d_{j-1} = d_{j-1}'$. Докажем, что $\Gamma_{j+1} = \Gamma_{j+1}'$, $d_j = d_j'$. Используя (7), можно написать

$$\Gamma_j X^{d_j} + a_{j+1} = (\Gamma_j X^{d_j'} + a_{j+1}) X^{\rho_{j+1}}. \tag{8}$$

Из (8) имеем $d_j - d_j' \equiv \rho_{j+1}$, mod $[b_1, b_2, \cdots b_j]$ и $\rho_{j+1} \equiv 0$, mod (b_{j+1}). Решая их совместно, получим $d_j - d_j' \equiv c b_{j+1}$, mod $[b_1, b_2, \cdots b_j]$. Так как $d_j - d_j' < ([b_1, b_2, \cdots b_j], b_{j+1})$, то $d_j = d_j'$ и $\Gamma_j = \Gamma_j'$.

Доказательство пункта 2. Любой элемент идеала U можно представить как

$$u = u_1 + u_2 + \cdots + u_i + \cdots + u_t, \tag{9}$$

где $u_i \in U_i$.

Так как всегда можно найти $a_i \in A_i$ такое, что $u_i = a_i X^{\vartheta_i}$, то из (9) следует

$$u = a_1 X^{\vartheta_1} + \cdots + a_i X^{\vartheta_i} + \cdots + a_t X^{\vartheta_t}. \tag{10}$$

Количество различных элементов вида (10) равно произведению $b_1 \cdot b_2 \cdots b_i \cdots b_t$, где $a_1, a_2 \cdots a_t$ зафиксированы. Но количество элементов, принадлежащих циклам, представители которых имеют вид (1), равно произведению $\pi_1 \cdot \pi_2 \cdots \pi_t$, где $\pi_j = ([b_1, b_2, \cdots b_j], b_{j+1})$ — количество элементов множества D_j. Подставляя значение π_j, получим $N = b_1 \cdot b_2 \cdots b_t$, что и требовалось доказать.

Ս. Ճ. ՀՈՎՀԱՆՆԻՍՅԱՆ, Վ. Գ. ՏԱՂՋՅԱՆ

ԵՐԿՈՒԱԿԱՆ ՑԻԿԼԻԿ ԱՅԲՈՒԲԵՆՆԵՐՈՒՄ ՑԻԿԼԻԿ ՆԵՐԿԱՅԱՑՈՒՑԻՉՆԵՐԸ ԳՏՆԵԼՈՒ ՄԵԹՈԴԸ

Ա մ փ ո փ ո ւ մ

Դիտարկվում է ցիկլիկ կոդերի ուղղող հնարավորությունները հետազոտելու նպատակով այդ կոդերի կշռային սպեկտրը գտնելու խնդիրը։ Բերվում է ցիկլիկ ներկայացուցիչները գտնելու մեթոդը, որը հեշտացնում է սպեկտրի հաշվումը։

ЛИТЕРАТУРА

1. *J. M. Goethals*. IEEE Trans. on Inf. Theory, 12, № 3, 1966.
2. *Дж. Мак-Вильямс*. Кибернетический сборник, 1967.