С. Ш. ОГАНЕСЯН, В. Г. ЯГДЖЯН

ОБЪЕДИНЕНИЕ ЦИКЛИЧЕСКИХ ПРЕДСТАВИТЕЛЕЙ ПО ОДИНАКОВЫМ ВЕСАМ В БИНАРНЫХ АЛФАВИТАХ

Принятые обозначения:

n — блоковая длина алфавита,

U_i — минимальный идеал,

$h_i(x)$ — неприводимый полином над полем $GF(2)$,

$g_i(x)$ — порождающий полином идеала U_i, равный $(X^n-1)/h_i(x)$,

e_i — показатель полинома $h_i(x)$,

k_i — степень полинома $h_i(x)$,

$\varepsilon_i(x)$ — идемпотент идеала U_i,

m_i — количество циклических представителей идеала U_i, равное $(2^{k_i}-1)/e_i$,

v — буква циклического алфавита,

$\alpha_i(x)$ — примитивный элемент поля $GF(2^{k_i})$ по модулю $h_i(x)$.

Так как данная статья связана с предыдущей статьей, то более подробное объяснение принятых обозначений и понятий можно найти в предыдущей статье.

* * *

Для сокращения машинного времени при вычислении весового спектра циклического алфавита (корректирующих кодов) был дан метод нахождения циклических представителей*). Но для алфавитов с большим количеством букв машинное время, необходимое для вычисления спектра, остается неприемлемым.

К счастью, оказывается, что нет необходимости нахождения весов всех циклических представителей. Для циклических представителей алфавита, являющегося минимальным идеалом, был дан метод в работе [1] объединения циклических представителей алфавита по одинаковым весам.

В настоящей работе приводится способ объединения циклических представителей алфавита, являющегося объединением двух минимальных идеалов, при $(n, 2) = 1$.

---

*) См. настоящий сборник, стр. 35.

В конце статьи рассматривается пример, в котором хотя алфавит и содержит малое количество букв, но даже в этом случае наглядно видно, что количество различных весовых представителей существенно уменьшается.

Теорема 1. Пусть $(m_i, e_i) = 1$, тогда в качестве циклических представителей минимального идеала U_i можно выбрать

$$(0, \beta_i^0(x)\, z_i(x), \beta_i^1(x)\, z_i(x), \cdots, \beta_i^{m_i-1}(x)\, z_i(x)), \text{ где}$$

$$\beta_i(x) = z_i^{e_i}(x).$$

Доказательство. Докажем, что равенство

$$\beta_i^j(x) \cdot z_i(x) \equiv (\beta_i^{j'}(x) \cdot z_i(x))\, X^{n_i}, \quad \bmod (X^{n_i} - 1), \tag{1}$$

выполняется лишь тогда, когда $j = j'$, при любом целом значении p.

Из (1), с учетом $z_i(x) = g_i(x)\, l_i(x)$, получим

$$\beta_i^j(x)\, l_i(x) \equiv \beta_i^{j'} l_i(x) \cdot X^{n_i}, \quad \bmod (h_i(x)). \tag{2}$$

Но так как $(l_i(x), h_i(x)) = 1$ (в противном случае $z_i(x) = 0$, т. е. $U_i = 0$), то равенство (2) примет вид

$$\beta_i^{j'}(x)\,(X^{n_i} - \beta_i^{j-j'}(x)) \equiv 0, \quad \bmod (h_i(x)), \tag{3}$$

и, учитывая, что $(\beta_i^j(x), h_i(x)) = 1$ (в силу условия, что $\beta_i^j(x)$ является ненулевым элементом поля $GF(2^{k_i})$ по модулю неприводимого полинома $h_i(x)$), получим

$$X^{n_i} - \beta^{j-j'}(x) \equiv 0, \quad \bmod (h_i(x)). \tag{4}$$

Подставим в (4) $z_i^{e_i}(x) = \beta_i(x)$

$$X^{n_i} \equiv z_i^{e_i(j-j')}(x), \quad \bmod (h_i(x)). \tag{4'}$$

Так как порядок элемента X^{n_i} из поля $GF(2^{k_i})$ может принимать значения, только равные e_i/r_i, где r_i — любой делитель e_i (из-за условия, что порядок элемента X равен e_i), то порядок элемента $z_i^{e_i(j-j')}(x)$, в силу (4'), равен также e_i/r_i. Из вышеуказанного и того, что порядок $z_i(x)$ есть $(2^{k_i} - 1)$, следует

$$e_i(j - j') \cdot e_i/r_i \equiv 0, \quad \bmod (2^{k_i} - 1). \tag{5}$$

Сократим (5) на e_i и умножим на r_i:

$$e_i(j - j') \equiv 0, \quad \bmod (m_i). \tag{5'}$$

Так как $j, j' < m_i$ и $(m_i, e_i) = 1$, то из (5') следует $j = j'$.

Из того, что $j = j'$, следует, что все элементы вида $\beta_l^j(x)\,\varepsilon_l(x)$ принадлежат различным циклам, при $j = 0, 1, \cdots, (m_l^i - 1)$, т. е. элементы $\{\beta_l^j(x)\,\varepsilon_l(x)\}$ есть циклические представители идеала U_l, что и требовалось доказать.

Теорема 2. Циклическими представителями идеала $U = U_1 \cup U_2$, если $(m_1, e_1) = 1$, $(m_2, e_2) = 1$, можно выбрать

$$0,\ \{\beta_1^{j_1}(x)\,\varepsilon_1(x)\},\ \{\beta_2^{j_2}(x)\cdot\varepsilon_2(x)\},\ \{\beta_1^{j_1}(x)\,\varepsilon_1(x)\,X^d + \beta_2^{j_2}(x)\,\varepsilon_2(x)\},$$

где $j_1 = 0, 1, \cdots, (m_1 - 1)$; $\quad j_2 = 0, 1, \cdots, (m_2 - 1)$;

$$d = 0, 1, \cdots, (D - 1) \quad D = (e_1, e_2).$$

Доказательство. Доказательство теоремы 2 можно провести, используя результаты работы*) и теорему 1.

Теорема 3. Буквы v и v^2 бинарных циклических алфавитов при нечетном n имеют одинаковый вес.

Доказательство. Пусть $v = \sum_{j=0}^{n-1} a_j X^j \quad a_j \in GF(2)$, тогда

$$v^2 = \sum_{j=0}^{n-1} a_j^2 X^{2j} \equiv \sum_{j=0}^{n-1} a_j X^{2j}, \quad \bmod (X^n - 1),$$

так как $a_j^2 = a_j$ в поле $GF(2)$.

Количество ненулевых членов в полиноме v^2 не может быть больше, чем в v. Остается доказать, что

$$a_j X^{2j} \equiv a_{j'} \cdot X^{2j'}, \quad \bmod (X^n - 1), \tag{6}$$

где $a_j = a_{j'} = 1$, только при $j = j'$.

Сравнение (6) выполняется только в случае $2j \equiv 2j'$, $\bmod (n)$, но так как $(n, 2) = 1$, то получим $j = j'$, что и требовалось доказать.

На основании теоремы 3 можно разбить циклические представители идеала U_l на классы, посредством возведения их в квадрат.

Пусть ω принимает в качестве своих значений одно из чисел $\{0, 1, \cdots, (m_l^i - 1)\}$. Подстановка $\omega \to 2\omega$ разбивает множество чисел $\{0, 1, \cdots, (m_l - 1)\}$ на непересекающиеся циклы $C(m_l) = \{C_{1_l}, C_{2_l}, \cdots, C_{t_l}\}$, где t_l — количество циклов в $C(m_l)$, C_{j_l} — множество чисел в j_l-ом цикле. Обозначим f_{j_l} — число чисел в j_l-ом цикле.

Циклы $C(m_l)$ разбивают циклические представители идеала на классы следующим образом: циклу j_l соответствует класс циклических представителей вида $\{\beta_l^{C_{j_l}}(x)\,\varepsilon_l(x)\}$.

Из теоремы 3 следует, что циклические представители, принадлежащие одному классу, имеют одинаковый вес.

---

*) См. настоящий сборник, стр. 35.

Из каждого j_i-цикла выберем наименьшее число ω_{j_i} и поставим в соответствие каждому классу $\{\beta_i^{\omega_{j_i}}(x)\, z_i(x)\}$ представитель $a_{j_i} = \beta_i^{\omega_{j_i}}(x)\, z_i(x)$, называемый квадратичным представителем. Теперь видно, что для вычисления весового спектра циклических представителей минимального идеала достаточно вычисление спектра квадратичных представителей.

Наша задача — найти квадратичные представители идеала $U = U_1 \cup U_2$.

Так как квадратичные представители для минимальных идеалов U_1, U_2 войдут и в $U = U_1 \cup U_2$, то остается найти квадратичные представители для циклических представителей вида

$$\{\beta_1^{j_1}(x)\, z_1(x)\ X^d + \beta_2^{j_2}(x)\, z_2(x)\}, \text{ где } j_1 = 0, 1, \cdots (m_1 - 1)$$

$$j_2 = 0, 1, \cdots, (m_2 - 1) \quad d = 0, 1, \cdots, (D-1), \quad D = (e_1, e_2).$$

Лемма. Равенство

$$X^i \cdot (\beta_1^{j_1}(x)\, z_1(x)\, X^d + \beta_2^{j_2}(x)\, z_2(x))^{2^\nu} = (\beta_1^{j_1'}(x)\, z_1(x)\, X^{d'} + \beta_2^{j_2'}(x)\, z_2(x)), \tag{7}$$

где j_1, $j_1' < m_1$, j_2, $j_2' < m_2$, d, $d' < D$, i, ν — любые целые числа, справедливо при условиях

$$j_1 \cdot 2^\nu - j_1' \equiv 0, \mod (m_1),$$

$$j_2 \cdot 2^\nu - j_2' \equiv 0, \mod (m_2),$$

$$d \cdot 2^\nu - d' \equiv 0, \mod (D).$$

Доказательство. Раскрывая левую часть равенства (7), получим

$$\beta_1^{j_1 \cdot 2^\nu}(x)\, z_1(x)\, X^{2^\nu d + i} + \beta_2^{j_2 \cdot 2^\nu}(x)\, z_2(x)\, X^i =$$

$$= \beta_1^{j_1'}(x)\, z_1(x)\, X^{d'} + \beta_2^{j_2'}(x)\, z_2(x). \tag{8}$$

Из условия, что U является прямой суммой идеалов U_1, U_2, равенство (8) распадается на следующие равенства:

$$\beta_1^{j_1 \cdot 2^\nu}(x)\, z_1(x)\, X^{2^\nu d + i} = \beta_1^{j_1'}(x)\, z_1(x)\, X^{d'}, \tag{9}$$

$$\beta_2^{j_2 \cdot 2^\nu}(x) \cdot z_2(x)\, X^i = \beta_2^{j_2'}(x)\, z_2(x). \tag{10}$$

Из равенств (9) и (10) вытекают следующие сравнения:

$$2^\nu j_1 \equiv j_1', \quad \mod (m_1), \tag{11}$$

так как порядок $\beta_1(x)$ есть m_1,

$$2^{\mu} \cdot j_2 \equiv j_2', \mod(m_2), \tag{12}$$

так как порядок $\beta_2(x)$ есть m_2;

$$2^{\mu} \cdot d + i \equiv d', \mod(e_1), \tag{13}$$

так как период $\beta_1(x)\,\varepsilon_1(x)$ есть e_1,

$$0 \equiv i, \mod(e_2), \tag{14}$$

так как период $\beta_2(x) \cdot \varepsilon_2(x)$ есть e_2.

Решая совместно (13) и (14), получим

$$d \cdot 2^{\mu} - d' \equiv c \cdot e_2, \mod(e_1), \tag{15}$$

где c — любое целое число. Из (15) следует $d \cdot 2^{\mu} - d' \equiv 0, \mod(D)$, что и требовалось доказать.

Множество чисел $\{0, 1, \cdots, (D-1)\}$ разобьем на циклы $C(D) = \{C_{1_3}, C_{2_3}, \cdots C_{t_3}\}$ при помощи подстановки $\omega \to 2\omega$, t_3 — количество циклов в $C(D)$, C_{j_3} — множество чисел в j_3 цикле, f_{j_3} — количество чисел в j_3 цикле.

Из каждого j_3-го цикла выберем наименьшее число ω_{j_3} и поставим в соответствие ему $a_{j_3} = X^{\omega_{j_3}}$.

Теорема 4. Элементы вида

$$\{a_{j_1}^{2^{\varphi_1+\varphi_3}} \cdot a_{j_3}^{2^{\varphi_3}} + a_{j_2}\} \tag{16}$$

являются квадратичными представителями циклических представителей вида $\{\beta_1^{j_1}(x)\,\varepsilon_1(x)\,X^d + \beta_2^{j_2}(x) \cdot \varepsilon_2(x)\}$, где

$$\varphi_1 = 0, 1 \cdots, ((f_{j_1}, f_{j_3}) - 1),$$

$$\varphi_3 = 0, 1, \cdots, (([f_{j_1}, f_{j_3}]\, f_{j_3}) - 1),$$

$$j_1 = 0, 1, \cdot\cdot, t_1, \quad j_2 = 0, 1, \cdot\cdot, t_2, \quad j_3 = 0, 1, \cdots, t_3.$$

Доказательство. Доказательство теоремы 4 разобьем на две части.

а) Все квадратичные представители являются различными или, что то же самое,

$$(a_{j_1}^{2^{\varphi_1+\varphi_3}} \cdot a_{j_3}^{2^{\varphi_3}} + a_{j_2})^{2^{\mu}} = (a_{j_1'}^{2^{\varphi_1'+\varphi_3'}} \cdot a_{j_3'}^{2^{\varphi_3'}} + a_{j_2'}), \tag{17}$$

где μ — любое целое число, выполняется только в случае

$$j_1 = j_1', \; j_2 = j_2', \; j_3 = j_3', \; \varphi_1 = \varphi_1', \; \varphi_3 = \varphi_3'.$$

б) Все квадратичные представители охватывают все циклические представители.

Доказательство пункта а.

В равенстве (17) заменим a_{j_1} их значениями, тогда получим

$$(\beta_1^{\omega_{j_1}\cdot 2^{\tau_1+\tau_2}}(x)\varepsilon_1(x)X^{\omega_{j_3}\cdot 2^{\tau_3}}+\beta_2^{\omega_{j_3}}(x)\varepsilon_2(x))^{2^{\mu}}=$$

$$=(\beta_1^{\omega_{j_1}\cdot 2^{\tau_1'+\tau_3'}}(x)\varepsilon_1(x)X^{\omega_{j_3}\cdot 2^{\tau_3'}}+\beta_2^{\omega_{j_3}}(x)\varepsilon_2(x). \qquad (17')$$

Равенство (17) приводит к следующим сравнениям, исходя из леммы

$$\omega_{j_1}\cdot 2^{\tau_1+\tau_2+\mu}\equiv\omega_{j_1'}\cdot 2^{\tau_1'+\tau_3'}, \mod(m_1), \qquad (18)$$

$$\omega_{j_2}\cdot 2^{\mu}\equiv\omega_{j_2'}, \mod(m_2), \qquad (19)$$

$$\omega_{j_3}\cdot 2^{\tau_2+\mu}\equiv\omega_{j_3'}\cdot 2^{\tau_3'}, \mod(D). \qquad (20)$$

Но так как ω_{j_1} — есть элемент цикла, полученного при помощи подстановки $\omega\to 2\omega$, то из (18), (19), (20) следует: $\omega_{j_1}=\omega_{j_1'}$, $\omega_{j_2}=\omega_{j_2'}$, $\omega_{j_3}=\omega_{j_3'}$, или, что то же самое, $j_1=j_1'$, $j_2=j_2'$, $j_3=j_3'$.

Сравнения (18), (19), (20) перепишутся в виде:

$$\omega_{j_1}2^{\tau_1+\tau_2-\tau_1'-\tau_3'+\mu}\equiv\omega_{j_1}, \mod(m_1),$$

$$\omega_{j_2}2^{\mu}=\omega_{j_2}, \mod(m_2),$$

$$\omega_{j_3}2^{\tau_2-\tau_3'+\mu}\equiv\omega_{j_3}, \mod(D).$$

Степени при двойках кратны длинам циклов, поэтому

$$\tau_1+\tau_2-\tau_1'-\tau_3'+\mu\equiv 0, \mod(f_{j_1}), \qquad (21)$$

$$\mu\equiv 0, \mod(f_{j_2}), \qquad (22)$$

$$\tau_2-\tau_3'+\mu\equiv 0, \mod(f_{j_3}), \qquad (23)$$

Сравнения (21), (23) можно привести к сравнениям

$$\tau_1-\tau_1'+\tau_2-\tau_3'+\mu\equiv 0, \mod((f_{j_1}, f_{j_3})), \qquad (21')$$

$$\tau_2-\tau_3'+\mu\equiv 0, \mod((f_{j_1}, f_{j_3})), \qquad (23')$$

откуда $\tau_1\equiv\tau_1'$, $\mod((f_{j_1}, f_{j_3}))$, но так как

$$\tau_1, \tau_1'<(f_{j_1}, f_{j_3}), \text{ то } \tau_1=\tau_1'. \qquad (24)$$

Подставим (24) в (21):

$$\tau_2-\tau_3'+\mu\equiv 0, \mod(f_{j_1}). \qquad (25)$$

Имеем $f_{j_1}=h_{j_1}\cdot B$. $f_{j_3}=h_{j_3}\cdot B$, где $B=(f_{j_1}, f_{j_3})$; умножив (25) на h_{j_3}, (23) на h_{j_1}, получим

$$\mu h_{j_3}\equiv(\tau_2-\tau_3')h_{j_1}, \mod([f_{j_1}, f_{j_3}]). \qquad (26)$$

$$\mu h_{j_1} \equiv (\varphi_3 - \varphi_3') h_{j_1}, \mod ([f_{j_1}, f_{j_3}]). \tag{27}$$

Сравнения (26), (27), (22) можно привести к сравнениям

$$\mu h_{j_2} \equiv (\varphi_3 - \varphi_3') h_{j_2}, \mod (([f_{j_1}, f_{j_3}], f_{j_2})). \tag{28}$$

$$\mu h_{j_1} \equiv (\varphi_3 - \varphi_1') h_{j_1}, \mod (([f_{j_1}, f_{j_3}], f_{j_2})), \tag{29}$$

$$\mu \equiv 0, \mod (([f_{j_1}, f_{j_2}], f_{j_3})), \tag{30}$$

или

$$(\varphi_3 - \varphi_3') h_{j_2} \equiv 0, \mod (([f_{j_1}, f_{j_3}], f_{j_3})), \tag{28'}$$

$$(\varphi_3 - \varphi_3') h_{j_1} \equiv 0, \mod (([f_{j_1}, f_{j_3}], f_{j_2})). \tag{29'}$$

Учитывая, что $(h_{j_1}, h_{j_3}) = 1$, $\varphi_3, \varphi_3' < ([f_{j_1}, f_{j_3}], f_{j_2})$, получим из (28′) $\varphi_3 = \varphi_3'$, что и требовалось доказать.

Доказательство пункта б.

Найдем период квадратичного представителя (т. е. количество циклических представителей, охватываемых данным квадратичным представителем) или, иными словами, найдем наименьшее μ, при котором выполняется равенство

$$(a_{j_1}^{2^{\varphi_1 + \varphi_3}} \cdot a_{j_3} + a_{j_2})^{2^\mu} = a_{j_1}^{2^{\varphi_1 + \varphi_3}} \cdot a_{j_3} + a_{j_2}. \tag{31}$$

Равенство (31) распадается на следующие сравнения:

$$\mu \equiv 0, \mod (f_{j_1}),$$

$$\mu \equiv 0, \mod (f_{j_2}),$$

$$\mu \equiv 0, \mod (f_{j_3}).$$

Решая их совместно, получим, что наименьшее $\mu = [f_{j_1}, f_{j_2}, f_{j_3}]$.

Количество квадратичных представителей при фиксированных

j_1, j_2, j_3 равно $(f_{j_1}, f_{j_3})([f_{j_1}, f_{j_3}], f_{j_2})$.

Отсюда количество циклических представителей, принадлежащих квадратичным циклам, при фиксированных j_1, j_2, j_3, равно

$$(f_{j_1}, f_{j_3})([f_{j_1}, f_{j_3}], f_{j_2}) \cdot [f_{j_1}, f_{j_2}, f_{j_3}] =$$

$$= (f_{j_1}, f_{j_3})[f_{j_1}, f_{j_3}] f_{j_2} = f_{j_1} \cdot f_{j_2} \cdot f_{j_3},$$

что и требовалось доказать.

Пример

Найдем квадратичные циклические представители для идеала $U = U_1 \cup U_2$, где U_1 — минимальный идеал, порожденный полиномом

$$g_1(x) = (X^{63} - 1)/(x^6 + x^3 + 1),$$

U_2 — минимальный идеал, порожденный полиномом

$$g_2(x) = (X^{63} - 1)/(x^2 + x + 1),$$

тогда $k_2 = 6$, $e_2 = 9$, $m_2 = (2^{k_2} - 1)/e_2 = 7$,

$$z_2(x) = (x + 1),\ \beta_2(x) = z^3(x) = x^3 + x^2 + x,$$

$$z_2(x) = (1 + x^3) \sum_{j=0}^{6} x^{9j},$$

$$k_2 = 2,\ e_2 = 3,\ m_2 = (2^{k_2} - 1)/e_2 = 1,$$

$$z_2(x) = x,\ \beta_2(x) = z_2^3(x) = 1,$$

$$z_2(x) = (1 + x) \sum_{j=0}^{20} x^{3j},\ D = (e_1, e_2) = 3.$$

Разобьем числа m_1, m_2 и D на циклы

$C(m_1) = C(7)$

j_1	C_{j_1}			f_{j_1}	ω_{j_1}
1	1	2	4	3	1
2	3	6	5	3	3
3	0			1	0

$C(m_2) = C(1)$

j_2	C_{j_2}	f_{j_2}	ω_{j_2}
1	0	1	0

$C(D) = C(3)$

j_3	C_{j_3}		f_{j_3}	ω_{j_3}
1	1	2	2	1
2	0		1	0

Квадратичные представители для минимальных идеалов будут:

$$a_{1_1} = \beta_1^{\omega_{1_1}}(x) z_1(x) = \beta_1(x) z_1(x),\quad a_{2_1} = \beta_1^{31}(x) z_1(x)$$

$$a_{3_1} = \beta_1^{0}(x) z_1(x) = z_1(x),\quad a_{1_2} = \beta_2^{0}(x) z_2(x) = z_2(x).$$

Представителями $C(D)$ будут

$$a_{1_3} = X^{\omega_{1_3}} = X,\quad a_{2_3} = X^0 = 1.$$

Так как квадратичные представители для минимальных идеалов U_1 и U_2 войдут в $U = U_1 \cup U_2$, то остается найти квадратичные представители вида $a_{j_3}^{2^{\tau_1+\tau_2}} \cdot a_{j_3}^{2^{\tau_3}} + a_{j_3}$.

Каждому квадратичному представителю можно поставить в соответствие числа $(j_1, j_2, j_3, (\tau_1 + \tau_2), \tau_3)$.
Для

$$j_1 = 1,\ j_2 = 1,\ j_3 = 1$$

$$(f_{j_1}, f_{j_2}) = (3,2) = 1 \quad ([f^{j_1}, f^{j_2}], f_{j_3}) = ([3,2], 1) = 1,$$

откуда

$$\varphi_1 = 0, \quad \varphi_3 = 0,$$

$$\{1, 1, 1, 0, 0,\} \to a_{1_1}^{2^0} \cdot a_{1_2}^{2^0} + a_{1_3};$$

для

$$j_1 = 2, \quad j_2 = 1, \quad j_3 = 1,$$

$$(f_{j_1}, f_{j_2}) = (3,2) = 1 \quad ([f_{j_1}, f_{j_2}], f_{j_3}) = ([3,2], 1) = 1,$$

откуда

$$\varphi_1 = 0, \quad \varphi_3 = 0 \quad \{2, 1, 1, 0, 0\};$$

для

$$j_1 = 2, \; j_2 = 1, \; j_3 = 2,$$

$$(f_{j_1}, f_{j_3}) = (3,1) = 1 \quad ([f_{j_1}, f_{j_2}], f_{j_3}) = ([3,1], 1) = 1,$$

откуда

$$\varphi_1 = 0, \quad \varphi_3 = 0, \quad \{2, 1, 2, 0, 0\};$$

для

$$j_1 = 3, \quad j_2 = 1, \quad j_3 = 1,$$

$$(f_{j_1}, f_{j_3}) = (1,2) = 1 \quad ([f_{j_1}, f_{j_3}] \; f_{j_2}) = ([1,2], 1) = 1,$$

откуда

$$\varphi_1 = 0, \quad \varphi_3 = 0 \quad \{3, 1, 1, 0, 0\};$$

для

$$j_1 = 3, \quad j_2 = 1, \quad j_3 = 2,$$

$$(f_{j_1}, f_{j_3}) = (1, 1) = 1 \quad ([f_{j_1}, f_{j_2}], f_{j_3}) = ([1, 2], 1) = 1,$$

откуда

$$\varphi_1 = 1, \quad \varphi_3 = 0 \quad \{3, 1, 1, 0, 0\};$$

для

$$j_1 = 1, \quad j_2 = 1, \quad j_3 = 2,$$

$$(f_{j_1}, f_{j_3}) = (3, 1) = 1 \quad ([f_{j_1}, f_{j_3}], \quad f_{j_2}) = ([3, 1], 1) = 1,$$

откуда

$$\varphi_1 = 0, \quad \varphi_3 = 0, \quad \{1, 1, 2, 0, 0\};$$

Количество букв в данном алфавите равно $2^{k_1+k_2} = 2^8 = 256$, количество циклических представителей — 30, а количество квадратичных представителей равно 10. Для большей наглядности был приведен пример с малым количеством букв в алфавите. Для алфавитов с большим количеством букв разрыв между количеством квадратичных представителей и количеством циклических представителей довольно значительный.

Ս. Շ. ՀՈՎՀԱՆՆԻՍՅԱՆ, Վ. Գ. ՑԱՂՋՅԱՆ

ԵՐԿՈՒԱԿԱՆ ԱՂԲՅՈՒՐՆԵՐՈՒՄ ՑԻԿԼԻԿ ՆԵՐԿԱՅԱՑՈՒՑԻՉՆԵՐԻ ՄԻԱՑՈՒՄԸ ՄԻԵՎՆՈՒՅՆ ԿՇԻՌՆԵՐՈՎ

Ամփոփում

Դիտարկվում է ցիկլիկ ներկայացուցիչները քառակուսային ներկայացուցիչներին միացնելու խնդիրը, որը էապես հեշտացնում է ցիկլիկ այրուբենների ուղղող հնարավորությունների հետազոտումը։ Ապացուցված է երկու մինիմալ իդեալների միացում հանդիսացող այրուբենների քառակուսային ներկայացուցիչները գտնելու վերաբերյալ հիմնական թեորեմը, որը հեշտ է ընդհանրացնել համապատասխան սահմանափակումներին բավարարող ավելի ընդհանուր այրուբենների համար։

ЛИТЕРАТУРА

1. *J. M. Goethals*. IEEE Trans on. Inf. Theory, 12, № 3, 1966.