ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LVIII 1974 3

УДК 5198

МАТЕМАТИКА

В. И. Танрян, Г. Г. Хачатрян

К определению H-орбит циклических FG-кодов произвольной длины

(Представлено академиком АН Армянской ССР С. Н. Мергеляном 1/IV 1974)

Циклические $(n; k)$ коды могут быть рассмотрены как идеалы размерности „k" групповой алгебры FG циклической группы G порядка n над полем F. Если характеристика p поля F не делит порядок „n" группы G, то FG—алгебра полупроста, то есть разлагается в прямую сумму минимальных идеалов. Следуя [1], будем называть FG—кодом любой идеал групповой FG—алгебры. Элементы группы G образуют базис FG—алгебры и все кодовые характеристики рассматриваются в этом базисе.

В частности, вес элемента x $W(x)=\sum_{g\in G} a_g \cdot g (a_g \in F)$ равен числу ненулевых коэффициентов a_g.

Элементы произвольного FG—кода J естественным образом распадаются на орбиты по отношению к группе G. Очевидно, что все элементы одной G—орбиты имеют один и тот же вес и поэтому задача определения весового спектра кода J сводится к определению мощности G—орбит и нахождению их представителей. Аналогично можно рассматривать орбиты кода J по отношению к любой группе подстановок H базисных элементов G, переводящих код в себя.

Пусть идеал J FG—алгебры разлагается в прямую сумму идеалов

$$J=J_1 \oplus J_2 \oplus \ldots \oplus J_r.$$

Если известна структура H—орбит в прямых слагаемых J_γ ($\gamma=1; r$), то естественно ставить задачу определения структуры H—орбит идеала J.

Такое исследование произведено в настоящей работе для группы H взаимно—однозначных отображений FG—алгебры на себя, порожденной преобразованиями

$x \to gx$ ($g\in G$; $x\in FG$ алгебре)
$x \to x^p$ ($p=\mathrm{char}\, F$)
$x \to \beta^l x$ (β примитивный элемент поля F).

Элементы одной и той же H—орбиты в FG—алгебре имеют, очевидно, один и тот же вес.

Стационарные подгруппы и двойные смежные классы группы H по ним и структура H—орбит идеалов FG-алгебры. Пусть $G=(a)$ циклическая группа порядка n, F—конечное поле порядка $p^s(s\geqslant 1)$ и имеет место

$$(n,\ p^s-1)=1. \tag{1}$$

Обозначим через H_1 циклическую группу преобразований $c^i: x\to a^i x$ порядка n($x\in FG$-алгебре; $a^i\in G$; $i=\overline{1;n}$) через H_2—циклическую группу преобразований $d^i: x\to x^{p^i}$ порядка sk ($p=\operatorname{char} F$; $i=\overline{1,\ sk}$) k—показатель, которому принадлежит число q по модулю n через H_3—циклическую группу преобразований $\alpha^i: x\to\beta^i x$ порядка p^s-1 (β—примитивный элемент поля F, $i=\overline{1,\ p^s-1}$).

Согласно условию (2), как в этом нетрудно убедиться, группа $H_1'=(H_1;\ H_3)$, порождаемая циклическими группами H_1 и H_3, сама циклическая порядка $n(p^s-1)$ и в качестве ее образующего можно взять элемент $(c\alpha)$.

Тогда группу H можно рассматривать как полупрямое произведение двух циклических групп H_1' и H_2, при этом подгруппа H_1'—нормальный делитель группы H и группа H записывается следующими определяющими соотношениями $(c\alpha)^{n(p^s-1)}=1$; $d^{sk}=1$; $dc\alpha d^{-1}=c^p\alpha^p$.

Пусть n—любое натуральное число; $(n,p)=1$ и $n_1,\ldots,n_r$—суть все делители n. Тогда групповая FG—алгебра разлагается в прямую сумму минимальных идеалов размерностей $k_1,\ldots,k_r$ соответственно, где $k_i(i=\overline{1,r})$ есть минимальное натуральное число, для которого

$$q^{k_i}\equiv 1 \mod (ni) \qquad (q=p^s)$$

Рассмотрим минимальный идеал J_{k_i} размерности k_i (k_i соответствует n_i) в FG—алгебре. Пусть на J_{k_i} действует группа H. Определим стационарные подгруппы элементов $x\in J_{k_i}$ по отношению к действию H. Имеет место следующая теорема:

Теорема 1 *Подгруппы группы H, стационарные для элементов идеала J_{k_i} имеют вид:*

$$(c^{n_i})\times T$$

где

$$T=(c^l\alpha^j d^{sk_i\cdot\varphi_i^{-1}})=(c^l\alpha^j d^{sk(m_i\rho_i)-1}) \tag{2}$$

$$\rho_i/sk_i:\ l\equiv 0 \mod \varphi_1(m_i\rho_i);\ j\equiv 0 \mod \varphi_2(m_i\rho_i)$$

$$\varphi_1(\xi)=(p^{sk\xi-1}-1,n);\quad \varphi_2(\xi)=p^{(sk\xi-1,s)}-1$$

При этом каждая подгруппа вида (2) имеет порядок m_{kl} *и сопряжена с подгруппой* $A = (d^{sk(p_l-1)}) = (d^{sk(m_l p_l)-1})$.

Теорема 1 дает характеристику H—орбит в минимальном идеале. Определим теперь структуру H—орбит в прямой сумме минимальных идеалов. Согласно лемме ([2]) эта задача сводится к исследованию двойных смежных классов вида $N_i h N_j$, где $h \in H$ а N_1 и N_2 стационарные подгруппы элементов $x_1 \in J_{k_l}$ и $x_2 \in J_{k_j}$ соответственно.

Теорема 2. *Пусть* $N_i = (c^{n_i}) \times (c^{i_1} a^{j_1} d^{sk(m_l p_l)-1})$ *и* $N_j = (c^{n_j}) \times (c^{i_2} a^{j_2} d^{sk(m_j p_j)-1})$ *стационарные подгруппы элементов* $x \in J_{k_l}$ *и* $y \in J_{k_j}$ *идеалов в групповой* FG*—алгебре,* $k = m_i k_i = m_j k_j$; $q^{k_i} \equiv 1 \bmod(n_i)$ $q^{k_j} \equiv 1 \bmod(n_j)$ (n_i; n_j —делители n), $\gamma = m_i p_i, m_j p_j)$, $\rho = |m_i p_i, m_j p_j|$; $d_1 = (n_i, n_j)$ $d_2 = |n_i, n_j|$, $\varphi_1^*(\xi) = (p^{sk_i-1} - 1, d_1)$, $h = c^{i_2} a^{j_2} d^m$, $m = m_2 t + r$

$$(t = k\rho^{-1}).$$

Тогда, при каждом фиксированном r *существуют* $\eta(\gamma/i_1)$ *двойных смежных классов* N_i *и* N_j *порядка* $\rho \cdot n d_1^{-1} i_1$ (i_1—*любой делитель* γ). *Функция* $\eta(\gamma/i_1)$ *определяется следующим образом:*

$$\eta(\gamma/1) = \eta(\gamma) = \varphi_1^*(\gamma) \cdot \varphi_2(\gamma)$$

$$\eta(\gamma/i_1) = \left[\varphi_1^*(\gamma/i_1) \cdot \varphi_2(\gamma/i_1) - \sum_{\substack{j/i_1 \\ j<i_1}} j\eta(\gamma/j) \right] i_1^{-1}$$

Доказательство. Условием принадлежности элементов h_1 и h_2 группы H одному и тому же смежному классу группы H по ее полгруппам N_i и N_j является следующее:

$$n_1 h_1 n_2 = h_2 \tag{6}$$

где $n_1 \in N_i$, $n_2 \in N_j$. h_1; $h_2 \in H$

Подставляя выражения n_1; n_2; h_1; h_2 в (6), получаем

$$c^{i_1} a^{j_1} d^{sk(m_i p_i)-1 \cdot r_1} c^{\nu_1} a^{\varphi_1} d^{\psi_1} c^{i_2} a^{j_2} d^{sk(m_j p_j)-1 \cdot r_2} = c^{\nu_2} a^{\varphi_2} d^{\psi_2}$$

$$(0 \leqslant r_1 < m_i p_i; \quad 0 \leqslant r_2 < m_j p_j)$$

Необходимым условием для выполнения этого равенства является $sk(m_i p_i)^{-1} \cdot r_1 + \nu_1 + sk(m_j p_j)^{-1} \cdot r_2 \equiv \nu_2 \bmod(sk)$ или $\nu_1 \equiv \nu_2 \bmod(sk\rho^{-1})$.

Следовательно, разным остаткам r в показателях d соответствуют разные двойные смежные классы. Поэтому будем рассматривать двойные смежные классы при фиксированном r. Имеем:

$$N_i c^{i_1} a^{j_1} d^m N_j = N_i c^{i_1} a^{j_1} d^{m_3 t + r} N_j = N_i c^{i_1} a^{j_1} d^{m_3 t} \cdot N_j' d^r \tag{7}$$

где $N_j' = d^r N_j d^{-r}$.

Но порядок двойного смежного класса вида (7), очевидно, равен порядку двойного смежного класса $N_i c^{i_1} a^{j_1} d^{m_3 t} N_j'$. Наконец, так как произведение подгрупп N_i и N_j содержит элемент вида $c^{i_1} a^{j_1} d^{m_3 t}$, то можно свести исследование к рассмотрению двойных смежных классов вида

$$N_i c^i x^j N_j, \tag{8}$$

Порядок такого смежного класса определяется порядком пересечения

$$(c^{-i}x^{-j}N_i c^i x^j \cap N_j)\,\tilde{N}.$$

Ясно, что порядок $\tilde{N}$ делит величину $\gamma.\ n.\ d_2^{-1}$. Пусть A_i и A_j подгруппы порядка $\gamma.\ n.\ n_i^{-1}$ и $\gamma.\ n.\ n_i^{-1}$ групп N_i и N_j соответственно и имеют вид:

$$(c^{n_i}) \times (c^{i_1^*} x^{j_1^*} d^{sk_1^*-1}) \text{ и } (c^{n_j}) \times (c^{i_2^*} x^{j_2^*} d^{sk_1^*-1}).$$

Если i и j такие, что

$$(8)\ \begin{cases} i(p^{sk_1^*-1}-1) + i_1^* \equiv i_2^* \bmod(d_1) & (9) \\ j(p^{sk_1^*-1}-1) + j_1^* \equiv j_2^* \bmod(p^s-1), & (10) \end{cases}$$

то в этом случае порядок $\tilde{N} = \gamma.\ n.\ d_2^{-1}$ и следовательно, двойной смежный класс имеет порядок

$$(n.\ n_i^{-1}.\ n_j^{-1}.\ m_i \rho_i\ .\ m_j \rho_j)(\gamma.\ n.\ d_2^{-1})^{-1} = \rho.\ n.\ d_1^{-1}$$

Деля обе части сравнения (9) на $\varphi_1^*(\gamma)$ (так как $i_1 \equiv 0 \bmod(\varphi_1(\gamma))$: $i_2 \equiv 0 \bmod(\varphi_2(\gamma))$ а $\varphi_1^*(\gamma)$ делит $\varphi_2(\gamma)$) мы видим, что полученное сравнение имеет единственное решение по модулю $d_1|\varphi_1^*(\gamma)|^{-1}$. Следовательно, по модулю n оно имеет $n.\ d_1^{-1}\varphi_1^*(\gamma)$ решений. Аналогичным образом можно доказать, что число решений сравнения (10) относительно j равен $\varphi_2(\gamma)$. Поэтому система сравнений (8*) имеет $nd_1^{-1}.\ \varphi_1^*(\gamma) \cdot \varphi_2(\gamma)$ решений. Любой элемент вида $c^i x^j$, где i и j удовлетворяют системе сравнений (8*), порождает двойной смежный класс $N_i c^i x^j N_j$, порядок которого равен $\rho.\ n.\ d_1^{-1}$. Отсюда заключаем, что количество элементов вида $c^i x^j$, которые порождают различные двойные смежные классы вида $N_i c^i a_j \Delta N_j$, порядков $\rho.\ nd_1^{-1}$ равен

$$nd_1^{-1} \cdot \varphi_1^*(\gamma) \cdot \varphi_2(\gamma) \cdot n^{-1}d_1 = \varphi_1^*(\gamma) \cdot \varphi_2(\gamma).$$

Итак, мы доказали, что $\eta(\gamma/1) = \eta(\gamma) = \varphi_1^*(\gamma) \cdot \varphi_2(\gamma)$. Пусть i_1— любой собственный делитель величины γ. Через $\eta(\gamma/i_1)$ обозначим количество двойных смежных классов порядка $\rho \cdot n \cdot d_1^{-1} \cdot i_1$, которые соответствуют порядку пересечения $\tilde{N}$ равную $\gamma \cdot n \cdot d_2^{-1} \cdot i_1^{-1}$. Покажем, что число $i_1 \cdot n \cdot d_1^{-1} \cdot \eta(\gamma/i_1)$ равно количеству элементов вида $c^i x^j$, для которых

$$\alpha^{-1}c^{-l}A_1 c^l x^j = A_2^*,$$

где A_1^* и A_2^* подгруппы порядков $\gamma \cdot n \cdot d_2^{-1} \cdot i_1^{-1}$ групп N_l и N_j соответственно и $\alpha^{-1}c^{-l}A_1^* c^l x^j \neq A_2^*$, где A_1^* и A_2^* подгруппы групп N_l и N_j соответственно, порядок которых равен

$$n \cdot d_2^{-1} \cdot \gamma \cdot i_1^{-1} \cdot i_2 \qquad (i_2 \neq 1,\ i_2 / i_1)$$

Действительно, если для каких-то i^* и j^* имеет место:

$$a^{-j^*} c^{-i^*} B_1 c^{i^*} a^{j^*} = B_2,$$

где B_1 и B_2 подгруппы групп N_i и N_j, соответственно, порядков $n \cdot d_2^{-1} \cdot \gamma \cdot (i_1^*)^{-1}$, то $a^{-j^*} \cdot c^{-i^*} \cdot B_1' c^{i^*} a^{j^*} = B_2'$,

где B_1' и B_2' подгруппы порядков $n \cdot d_2^{-1} \cdot \gamma (i_2^*)^{-1}$ групп N_i и N_j, соответственно, где i_1^* / i_2^* $(i_1^* \neq i_2^*)$. Поэтому имеем

$$n \cdot d_1^{-1} \cdot i_1 \cdot \eta(\gamma / i_1) = n \cdot d_1^{-1} \cdot \varphi_1^*(\gamma / i_1) \cdot \varphi_2(\gamma / i_1) - n \cdot d_1^{-1} \sum_{\substack{j / i_1 \\ j \neq i_1}} j \eta(\gamma / j)$$

Этим завершается доказательство теоремы.

Прямым следствием теоремы (2) является теорема 3.

Теорема 3. *Пусть O_i и O_j соответственно орбиты для элементов $x_i \in J_{k_i}$ и $x_j \in J_{k_j}$, стационарные подгруппы которых N_i и N_j имеют порядки $m_i \rho_i \cdot n \cdot n_i^{-1}$ и $m_j \rho_j n \cdot n_j^{-1}$ соответственно, где* $k = m_i k_i = m_j k_j$

Тогда прямая сумма $O_i \oplus O_j$ распадается на $sk \rho^{-1} \cdot \eta_1(\gamma / i_1)$ орбит порядка $d_2 \cdot sk(q-1) \cdot i_1 \gamma^{-1}$, где i_1 пробегает все делители γ.

Теорема 3 допускает следующее обобщение.

Теорема 4. *Пусть J идеал в FG–алгебре разлагающиеся в прямую сумму минимальных идеалов*

$$J = J_{k_1} \oplus J_{k_2} \oplus \ldots\ldots \oplus J_{k_r},$$

где $\dim_F J_{k_i} = k_i > 1$; „k_i" –показатель q по модулю n_i; O_i –суть H–орбиты в идеалах соответственно и N_i –соответствующие им стационарные подгруппы, причем $(N_i) = m_i \rho_i \cdot n \cdot n_i^{-1}$ $(i = \overline{1,n})$

Тогда прямая сумма

$$O_1 \oplus O_2 \ldots \oplus Or$$

содержит

$$\frac{(sk)^{t-1} \cdot \eta(\gamma_1' / i_1) \cdot \eta(\gamma_2' / i_2) \ldots \eta(\gamma_r' / i_r)}{M_0 \cdot M_1 \ldots M_{r-2}} \quad \textit{орбит}$$

порядка $d_r \cdot sk(q-1) \cdot \gamma_r^{-1}$,

где $\gamma_r = (m_i \rho_i, m_j \rho_j, \ldots m_r \rho_r)$, $d_r = |n_i, n_j \ldots n_r|$ $\rho_r = |m_i \rho_i, m_j \rho_j \ldots m_r \rho_r|$, $k = m_i k_i = m_j k_j = m_r k_r$ $\gamma_l' = \gamma_{l+1} (i_1 \cdot i_2 \ldots i_l)^{-1}$ $(l = \overline{0, r-1})$ $(i_0 = 1)$ i_l–суть все делители γ_l' $M_l = |\gamma_{l-1}', \rho_l|$.

Теорема доказывается методом полной математической индукции.

Вычислительный центр Академии наук
Армянской ССР и Ереванского
государственного университета

Վ. Ի. ԹԱՐՅԱՆ, Գ. Հ. ՆԱԶԱՐՅԱՆ

Կամայական երկարության ցիկլիկ FG-կոդերի H-օրթոտաների որոշումը

Աշխատանքում ապացուցված է հետևյալ թեորեմը։

Թեորեմ 3. Ենթադրենք, O_i և O_j համապատասխանաբար $x_i \in J_{k_i}$ և $x_i \in J_{k_j}$ օրբիտաներն են, որոնց ստացիոնար ենթախմբերն ունեն համապատասխանաբար $m_i p_i n \cdot n_i^{-1}$ և $m_j p_j n n^{-1}$ կարգեր։

Այդ դեպքում $O_i \times O_j$ ուղղակի գումարը տրոհվում է $d_2 \cdot sk(q-1) i_1 \gamma^{-1}$ կարգի $sk p^{-1} \eta(\gamma/i_1)$ օրբիտաների, որտեղ i_1-ը γ-ի բոլոր բաժանարարներն են։

$\eta(\gamma/i_1)$ ֆունկցիան որոշվում է հետևյալ կերպ.

$$\eta(\gamma/1) = \eta(\gamma) = \varphi_1^*(\gamma) \cdot \varphi_2(\gamma) \qquad \eta(\gamma/i_1) = |\varphi_1^*(\gamma/i_1) \cdot \varphi_2(\gamma/i_1) - \sum_{\substack{j \mid i_1 \\ j \neq i_1}} j \eta(\gamma/j)| i^{-1}$$

որտեղ՝ $\varphi_1^*(\gamma) = (p^{sk_1} - 1, d_1)$; $\varphi_2(\gamma) = p^{(sk\gamma^{-1}, s)} - 1$ $d_1 = (n_1, n_2)$

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *С. Д. Берман*, «Кибернетика», №№ 1, 3, 1967. [2] *В. И. Тапрян*, Диссертация, ИППИ АН СССР, 1973.