ТРАДИЦИИ, ПОСОКИ, ПРЕДИЗВИКАТЕЛСТВА
Юбилейна национална научна конференция с международно участие
Смолян, 19–21 октомври, 2012

ДВОИЧНИ КОДОВЕ, ОПРЕДЕЛЕНИ ЧРЕЗ ГРУПОВ ПРЪСТЕН НА ЦИКЛИЧНА ГРУПА ОТ РЕД 35

Нели Керанова

Аграрен университет, Пловдив, България
nelikeranova@abv.bg

BINARY CODES, DEFINED BY A GROUP RING OF A CYCLIC GROUP OF ORDER 35

Neli Keranova

Agricultural university, Plovdiv, Bulgaria
nelikeranova@abv.bg

Abstract. *In this paper a code, generated with the help of group algebra of a cyclic group G of order 35 over the field GF(2), is analyzed. This code is generated by an idempotent, which is a sum of two minimal idempotents with dimension 3 and 12. The minimal distance of this code is equal to 8. The weight function of the code and the order of the group of the automorphisms are defined. The structure of the group of the automorphisms is considered.*

Key words: *code, cyclic group, idempotents, minimal distance, automorphism*

В настоящата работа конструираме код, определен върху групова алгебра над крайно поле. Основното поле, което се използва, се състои от два елемента и поради това кодът е двоичен. Групата, която определя кода, е циклична група от ред 35. Затова кодът се нарича цикличен. По-нататък в изложението ще изучаваме двоичен цикличен код, който за краткост ще наричаме само код.

Ще намерим идемпотентите на груповата алгебра KG. Нека ε е примитивен 35-ти корен на единицата. Тогава лесно се получават зависимостите:

$$\begin{aligned} \varepsilon^5+\varepsilon^{10}+\varepsilon^{20}&=1 \\ \varepsilon^{15}+\varepsilon^{25}+\varepsilon^{30}&=0 \end{aligned} \tag{1}$$

$$\varepsilon^7+\varepsilon^{14}+\varepsilon^{21}+\varepsilon^{28}=1 \tag{2}$$

Умножаваме всяко от уравненията (1) с уравнението (2) почленно и получаваме две нови съотношения:

$$\varepsilon+\varepsilon^2+\varepsilon^4+\varepsilon^8+\varepsilon^9+\varepsilon^{11}+\varepsilon^{16}+\varepsilon^{18}+\varepsilon^{22}+\varepsilon^{23}+\varepsilon^{29}+\varepsilon^{32}=0 \tag{3}$$

$$\varepsilon^3+\varepsilon^6+\varepsilon^{12}+\varepsilon^{13}+\varepsilon^{17}+\varepsilon^{19}+\varepsilon^{24}+\varepsilon^{26}+\varepsilon^{27}+\varepsilon^{31}+\varepsilon^{33}+\varepsilon^{34}=1 \tag{4}$$

Като използваме горните зависимости, както и характерите на групата G, намираме всичките 35 идемпотента над $K(\varepsilon)G$, а след като ги съберем по спрегнатост, определяме и минималните идемпотенти над KG:

$$e_0 = \sum_{g \in G} g \tag{5}$$

$$\begin{aligned} e_1 = {} & g + g^2 + g^3 + g^4 + g^6 + g^7 + g^8 + g^9 + g^{11} + g^{12} + g^{13} + g^{14} + \\ & + g^{16} + g^{17} + g^{18} + g^{19} + g^{21} + g^{22} + g^{23} + g^{24} + g^{26} + g^{27} + \\ & + g^{28} + g^{29} + g^{31} + g^{32} + g^{33} + g^{34} \end{aligned} \tag{6}$$

$$\begin{aligned} e_2 = {} & 1 + g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} + \\ & + g^{21} + g^{24} + g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} \end{aligned} \tag{7}$$

$$\begin{aligned} e_3 = {} & 1 + g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{15} + g^{16} + g^{18} + \\ & + g^{21} + g^{22} + g^{23} + g^{25} + g^{28} + g^{29} + g^{30} + g^{32} \end{aligned} \tag{8}$$

$$\begin{aligned} e_4 = {} & g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{16} + g^{18} + g^{21} + g^{22} + \\ & + g^{23} + g^{28} + g^{29} + g^{32} \end{aligned} \tag{9}$$

$$\begin{aligned} e_5 = {} & g^3 + g^6 + g^7 + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{21} + g^{24} + g^{26} + \\ & + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} \end{aligned} \tag{10}$$

където e_1 е с размерност 4, e_2 и e_3 са с размерност 3, а e_4 и e_5 са с размерност 12.

От алгебрична гледна точка всеки код е съвкупност от линейно пространство, линейно подпространство и фиксиран базис на линейното пространство. В нашия случай линейното пространство е груповата алгебра KG, линейното подпространство е идеалът KGe, базисът на линейното пространство се състои от всички елементи на групата G.

Определяме код $C = KGe$ над полето $K = Z_2$ от два елемента, като идемпотентът e, който поражда този код, избираме да е равен на сумата:

$$e = e_2 + e_4. \tag{11}$$

Следователно за кода C имаме параметри: дължина $n = 35$ и размерност $k = 3 + 12 = 15$. Ще намерим тегловния спектър, за да определим минималното разстояние на кода. Знаем, че всеки код има единствен елемент с тегло, равно на нула. Остава да определим теглата на останалите елементи, чийто брой е равен на $2^{12} - 1 = 4095$. За целта ще използваме някои свойства на кодовите думи, с чиято помощ ще сведем изчисленията до минимум, а именно:

$$d(a) = d(g^\alpha a), \;\; d(a) = d(a^{2^\alpha}), \tag{12}$$

където a е произволна дума от кода, а $\alpha \in R$ е реално число.

Имаме няколко случая при определяне вида на елементите на кода:

1 случай: Ако елементът е от вида $a = g^\alpha e_2$, то $d(a) = d(g^\alpha e_2) = d(e_2) = 20, \;\; \alpha = \overline{0,6}$. Следователно имаме седем елемента с тегло, равно на 20.

2 случай: Ако елементът е от вида $x = e_4 + ge_4$, то групираме всички степени на x в групи по модул 117, тъй като 4095 = 117.35. Тук избраният елемент има точно такъв вид, защото в степен, по-ниска от 117, която е делител на 117, не принадлежи на Ge. Имаме 12 групи съответно с представители: $e_4, x, x^3, x^5, x^7, x^9, x^{13}, x^{17}, x^{21}, x^{25}, x^{29}, x^{30}$. Намираме теглото само на представителите, а след това правим заключение на броя на съответните елементи от всяка група с какво тегло е, като използваме свойствата (12).

3 случай: Ако елементът е от вида $y = g^{\lambda} e_2 + x^{\mu}$, $\lambda = \overline{0,6}$, $\mu = \overline{0,116}$, то отново групираме елементите, както във втория случай и получаваме брой елементи със съответното им тегло.

След като обобщим резултатите от трите случая, получаваме и тегловния спектър на кода C, който изучаваме:

$$\begin{array}{rcccccccc} d = & 0 & 8 & 12 & 16 & 20 & 24 & 26 & 28 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ бр.ел. = & 1 & 70 & 3255 & 14910 & 12537 & 1540 & 420 & 35 \end{array} \qquad (13)$$

От тази схема става ясно, че минималното разстояние на кода е равно на 8. Получаваме следната основна теорема:

Теорема 1. *Нека G е циклична група от ред 35 и нека K е поле от два елемента. Нека e е идемпотент на KG, който е сума от два минимални идемпотента, съответно с размерност 3 и 12. Тогава идеалът KGe, разглеждан като код C спрямо KG с базис G, има параметри: $n = 35,\ k = 15,\ d = 8$ и тегловен спектър, даден чрез схема* (13)*, т.е. разглежданият код е от вида: [35, 15, 8].*

Сега ще изследваме групата от автоморфизмите на кода. Тя се състои от всички автоморфизми, които преобразуват елементите на кода в елементи на същия код, като запазват теглото на съответните елементи. Щом запазват теглото, следва че базисни елементи ще се преобразуват отново в базисни, тъй като само те имат тегло единица. Следователно тези автоморфизми представляват субституции и тогава групата от автоморфизмите $Aut(C)$ на кода C е подгрупа на симетричната група S_{35} от степен 35.

Ще изложим идеята за доказателство на следната основна теорема:

Теорема 2. *Групата от автоморфизмите на кода C се състои от следните субституции:*

$\alpha = (0\ 1\ 2\ 3 \ldots 34)$,

$\beta = (1\ 2\ 4\ 8\ 16\ 32\ 29\ 23\ 11\ 22\ 9\ 18)(3\ 6\ 12\ 24\ 13\ 26\ 17\ 34\ 33\ 31\ 27\ 19)(5\ 10\ 20)$
$(15\ 30\ 25)(7\ 14\ 28)$,

$\gamma = (1\ 8\ 29)(3\ 24\ 31)(4\ 11\ 18)(6\ 13\ 34)(9\ 16\ 23)(19\ 26\ 33)(14\ 21\ 28)$.

Тази група е изоморфна на директно произведение на симетричната група S_5 от пета степен и метацикличната група F от степен 21. Редът на групата $Aut(C)$ е 2520.

Доказателство: В доказателството на тази теорема за краткост означаваме с i елемента g^i.

Дефинираме автоморфизъм $\alpha : i \to i+1$, т.е. получаваме субституцията: $\alpha = (0\,1\,2\,3 \ldots 34)$. Тази се транзитивна върху всичките 35 елемента на групата G. Нулевата степен на g може да се преобразува във всички други степени, защото, ако искаме тя да се изобрази например в g^i, ще използваме субституцията α^i. Сега ще определим автоморфизъм, който запазва нулевата степен неподвижна, т.е. търсим един стабилизатор на g^0. Цялата група $Aut(C)$ се получава, като се направи разлагане по стабилизатора S, където $S = \{s \in Aut(C) / s(g^0) = g^0\}$. Това разлагане придобива вида: $Aut(C) = S + S\alpha + S\alpha^2 + \ldots + S\alpha^{34}$.

По-нататък трябва да определим елементите на кода, които образуват базис на линейното подпространство KGe. За целта взимаме всички елементи от разглеждания код, които са с тегло 8 и се представят чрез g^0 (те са известни от тегловния спектър на кода и принадлежат на KGe_4). Те са осем на брой, но повдигайки ги на втора степен, получаваме още осем елемента със същите свойства. Тогава имаме следните шестнадесет елемента:

$$
\begin{aligned}
a_1 &= 1+g^8+g^{15}+g^{18}+g^{23}+g^{25}+g^{28}+g^{30}\\
a_2 &= 1+g^7+g^{10}+g^{15}+g^{17}+g^{20}+g^{22}+g^{27}\\
a_3 &= 1+g^3+g^8+g^{10}+g^{13}+g^{15}+g^{20}+g^{28}\\
a_4 &= 1+g^5+g^7+g^{10}+g^{12}+g^{17}+g^{25}+g^{32}\\
a_5 &= 1+g^2+g^5+g^7+g^{12}+g^{20}+g^{27}+g^{30}\\
a_6 &= 1+g^3+g^5+g^{10}+g^{18}+g^{25}+g^{28}+g^{33}\\
a_7 &= 1+g^2+g^7+g^{15}+g^{22}+g^{25}+g^{30}+g^{32}\\
a_8 &= 1+g^5+g^{13}+g^{20}+g^{23}+g^{28}+g^{30}+g^{33}\\
a_9 &= 1+g+g^{11}+g^{15}+g^{16}+g^{21}+g^{25}+g^{30}\\
a_{10} &= 1+g^5+g^9+g^{14}+g^{19}+g^{20}+g^{30}+g^{34}\\
a_{11} &= 1+g^5+g^6+g^{16}+g^{20}+g^{21}+g^{26}+g^{30}\\
a_{12} &= 1+g^{10}+g^{14}+g^{15}+g^{20}+g^{24}+g^{29}+g^{34}\\
a_{13} &= 1+g^4+g^5+g^{10}+g^{14}+g^{19}+g^{24}+g^{25}\\
a_{14} &= 1+g+g^6+g^{10}+g^{15}+g^{20}+g^{21}+g^{31}\\
a_{15} &= 1+g^4+g^9+g^{14}+g^{15}+g^{25}+g^{29}+g^{30}\\
a_{16} &= 1+g^5+g^{10}+g^{11}+g^{21}+g^{25}+g^{26}+g^{31}
\end{aligned}
\qquad (14)
$$

за които чрез проверка установяваме, че имат сума равна на нула. Това от своя страна означава, че те са линейно зависими. Тъй като размерността на KGe_4 е 12, то само 12 от тях ще са линейно независими, а размерността на кода е 15. Следователно, трябва да определим още три елемента, принадлежащи на KGe_2, които са линейно независими, а заедно с горните 12, поради директната сума $KG = KGe_2 \oplus KGe_4$, следва, че те ще са базисни. Такива са следните елементи:

$$y_0 = e_2 + e_4,\ y_1 = gy_0,\ y_2 = g^2 y_0 \qquad (15)$$

По-нататък в изложението дефинираме автоморфизъм: $\beta : i \to 2i$, който съхранява нулевата степен на елемента g неподвижна и получаваме субституцията

$$
\begin{aligned}
\beta = &(1\ 2\ 4\ 8\ 16\ 32\ 29\ 23\ 11\ 22\ 9\ 18)(3\ 6\ 12\ 24\ 13\ 26\ 17\ 34\ 33\ 31\ 27\ 19)\\
&(5\ 10\ 20)(15\ 30\ 25)(7\ 14\ 28),
\end{aligned}
\qquad (16)
$$

която съвпада с тази от условието на теоремата.

Дефинираме и автоморфизъм γ по следния начин

$$\gamma = (1\ 8\ 29)(3\ 24\ 31)(4\ 11\ 18)(6\ 13\ 34)(9\ 16\ 23)(19\ 26\ 33)(14\ 21\ 28) \tag{17}$$

така, че и трите автоморфизма принадлежат на групата от автоморфизмите на кода. Редът на всяка от горните субституции е: α - от ред 35, β - от ред 12, γ - от ред 3. Ако допуснем, че има други субституции, принадлежащи на $Aut(C)$, то те ще пораждат S_4, а в S_4 има само една такава, която е от ред три. Щом групата, породена от тези субституции съдържа субституции от редове три и четири, то нейният ред ще бъде кратен на 12, т.е. ще бъде или 12, или 24. От ред 12 е алтернативната група от четвърта степен, но тя не съдържа елемент от ред 4, а съдържа само от редове 2 и 3, а в нашия случай от ред 4 е β^3. Следователно разглежданата група остава да бъде от ред 24, а именно групата S_4. Тогава за реда на групата $Aut(C)$ получаваме:

$$|Aut(C)| = |\alpha|.|S_4|.|\gamma| = 35.24.3 = 2520 \tag{18}$$

Остава да изследваме структурата на групата $Aut(C)$. За целта въвеждаме следните означения:

$$a = \alpha^5,\ b = \alpha^7 \tag{19}$$

и дефинираме групите:

$$M = \langle \alpha^5, \beta, \gamma \rangle,\ N = \langle \alpha^7, \beta, \gamma \rangle \tag{20}$$

Определяме хомоморфизмите:

$$\phi : Aut(C) \to S_5,\ \psi : Aut(C) \to S_7 \tag{21}$$

като доказваме, че $A = Ker\varphi = \langle \alpha^5, \beta^4 \rangle$ и е от ред 21 и $B = Ker\psi = \langle \alpha^7, \beta^3, \gamma \rangle$ от ред 120 . Тъй като от „Теория на групите“ е известно, че ядрото на всеки хомоморфизъм е нормален делител на съответната група, то A и B са нормални делители на $Aut(C)$ (Хол, 1959). Лесно се проверява, че тези две групи удовлетворяват условията: $A \cap B = E,\ A.B = Aut(C)$, то

$$|A.B| = \frac{|A|.|B|}{|A \cap B|} = 2520 = |Aut(C)|. \tag{22}$$

Следователно (Хол, 1959)

$$Aut(C) = A \times B \tag{23}$$

Установяваме, че групата A е изоморфна на метацикличната група F, а групата B - на симетричната група от пета степен S_5. Тогава, от (23), получаваме

$$Aut(C) \cong F \times S_5 \tag{24}$$

С това завършваме накратко изложеното доказателство на втората теорема от настоящата работа.

Така определихме вида на разглеждания код, реда на групата от автоморфизмите му, както и нейната структура. Това са едни от основните характеристики на даден код.

Литература

Хол, Маршал. Теория на групите.// Максимилиан къмпъни, 1959, с. 33, с. 56.