BINARY CODES, DEFINED BY A GROUP RING OF A CYCLIC GROUP OF ORDER 15

Neli Keranova
Agricultural University
4000, Plovdiv, Bulgaria,
nelikeranova@abv.bg

ABSTRACT

In this paper a code, generated with the help of group algebra of cyclic group G of order 15 over the field GF(2), is analyzed. This code is generated by an idempotent, which is a sum of two minimal idempotents, each of them with dimension 4. The minimal distance of this code is equal to 4. The weight function and the order of the group of the automorphisms are defined. The structure of the group of the automorphisms is considered. This group is represented by subgroups of substitutions.

Key words: *idempotent, code, automorphism, dimension, distance*

Some notes:

KG – group algebra of the group G over the field K;
[G:H] – index of the subgroup H in the group G;
e – idempotent of the KG;
[n, k, d] - linear code with length n , dimension k and minimal distance d;
Aut (C) – the group of the automorphisms of the code C.

Main results:

It is easy to obtain, that the $x^{15}-1$ is represented by the follow way:

$$x^{15}-1=(x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)$$

over the field K=Z_2 .

We define the idempotents of the group algebra KG by characters. We obtain the minimal idempotents, which are idempotents over KG, as for this aim we add the conjugated idempotents over $K(\varepsilon)G$, where ε is a primitive fifth /correspond to third or fifteenth/ root of the unit. All the minimal idempotents over the considered group algebra KG are:

$e_0=1+g+g^2+g^3+g^4+...+g^{13}+g^{14}$ with dimension 1
$e_1=g+g^2+g^4+g^5+g^7+g^8+g^{10}+g^{11}+g^{13}+g^{14}$ with dimension 2
$e_2=g+g^2+g^3+g^4+g^6+g^7+g^8+g^9+g^{11}+g^{12}+g^{13}+g^{14}$ with dimension 4
$e_3=g+g^2+g^3+g^4+g^6+g^8+g^9+g^{12}$ with dimension 4
$e_4=g^3+g^6+g^7+g^9+g^{11}+g^{12}+g^{13}+g^{14}$ with dimension 4.

We know, that each code is a set of linear space, linear subspace and a fixed basis of the linear space. In our case, the linear space is the group algebra , the subspace is the ideal KGe, where e is idempotent, which is equal to the sum $e=e_3+e_4$ and is with dimension 8. The basis consists the all elements of the group G .

Let $A\in C$ is a arbitrary element of the code C . Then
$A=g^{\lambda}e_3+g^{\mu}e_4=g^{\lambda}(e_3+g^{\mu-\lambda}e_4)$.

Hence, $g^{-\lambda}A=e_3+g^{\nu}e_4,\ \nu=\mu-\lambda,\ \lambda,\mu=\overline{0,14}$.

We will define the weight of each element of the code, as we define only the weight of the representatives of the cosets, after that we use the following properties of the code's words: $d(A) = d(A^{2^{\alpha}})$, $d(A) = d(g^{\lambda} A),\ \lambda = \overline{0,14}$.
The obtained results are moved in the table:

Representatives of the coset	Number of the elements	Weight of the elements
$g^{\lambda} e_3$	15	8
$g^{\mu} e_4$	15	8
$e_3 + g e_4$	60	10
$e_3 + g^3 e_4$	60	6
$e_3 + g^5 e_4$	30	4
$e_3 + g^7 e_4$	60	8
$g^{\alpha}(e_3 + e_4)$	15	8
0	1	0

As the dimension of the code is 8, then the code consists $2^8 = 256$ elements. We can write the weight spectrum of the considered code:

$$\begin{array}{lcccccc} & d = & 0 & 4 & 6 & 8 & 10 \\ (1) & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & \text{el.} = & 1 & 30 & 60 & 105 & 60 \end{array}$$

From (1) it follows, that the minimal distance of the code is equal to 4. Therefore, we have [15, 8, 4] – linear code. So we obtain the following basic theorem:

Theorem 1. Let G be a cyclic group of order 15 and let K be a field of two elements. Let e is an idempotent of KG, which is a sum of two minimal idempotents, each of them with dimension 4. Then the ideal KGe, considered as a code C regarding KG with basis G, has parameters: $n = 15,\ k = 8,\ d = 4$ and weight spectrum, which is given with the scheme (1).

A group of the automorphisms of the code C

The group of the automorphisms of the code consists the automorphisms of the whole space, which preserves the lengths of the elements of the linear space and maps the code into itself.

Further in this paper we will write only k instead g^k. Then, if φ is an arbitrary automorphism of the code, then it should satisfy the conditions:
1. $\varphi(x) \in C, \quad x \in C$;
2. $d(x) = d(\varphi(x))$, $x \in C$;
3. $\varphi(x + y) = \varphi(x) + \varphi(y)$, $x, y \in C$.
The condition $\varphi(\lambda x) = \lambda \varphi(x),\ \lambda = 0, 1$, we verify directly.

The map φ saves the lengths of the elements. Because, only the elements of the basis have weight 1, then they are maped again into basis elements. We will find the substitutions, which are satisfied the upper conditions. In the substitutions, which we will consider, only the positions of the powers of the element g change places. One substitution, which corresponds to the map $\varphi(k) = k + 1$, is:

$\alpha = (0\ 1\ 2\ 3\ 4\ 5\ 6\ ....\ 14)$.

Let's take an arbitrary element with length 4. From it, by multiplication with the corresponding powers of g, we will obtain four elements with lengths 4, which consist the unit. We raise to second power each of them and again we obtain four elements. We have eight elements, which are with length 4 and consist 1. We will prove, that these elements are linear independent and because the dimension of the code is 8, then they form a basis. We obtain the elements:

$$\begin{aligned}
&a_1 = 1 + g^7 + g^{10} + g^{12}, \quad a_2 = 1 + g^3 + g^{10} + g^{13},\\
(2)\qquad &a_3 = 1 + g^2 + g^5 + g^{12}, \quad a_4 = 1 + g^3 + g^5 + g^8,\\
&a_5 = 1 + g^5 + g^9 + g^{14}, \quad a_6 = 1 + g^5 + g^6 + g^{11},\\
&a_7 = 1 + g^4 + g^9 + g^{10}, \quad a_8 = 1 + g + g^6 + g^{10}.
\end{aligned}$$

Each of them we interpret as a vector and the coefficients before the powers of g - its co-ordinates. We put the co-ordinates in a matrix, which consists of 8 rows and 15 columns. In the left half we obtain the unit matrix. Hence, these eight elements are linear independent. Since, they are basis.

We form a subgroup H of the group of the automorphisms, which consists all substitutions, which save static the power 0 of the element. If β is a representative of this subgroup, then

$\beta = (1\ 2\ 4\ 8)(3\ 6\ 12\ 9)(5\ 10)(7\ 14\ 13\ 11)$.

We note with H_1 the subgroup of H, which saves static the 0, 5-th and 10-th powers of the element g. Then

$\gamma = (2\ 14)(3\ 6)(4\ 7)(8\ 11)(9\ 12)(1\ 13)$

is a representative of this subgroup.

Let H_2 be a subgroup of H_1, which saves static the 0, 5-th, 10-th and 3-rd powers of the element g. Then

$\delta = (1\ 4\ 7)(2\ 11\ 14)(6\ 9\ 12)$.

Let H_3 is a subgroup of H_2, which saves the abovementioned powers and the 6-th power. Then :

$\eta = (2\ 14)(4\ 7)(9\ 12)$.

The last subgroup H_4, which saves all powers of the element g, has a representative the identical substitution. We calculate the indexes of each subgroup:

$[AutC : H] = 15, [H : H_1] = 2, [H_1 : H_2] = 4, [H_2 : H_3] = 3, [H_3 : H_4] = 2, [H_4 : E] = 1$.

Then the order of the group of the automorphisms of the code is:

$| AutC | = 15.2.4.3.2.1 = 720$.

Further in this paper we consider the following substitutions:

$a = \alpha^3 = (0\ 3\ 6\ 9\ 12)(1\ 4\ 7\ 10\ 13)(2\ 5\ 8\ 11\ 14)$

and

$b = \alpha^5 = (0\ 5\ 10)(1\ 6\ 11)(2\ 7\ 12)(3\ 8\ 13)(4\ 9\ 14)$.

We note $N = \langle \alpha, \beta, \gamma, \delta \rangle$ the group, which is generated by a and b .Then the order of N is equal to 360. We form the group $K = \langle a, \beta, \gamma, \delta \rangle$. Since the order of K is 120, then we have three cosets: K, Kb, Kb^2. If $\varphi : K \to S_3$, is a homomorphism, by which of arbitrary element of K corresponds a substitution of three elements, then

(3) $$\varphi(x)=\begin{pmatrix} K & Kb & Kb^2 \\ Kx & Kbx & Kb^2x \end{pmatrix}.$$

We consider for each of elements of K what kind of substitution corresponds. For example: for $x=\alpha^3$: $K\alpha^3=K$, because $\alpha^3\in K$. By analogy, we obtain, that $\varphi(\alpha^3)=E$.

Further we repeat similarly for $\beta\in K$, when $Kb\beta=Kb\beta^{\lambda}$, $\lambda=1{,}2$. Again by verification determine, that $Kb\beta=Kb^2$, hence $\varphi(\beta)=(1\ 2)$.

Analogically follows, that $\varphi(\gamma)=E$, $\varphi(\delta)=E$. Then $\alpha^3,\ \beta^2,\ \gamma,\ \delta\in Ker\varphi$. Therefore, the order of the kernel $Ker\varphi$ is equal to 60.

We define the group $L=\left\langle\alpha^5,\ M\right\rangle$, where we note $M=Ker\varphi$. The order of L is 180. We know, that, if one subgroup is of order 2 in given group, then it is invariant subgroup. Then L is invariant subgroup in N. By analogy we obtain, that K is invariant in L, too. We have the succession:

$$Aut(C)\geq N\geq L\geq K\geq M\ .$$

Then the order of indexes of the $Aut(C)$ is: 2, 2, 3, 60.

Let's take the following elements of the group M :

(4) $$x_1=\alpha^{-3}\delta\alpha^3,\ x_2=\alpha^{-3}\beta^2\alpha^3,\ x_3=\gamma\ .$$

By direct verification is established, that these three elements satisfy the conditions of the Alternative group:

$$A_5=\left\{x_1^3=1,\ x_2^2=1,\ x_3^2=1,\ (x_1x_2)^3=1,\ (x_1x_3)^2=1,\ (x_2x_3)^3=1\right\}.$$

Therefore, both groups are isomorphic. We verify, that M is invariant subgroup in L and each element of L is product of elements of M and $\left\langle b\right\rangle$. Hence L is direct product of the groups M and $\left\langle b\right\rangle$.

References:

1. MacWilliams, F. J., Sloane, N. J. A. 1979, The theory of error-correcting codes , (Russian), Moscow, Connection
2. Hall, M. J. , 1959, The theory of groups, New York, Maximilian