***Intelligent Information Management*, 2012, 4, 309-310**
doi:10.4236/iim.2012.425043 Published Online October 2012 (http://www.SciRP.org/journal/iim)

Automorphism of Cyclic Codes

Naser Amiri
Department of Mathematices, Payame Noor University, Tehran, Iran
Email: n_amiri@pnu.ac.ir

Received July 24, 2012; revised August 27, 2012; accepted September 14, 2012

ABSTRACT

We investigate how the code automorphism group can be used to study such combinatorial object as codes. Consider *GF*(q^n) as a vector over *GF*(*q*). For any $k = 0, 1, 2, 3, \cdots, n$. Which *GF*($q^n$) exactly one subspace *C* of dimension *k* and which is invariant under the automorphism.

Keywords: Code; Cyclic Code; Automorphism

1. Introduction

There are many kind of automorphism group in mathematics. Among them such automorphism group as a code automorphism, (see [1-3]) design automorphism is important to combinatories. These automorphism groups play a key role in determining the corresponding structure, and provide a playground to study elementary algebra. In particular, code automorphism group is useful in determining the structure of codes, computing weight distribution, classifying codes, and devising decoding algorithm, and many kinds of code automorphism group algorithms. In this paper, we will investigate how the code automorphism group can be used to study some combinatorial structures.

2. Codes and Code Automorphism Group

Let *F* be a finite field. Any subset *C* of F^n is called an *q*-array code where $F = GF(q)$. If *C* is a subset of F^n, then *C* is called a linear code. In this section we introduce basic definition related to code automorphism group, and introduce some computation to find the weight distribution of a code using its automorphism group.

Definition 2.1. Let *C* be a binary code of length *n*. The binary code of length of $n + 1$ obtained from *C* by adding check bit is called the extended code of *C*. The permutation of coordinate place which send *C* into itself from the code automorphism group of *C* denoted by Aut(*C*). Two binary codes C_1 and C_2 are equivalent if there is a permutation of coordinate place which sends C_1 onto C_2.

If $C \in \left(GF(q)\right)^n$ is a none binary code, Aut(*C*) consists of all monomial matrix *A* over *GF*(*q*) such that $v \in C$ for all $v \in C$. Note that if two binary codes C_1 and C_2 are equivalent, then Aut(C_1) and Aut(C_2) are isomorphic. But the converse may not always hold. Let *C* be a binary code and H be a subgroup of Aut(*C*). For a codeword $v \in C$, the number of 1 in the coordinate place of *v* is the weight of *v* and denoted by $wt(v)$. Usually N_i denotes the number of codewords in C of weight *i* and $N_i(H)$ the number of codewords which are fixed by some element of *H*. Now, we will investigate a method of using the automorphism of group to find out the weight distribution of a given code *C*.

Theorem 2.2. Let *C* be a binary code and H be a subgroup of Aut(*C*). Then $N_i \equiv N_i(H)$ (mode *O*(*H*)).

Proof. The codewords of weight *i* can be divided into two classes those fixed by some element of *H*. If $v \in C$ is not fixed by any element of *H* then the *O*(*H*) codeword $g \times v$ for *g* in *H* must be distinct. Then $N_i - N_i$ (*H*) is multiple of *O*(*H*).

Recall that an action of a group on a set *X* is the function $f : G \times X \to X$ such that $f(g, x)$ is denoted by gx and with the following properties. $\left((g_1 g_2)x = g_1(g_2 x)\right)$ and ($ex = x$). If *x*, *y* are in *X*, we say that $x \sim y$ if there is g in *G* such that $y = gx$. And if *x* in *X*, we defined $G_x = \{ g | gx = x \}$ is called the isotropy or (stabilizer) subgroup of *G*, or subgroup fixing by *x*.

Definition 2.3. Let *C* be a binary code of length n and *G* is a subgroup of Aut(*C*). Then G acts on the coordinate place $X = \{1, 2, 3, \cdots, n\}$. A subset $Y = \{C_1, C_2, \cdots, C_K\}$ of *X* is called a coordinate base for *G* provided that the identity element fixes all the coordinate places for *G* provided that the identity element fixes all the coordinate places c_i.

A strong generators for *G* on *X* relative to the ordered coordinate bases $\{C_1, C_2, \cdots, C_K\}$ is a generating set *S* for *G* such that $G_{c_1 c_2 \cdots c_j}$ is generating by $S \cap G_{c_1, c_2, \cdots, c_j}$, for $j = 1, 2, 3, \cdots, t$.

Let $G^j = G_{c_1 \cdots c_j}$, $G^0 = G$ and $\Delta_j = \left[G^{j-1} : G^j\right]$, for $j = 1, 2, \cdots, k$. Note that $O(\text{Aut}(\text{C})) = \prod \Delta_J$, when

$G = \mathrm{Aut}(C)$.

Definition 2.4. A Hadamard matrix H of order n is an $n \times n$ matrix of 1 and –1 such that $HH^T = H^T H = nI_n$. Two Hadamard matrix are equivalent if one can obtained from other by permutating rows and column and multiplying rows and columns by −1.

Let H be 4m × 4m Hadamard matrix and $N(H)$ be the matrix obtained from H by deleting the first row and column. Now let A_H and $A_{N(H)}$ be the matrices obtained from H and N_H respectively by replacing 1 with 0. Let C_H and ${}_{N(H)}$ be the binary codes generated by the rows of A_H and $A_{N(H)}$ respectively.

Theorem 2.5. Let H be a 4m × 4m normalized Hadamard matrix and m be an even integer. Then C_H is the extended code of $C_{N(H)}$.

Proof. Let E be the extended code of $C_{N(H)}$. Note that $A_{N(H)}$ is an incidence matrix of a (4m – 1, 2m – 1, m – 1) design (*i.e.* 4m – 1 point a set of b block. Each block has 2 m – 1 point. Every 2 point lie on exactly m – 1 block). With b = 4m – 1 = ν. Note that the number of 1 in each row of $A_{N(H)}$ is also m – 1, since $A_{N(H)}$ is an incidence matrix and ν = b. Also the sum of all rows of $A_{N(H)}$ is an all one vector since m – 1 is an odd integer. Thus all one vector of length 4m is in E, and the length 4m vector is also in E. Note that those vector generate E, an each row of A_H is an element of E. Hence C_H is the extended code of $C_{N(H)}$.

3. Cyclic Codes

Let V be the n-dimensional vector space $(n \geq 2)$ over the finite field Z_{p^m} or $\left(GF\left(p^m\right)\right)$ and ϕ the endomorphism which causes a cyclic shift of coordinate according to a given bases $\beta = \{ e_0, e_1, \cdots, e_{n-1} \}$.

$\phi(a_0, a_1, \cdots, a_{n-1}) = (a_{n-1}, a_0, \cdots, a_{n-2})$. We consider the n-dimensional linear space generated by the elements of $GF\left(p^{mn}\right)$ as a vector space over $GF\left(p^m\right)$ and take the bases β a normal bases

$\beta = \left\{ e_0 = a, e_1 = \sigma(a), \cdots, e_{n-1} = \sigma^{n-1}(a) \right\}$. Where

$\sigma(a) = a^{p^m}$, $a \in GF\left(p^{mn}\right)$.

Definition 3.1. A k-dimensional linear subspace C of V is called cyclic code if for all $a \in V$ as a in C then $\phi(a)$ in C.

We will recall that $V = GF\left(p^m\right)[x] / \langle x^n - 1 \rangle$, and C is a cyclic code iff C is an ideal of $GF\left(p^m\right)[x] / \langle x^n - 1 \rangle$. The generator polynomial g of C is the monic polynomial of lowest degree in the ideal, g is a divisor of x^n – 1 and dimension(C) = $n - \deg\left(g(x)\right)$, and $\left\{ g, xg, x^2 g, \cdots, x^{(n-\deg-1)} \right\}$ is a bases of C.

Recall that $\mathrm{ord}_n\left(p^m\right)$ is the order of p^m in Z_n. And $Q_n(x)$ the nth cyclothymic polynomial. We have $x^n - 1 = \prod\left(Q_n(x)\right)$.

Proposition 3.2. Let $V = GF\left(p^m\right)[x] / \langle x^n - 1 \rangle$, and $n = p^a b$ with $(p, b) = 1$. Then we have: (1) If b = 1 or $b = p^a + 2$ is a prime and $\mathrm{orb}_b\left(p^m\right) = \phi(b)$, where ϕ is the Uler function, then for any $k = 1, 2, \cdots, n$ exists exactly one cyclic code of dimension k.

Proof. If b = 1, then for $t = 0, 1, \cdots, p^a$. Then only cyclic code of dimension t is $x^n - 1 / \left(Q_1(x)\right)^t$. If $b = p^a$ + 2 where b is prime with $\mathrm{orb}_b\left(p^m\right) = \phi(b)$, then for $t_1, t_2 = 0, \cdots, p^b$ the only cyclic code of dimension $t_1 + \left(p^b + 1\right) \times t_2$ is $\dfrac{\langle x^n - 1 \rangle}{Q_1(x)^{t_1} \times Q_2(x)^{t_2}}$.

Theorem 3.3. Let $GF\left(p^{nbp^a}\right)$ be a vector space over $GF\left(p^n\right)$. Then for any $k = 0, \cdots, p^a$ there is exactly one cyclic code of dimension k which is invariant under the automorphism $GF\left(p^n\right)$ if and only if b = 1 or $b = p^n + 2$.

Proof. It is clearly.

4. Acknowledgements

I would like to thank the referees for their valuable common and suggestion leading to this improved version of the paper.

REFERENCES

[1] A. A. Andrad and R. Palazzo Jr., "Constraction and Decoding of BCH Codes over Finite Commutative Ring," *Linear Algebra and Its Applications*, Vol. 286, 1999, pp. 69-85.

[2] A. A. Andrad and R. Palazzo Jr., "On Coding Collineating Graphs Of Symmetric Block Design," *Journal of Combinatorial Theory*, Vol. 11, No. 3, 1971, pp. 272-281.

[3] R. C. Bose and D. K. Ray-Chaudhuri, "On a Class of Error-Correcting Binary Group Codes," *Information and Control*, Vol. 3, No. 1, 1960, pp. 68-79.