Trakia Journal of Sciences, Vol. 7, Suppl. 2, pp 121-124, 2009

Available online at:
http://www.uni-sz.bg

ISSN 1313-7050 (print)
ISSN 1313-3551 (online)

Original Contribution

THE RELATION BETWEEN THE $(1-u^2)$- CYCLIC CODES OVER $F_{p^k}+uF_{p^k}+u^2F_{p^k}$ AND THE CODES OVER F_{p^k}

Yasemin Cengellenmis*

* Department of Mathematics, Trakya University, Edirne, TURKEY

ABSTRACT

One of the most important problems of coding theory is to construct codes with best possible minimum distances. A new map for $(1-u^2)$-cyclic code over $A=F_{p^k}+uF_{p^k}+u^2F_{p^k}$, $k\in N$, $u^3=0$ was introduced in [2]. In this paper, via this map, the relation between the linear $(1-u^2)$-cyclic codes over A and the code over F_{p^k} is established. In this way, it may be obtained the new linear codes over F_{p^k}, by using computer as in [4] and [5] .

Key Words: *coding theory, codes, best minimum distances*

INTRODUCTION

In [1], Christine Bachoc introduced the linear codes over F_p+uF_p p is a prime. In [4], a Gray map for codes over F_3+uF_3 was introduced and the relation between the codes over F_3+uF_3 and F_3 was established, via this map. Using this relation, new linear codes over F_3 was found. Later, for R is finite commutative ring with identity, a Gray map for codes over

$R_a=R+uR+u^2R+.....+u^{m-1}R$,

$u^m=a$, $a\in R$, $m\in N$, u is an indeterminate was introduced[1]. Via this map, the relation between the codes over R_a and R was established in [5]. By using computer, it is obtained the new linear codes over F_5. A new Gray map on A was introduced in [2]. In this paper, the relation between the linear $(1-u^2)$-cyclic codes over A and the codes over F_{p^k} is established via this map.

PRELIMINARIES

Let R be a finite commutative ring with identity. Let $n\in N$. An R- submodule of R^n is called a linear code of length n over R.

Let $\rho : R^n \times R^n \longrightarrow N\cup\{0\}$ be distance function. For $E\subset R^n$, let $\rho(E)=\min\{\rho(x,y)\,|\,x\neq y \text{ and } x,y\in E\}$.

A linear code C of length n is said to be an (n,M)-linear code if and only if $|C|=M$. Morever if $\rho(C)=d$ then C will be called an (n,M,d) –linear code, $\rho(C)$ is called the minimum distance of C with respect to ρ. Furthermore , if C is a s-free submodule with minimum distance d, length n, then C is called [n,s,d]-linear code. The Hamming weight of a codeword $c=(c_1,c_2,...c_n)$, $w_H(c)$ is the number of nonzero entires of c. Also the Hamming weight of a codeword can be defined to be the sum of the weights of its components,

[1]***Correspondence to**: *Yasemin Cengellenmis, Department of Mathematics, Trakya University, Edirne, TURKEY ;*
e-mail: ycengellenmis@yahoo.com

say

$$w_H(c) = \sum_{i=0}^{n} w_H(c_i) \qquad (1)$$

Where $w_H(c_i)$ is zero if $c_i = 0$ and 1 otherwise. The Hamming distance of two codewords c, e denoted by $d_H(c,e)$ is the Hamming weight of their difference.

Let A be the commutative ring $F_{p^k} + uF_{p^k} + u^2F_{p^k}$ where $k \in N$, $u^3 = 0$ and $F_{p^k} = GF(p^k)$. The ring is endowed with the obvious addition and multiplication with the property that $u^3 = 0$. Then A is a finite chain ring with maximal ideal uA and residue field F_{p^k}.

Let the C be a code of length n over A. Let ν be maps from A^n to A^n given by

$$\nu : A^n \longrightarrow A^n \qquad (2)$$
$$(r_0,.....,r_{n-1}) \mapsto ((1-u^2)r_{n-1}, r_0.....,r_{n-2})$$

Then C is said to be $(1-u^2)$- cyclic if $\nu(C) = C$.

Let $P(C) = \{\sum_{i=0}^{n-1} r_i x^i \,|\, (r_0,.....,r_{n-1}) \in C\}$ be code C's polynomial representation. A code C of length n over A is $(1-u^2)$- cyclic if and only if $P(C)$ is an ideal of $R[x]/\langle x^n - (1-u^2)\rangle$.

Let $a \in F_{p^k}^{p^{2k}n}$ with

$$a = (a_0, a_1,...,a_{p^{2k}n-1}) = (a^{(0)} \,|\, ... \,|\, a^{(p^{2k-1}-1)}),$$

$a^{(i)} \in F_{p^k}^{pn}$ for all $i = 0,1,....,p^{2k-1}-1$. Let $\sigma^{\otimes p^{2k-1}}$ be the map from $F_{p^k}^{p^{2k}n}$ to $F_{p^k}^{p^{2k}n}$ given by

$$\sigma^{\otimes p^{2k-1}} : F_{p^k}^{p^{2k}n} \longrightarrow F_{p^k}^{p^{2k}n}$$
$$a \mapsto$$
$$\sigma^{\otimes p^{2k-1}}(a) = (\tilde{\sigma}(a^{(0)}) \,| \,..... \,|\tilde{\sigma}(a^{(p^{2k-1}-1)})) \qquad (3)$$

Where $\tilde{\sigma}$ is the usual cyclic shift $(c_0,...,c_{pn-1}) \mapsto (c_{pn-1}, c_0,.....,c_{pn-2})$ on $F_{p^k}^{pn}$. A code $\tilde{C}$ of length $p^{2k}n$ over F_{p^k} is said to be quasi-cyclic codes of index p^{2k-1} if $\sigma^{\otimes p^{2k-1}}(\tilde{C}) = \tilde{C}$ [2].

In [3], a homogeneous weight on arbitrary finite chain rings is defined; we give it here for the case of the ring $A = F_{p^k} + uF_{p^k} + u^2F_{p^k}$.

The homogeneous weight of $r \in A$ is given by

$$w_{\hom}(r) = \begin{cases} p^{2k} & if\ r \in Au - \{0\} \\ p^{2k} - p^k & if\ r \in A - Au \\ 0 & otherwise \end{cases} \qquad (4)$$

This extends to a weight function in A^n. If $c = (c_0,.....,c_{n-1}) \in A^n$, then

$$w_{\hom}(c) = \sum_{i=0}^{n-1} w_{\hom}(c_i) \qquad (5)$$

The homogeneous distance $d_{\hom}(x,y)$ between any distinct vectors $x, y \in A^n$ is defined to be $w_{\hom}(x-y)$.

Any element $\varepsilon \in Z_{p^k}$ has p-adic representation

$$\gamma_{0,\varepsilon} + \gamma_{1,\varepsilon} p + ... + \gamma_{(k-1),\varepsilon} p^{k-1}$$

where $\gamma_{i,\varepsilon} \in \{0,1,....,p-1\}$. If α is a fixed primitive element of F_{p^k}, then corresponding to every $\varepsilon \in Z_{p^k}$ is an element $\alpha_\varepsilon \in F_{p^k}$ given by

$$\alpha_\varepsilon = \gamma_{0,\varepsilon} + \gamma_{1,\varepsilon}\alpha + ... + \gamma_{(k-1),\varepsilon}\alpha^{k-1} \qquad (6)$$

We define the Gray map ϕ on A in [2], which is a special case of the Gray map defined,

$$\phi : A^n \longrightarrow F_{P^k}^{P^{2k}n}$$

$$x + yu + zu^2 \mapsto (z, \alpha_1 x \oplus z, \alpha_2 x \oplus z, \ldots\ldots, \alpha_{P^k-1} x \oplus z,$$
$$\alpha_1 y \oplus z, \alpha_1 x \oplus \alpha_1 y \oplus z, \ldots\ldots, \alpha_{P^k-1} x \oplus \alpha_1 y \oplus z,$$
$$\alpha_2 y \oplus z, \alpha_1 x \oplus \alpha_2 y \oplus z, \ldots\ldots, \alpha_{P^k-1} x \oplus \alpha_2 y \oplus z, \quad (7)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$\alpha_{P^k-1} y \oplus z, \alpha_1 x \oplus \alpha_{P^k-1} y \oplus z, \ldots\ldots\ldots, \alpha_{P^k-1} x \oplus \alpha_{P^k-1} y \oplus z)$$

Where $\oplus$ is componentwise addition in F_{P^k} .The Gray map ϕ is an isometry from $(A^n, d_{\hom})$ to $F_{P^k}^{P^{2k}n}$ under the Hamming distance [2].

It is naturally extended as the following,

$$\phi : M_{s\times n}(A) \longrightarrow M_{s\times p^{2k}n}(IF_{p^k})$$

$$\begin{bmatrix} c^1 \\ c^2 \\ \ldots \\ c^s \end{bmatrix}_{s\times n} \mapsto \phi\left(\begin{bmatrix} c^1 \\ c^2 \\ \ldots \\ c^s \end{bmatrix}\right) = \begin{bmatrix} \phi(c^1) \\ \ldots\ldots \\ \ldots\ldots \\ \phi(c^s) \end{bmatrix}_{s\times p^{2k}n} \quad 8)$$

Where $M_{s\times n}(S)$ denotes the set of $s \times n$ matrices over a ring S.

Proposition 1.1:- *[2]*

$\phi \circ \nu = \sigma^{\otimes p^{2k-1}} \circ \phi$.

Theorem 1.2:-*[2]* A code C of length n over A is $(1-u^2)$- cyclic if and only if $\phi(C)$ is quasi-cyclic of index p^{2k-1} and length $p^{2k}n$ over F_{p^k} .

Theorem 1.3: Let C be $(1-u^2)$-cyclic codes over A with $d_{\hom}(C) = d$. Then $\phi(C)$ is quasi-cyclic codes of index p^{2k-1} with $d_H(\phi(C)) = d$. ie.

$$d_{\hom}(c,e) = d_H(\phi(c), \phi(e)) \quad (9)$$

Proof: Since ϕ is isometry, we have the equality. By using the definition of the minimum distance, we have $d_{\hom}(C) = d_H(\phi(C))$.

Lemma 1.4: If $G_{s\times n}$ is a generator matrix of a code C of full rank s over A , then

$$\begin{bmatrix} \phi(G) \\ \phi(uG) \\ \phi(u^2G) \end{bmatrix}_{3s\times p^{2k}n} \quad (10)$$

is a generator matrix for $\phi(C)$, where u^iG is a matrix obtained by multiplying the rows of G by u^i , $i = 0,1,2$.

Proof: Let $v_1, v_2, \ldots\ldots, v_s$ be the row vectors of G which are linearly independent over A . The claim is that

$$\phi(v_1), \ldots\ldots\ldots\ldots, \phi(v_s), \phi(uv_1), \ldots\ldots, \phi(uv_s), \phi(u^2v_1), \ldots., \phi(u^2v_s) \quad (11)$$

are linearly independent over F_{p^k} .

Assume the opposite, then there exist $\alpha_i \in F_{p^k}$ for $1 \le i \le 3s$, not only zeros, such that

$$\alpha_1\phi(v_1) + \ldots\ldots + \alpha_s\phi(v_s) + \alpha_{s+1}\phi(uv_1) + \ldots\ldots\ldots\ldots + \alpha_{2s}\phi(uv_s) + \alpha_{2s+1}\phi(u^2v_1) + \ldots\ldots + \alpha_{3s}\phi(u^2v_s) = 0 \quad (12)$$

Since ϕ is A - linear, we have

$$\phi(\alpha_1 v_1 + \ldots\ldots + \alpha_s v_s + \alpha_{s+1} uv_1 + \ldots\ldots\ldots\ldots + \alpha_{2s} uv_s + \alpha_{2s+1} u^2 v_1 + \ldots\ldots + \alpha_{3s} u^2 v_s) = 0 \quad (13)$$

since ϕ is injective , $v_1, v_2, \ldots\ldots, v_s$ are linearly independent over A , then we have $\alpha_i = 0$ *for* $1 \le i \le 3s$. This is contradiction. Therefore

$$\phi(v_1), \ldots\ldots\ldots\ldots, \phi(v_s), \phi(uv_1), \ldots\ldots, \phi(uv_s), \phi(u^2v_1), \ldots\ldots, \phi(u^2v_s) \quad (14)$$

generate a module over $F_{P^k}^{P^{2k}n}$. Hence the matrix (10) which consists of these rows

generates $\phi(C)$.

Theorem 1.5: If C is $(1-u^2)$ cyclic code over A length n, dimension s, with respect to $d_{\hom}(C) = d$, then $\phi(C)$ is an distance invariant quasi-cyclic code of index p^{2k-1} over F_{p^k}, length $p^{2k}n$, dimension $3s$ with respect to d.

Proof: Since C has a generator matrix of full rank s, then by Lemma 1.4, $\phi(C)$ will be generated by a matrix of full rank $3s$ and size $3s \times p^{2k}n$. Hence $\phi(C)$ is $3s$-free. •

In this way, it can be obtained the new linear codes over F_{p^k}, by using computer programme as in [4] and [5].

REFERENCES

1. C. Bachoc, Applications of the Coding Theory to the Construction of Modular Lattices, *J. Comb. Theory,* Ser A 78, 92-119, 1997.
2. Y.Cengellenmis, F. Oke, On $(1-u^2)$-cyclic codes over $F_{p^k} + uF_{p^k} + u^2F_{p^k}$, *Advances and Applications in Discrete Mathematics, (to be accepted)*.
3. M.Greferath and S.E.Schmidt, Gray Isometries for Finite Chain Rings and a Nonlinear Ternary $(36,3^{12},15)$ code. *IEEE Trans. on Inf. Theory* 45, 2522-2524, 1999.
4. T.A Gulliver, Masaaki Harada, Codes over $F_3 + uF_3$ and Improvements to the Bounds on Ternary Linear Codes. *Des Codes and Cryptogr* .22, no 1, 89-96, 2001
5. Siap ,D.K. Ray-Chaudhuri, New Linear Codes over F_5 Obtained by Tripling Method and Improvements on Bounds, *IEEE Trans. on Inf .Theory* .VOL 48, NO 10, 2764-2768,2002.