International Journal of Engineering Research and Development
ISSN: 2278-067X, Volume 1, Issue 9 (June 2012), PP.34-37
www.ijerd.com

Cyclic Codes of Length 2^k Over $Z_2{}^m$

Arpana Garg[1], Sucheta Dutt[2]
[1,2]*Department of Applied Science, PEC University of Technology, Sector – 12, Chandigarh, India.*

Abstract—*In this paper, the structure of cyclic codes over Z_{2^m} of length 2^k for any natural number k is studied. It is proved that cyclic codes over $R = Z_{2^m}[x]/<x^n-1>$ of length n = 2^k are generated by at most m elements.*

Keywords*— Codes, Cyclic codes, Ideals, Principal ideal Ring*

I. INTRODUCTION

Let *R* be a commutative finite ring with identity. A *linear code C* over *R* of length *n* is defined as a *R*-submodule of R^n. A *cyclic code C* over *R* of length *n* is a linear code such that any cyclic shift of a codeword is also a codeword, that is, whenever $(c_1, c_2, c_3, \ldots, c_n)$ is in *C* then so is $(c_n, c_1, c_2, \ldots, c_{n-1})$.

Most of the work on cyclic codes over Z_4 has been done in [2,6,7]. Cyclic codes over ring Z_m are studied by Abualrub in [3] where length of code is relatively prime to *m*. Structure of Cyclic codes over Z_{p^2} of length p^e is studied in [8,12]. T.Abualrub and I.Siap give the structure of cyclic codes over rings of characteristic *2,* that is, $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2 Z_2$ in [11]. In [10], Structure of cyclic codes over Z_8 is given. A class of constacyclic codes is studied by Dinh in [1] and Zhu in [13].

In this paper, we study the structure of cyclic codes of length 2^k over Z_{2^m} and prove that cyclic codes of length 2^k over Z_{2^m} are generated by at most *m* elements.

II. PRELIMINARIES

Codewords of a cyclic code of length *n* over a ring *R* can be represented by polynomials modulo $x^n - 1$. Thus any codeword $c = (c_0, c_1, c_2, \ldots, c_{n-1})$ can be represented by polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}$ in the ring *R*.

2.1 Definition : Define a map $\varphi : Z_{2^m}[x]/<x^n-1> \rightarrow Z_2[x]/<x^n-1>$ such that φ maps zero divisors in Z_{2^m} to 0; and units of Z_{2^m} to 1; and *x* to *x*.

It is easy to prove that φ is an epimorphism of rings.

Any polynomial $f(x) \in Z_{2^m}[x]/<x^n-1>$ can be represented as $f(x) = f_1(x) + 2f_2(x) + 2^2 f_3(x) + \ldots + 2^{m-1} f_m(x)$ where $f_i(x) \in Z_2[x]/<x^n-1> \forall i$. The image of $f(x)$ under φ is $f_1(x)$.

2.2. Definition [9]: The content of the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$ where the *a_i's* belong to Z_{2^m}, is the greatest common divisor of $a_0, a_1, a_2, \ldots, a_m$.

2.3. Lemma [2]: If *R* is a local ring with the unique maximal ideal *M* and $M=(a_1,a_2,\ldots,a_n)=<a>$, then $M=<a_i>$ for some i.

Consider the ring $R = Z_{2^m}[x]/<x^n-1>$. Let *C* be an ideal in *R* of length 2^k over Z_{2^m}. The following lemmas can be easily proved.

2.4. Lemma: *R* is a local ring with the unique maximal ideal $M = <2, x-1>$.

2.5. Lemma: *R* is not a Principal ideal ring.

III. GENERATORS OF CYCLIC CODES OVER Z_{2^m}

We start the section with the following:

3.1. Lemma: Let *C* be a cyclic code of length 2^k over Z_{2^m}. If minimal degree polynomial *g(x)* in *C* is monic, then *C*=<*g(x)*>.

Proof: Let $g(x) = g_0(x) + 2g_1(x) + 2^2 g_3(x) + \ldots + 2^{m-1} g_{m-1}(x)$ such that $g_0(x) \neq 0$ and $g_i(x) \in Z_2(x)/<x^n - 1>$ be the minimal polynomial in *C* whose leading coefficient is a unit. Let *c(x)* be a polynomial in *C,* By division algorithm there exists *q(x)* and *r(x)* over Z_{2^m} such that *c(x)=g(x)q(x)+r(x)* where *r(x) = 0* or $\deg(r(x)) < \deg(g(x))$. This implies $r(x)=c(x)\text{-}g(x)q(x) \in C$. If $r(x) \neq 0$, then $\deg(r(x)) < \deg(g(x))$ which is a contradiction to the choice of degree of *g(x).* Therefore *r(x)=0,* that is , every polynomial *c(x)* in *C* is multiple of *g(x).* Hence *C* = <*g(x)*>.

3.2. Lemma: Let *C* be a cyclic code of length 2^k over Z_{2^m}. If *g(x)* is a minimal degree polynomial in *C* of degree '*t*' with leading coefficient $2^s h_1$ where $1 \leq s < m$ and h_1 is an odd integer, then content of *g(x)* is 2^s. That is $g(x) = 2^s q_s(x)$, where $q_s(x) \in Z_{2^{m-s}}[x]/<x^n - 1>$.

Proof: Let *g(x)* be a minimal degree polynomial in *C* of degree '*t*' with leading coefficient $2^s h_1$ where $1 \leq s < m$ and h_1 is an odd integer. Let $g(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_t x^t$ such that $a_t = 2^s h_1$. Now, we claim that $a_i \equiv 0 (\bmod 2^s) \forall i$. Suppose this is not so. This implies there exist some $j < t$ such that $a_j \neq 0 (\bmod 2^s)$. Then $2^{m-s} g(x)$ is a non zero polynomial of degree less than degree of $g(x)$ and belongs to *C,* which contradicts the minimality of $g(x)$. Hence $a_i \equiv 0 (\bmod 2^s) \forall i$ and content of $g(x)$ is 2^s. Therefore $g(x) = 2^s q_s(x)$ where $q_s(x) \in Z_{m-s}[x]/<x^n - 1>$.

3.3. Lemma: Let *C* be a cyclic code of length 2^k over Z_{2^m}. Let *g(x)* be a minimal degree polynomial in *C* of degree *'t'* with leading coefficient $2^s h_1$ where $1 \leq s < m$ and h_1 be an odd integer. Let all polynomials in *C* have leading coefficient $2^u h$ such that $u \geq s$. Then $C =< g(x) >=< 2^s q_s(x) >$ where $q_s(x) \in Z_{2^{m-s}}[x]/<x^n - 1>$.

Proof: Since *g(x)* is minimal degree polynomial in C, by *Lemma 3.2.,* content of *g(x)* is 2^s and $g(x) = 2^s q_s(x)$, where $q_s(x) \in Z_{2^{m-s}}[x]/<x^n - 1>$. We claim that all polynomials in *C* are multiple of $g(x) = 2^s q_s(x)$. If possible, let there exist a minimal polynomial *c(x)* of degree *'p'* in *C* which is not divisible by *g(x).* Then there exists $r(x) (\neq 0)$ such that $c(x) = g(x)\, v\, x^{p-t} + r(x)$ where $\deg\ r(x) < \deg(c(x))$ and *v* is an integer. Because *C* is an ideal, therefore $r(x) = c(x) - g(x)\, v\, x^{p-t} \in C$. As $\deg\ r(x) < \deg(c(x))$ and $r(x) \in C$ we must have $2^s q_s(x) \mid r(x)$. This implies $2^s q_s(x) \mid c(x)$, which is a contradiction. Therefore all polynomials in *C* are multiples of $g(x) = 2^s q_s(x)$ Hence $C =< g(x) >=< 2^s q_s(x) >$

3.4. Lemma: Let *C* be a cyclic code of length 2^k over Z_{2^m} not containing any monic polynomial. Let *g(x)* be minimal degree polynomial in *C* of degree '*t'* with leading coefficient $2^{s_1} h_1$ where $1 \leq s_1 < m$ and h_1 is an odd integer. Then $C =< 2^{s_c} q_c(x), 2^{s_{c-1}} q_{c-1}(x), \ldots, 2^{s_2} q_2(x), 2^{s_1} q_1(x) >$ where $0 < s_c < s_{c-1} < \ldots < s_2 < s_1$ and $2^{s_i} q_i(x)$ is minimal degree polynomial in *C* among all polynomials in *C* with leading coefficient less than odd multiple of $2^{s_{i-1}}$ for $1 \leq i \leq c$. Moreover, $q_1(x) \mid q_2(x) \mid q_3(x) \mid \ldots \mid q_c(x)$ which implies $C \subset < q_1(x) >$.

Proof: Now, *g(x)* is minimal degree polynomial in *C* with leading coefficient $2^{S1}h_1$. By *Lemma 3.2,* content of *g(x)* is 2^{s_1} and therefore $g(x)=2^{S1}q_1(x)$. Let $c(x)\in C$. As *C* does not contain any monic polynomial, leading coefficient of $c(x)$ is a zero divisor i.e. of the type $2^p h_p$. If leading coefficient of *c(x)* is greater than or equal to $2^{S1}h_1$, then by *Lemma 3.3.* $2^{S1}q_1(x)$ divides *c(x)* that is *c(x)* is multiple of $2^{S1}q_1(x)$. If leading coefficient of *c(x)* is less than $2^{S1}h_1$ then let $2^{S2}q_2(x)$ be a minimal polynomial among all polynomials with leading coefficient less than $2^{S1}h_1$. Then $s_2 < s_1$ and $\deg(2^{s_2}q_2(x)) > \deg(2^{s_1}q_1(x))$. Now, divide *c(x)* by $2^{S2}q_2(x)$. Then there exist *Q(x)* and *R(x)* such that

$$c(x)=2^{S2}q_2(x)Q(x)+R(x) \qquad (1)$$

where *R(x)* = 0 or $\deg(R(x))<\deg(2^{S2}q_2(x))$. If $\deg(R(x))<\deg(2^{S2}q_2(x))$ then leading coefficient of $R(x)$ is greater than or equal to $2^{S1}h_1$. Therefore *R(x)* is multiple of $2^{S1}q_1(x)$ and there exist *W(x) s.t.* $R(x)=2^{S1}q_1(x)W(x)$
Putting this value in equation (1), we get $c(x)=2^{S2}q_2(x)Q(x)+2^{S1}q_1(x)W(x)$

Now, if code *C* does not contain any polynomial with leading coefficient less than $2^{S2}h_2$ then $c(x)\in\, <2^{S2}q_2(x),2^{S1}q_1(x)>$ and $C=\,<2^{S2}q_2(x),2^{S1}q_1(x)>$. Otherwise choose minimal polynomial among all polynomials in *C* with leading coefficient less than $2^{S2}h_2$. Let it be $2^{S3}q_3(x)$ such that $s_3<s_2<s_1$.

Then $\deg(2^{S3}q_3(x))>\deg 2^{S2}q_2(x)>\deg 2^{S1}q_1(x)$. Continuing in this way, we shall get a sequence of generators $2^{S_3}q_3(x),2^{S_4}q_4(x),\ldots.$ for C. Because the sequence $\{s_i\}$ is a decreasing sequence of positive numbers, this process must come to an end in finite number of steps, say c, and we obtain that $C=\,<2^{S_c}q_c(x),2^{S_{c-1}}q_{c-1}(x),\ldots,2^{S_2}q_2(x),2^{S_1}q_1(x)>$ where $0<s_c<s_{c-1}<\ldots.<s_2<s_1$ and $2^{S_i}q_i(x)$ is minimal degree polynomial in *C* among all polynomials in *C* with leading coefficient less than odd multiple of $2^{S_{i-1}}$ for $1\le i\le c$.

It is easy to prove that $q_1(x)\,|\,q_2(x)\,|\,q_3(x)\,|\ldots|\,q_c(x)$ which implies $C\subset\,<q_1(x)>$.

3.5.Lemma : Let *C* be a cyclic code of length 2^k over Z_{2^m} . Let $g(x)=2^{S1}q_1(x)$ be minimal degree polynomial in *C.* Then $C=\,<f(x),2^{S_c}q_c(x),2^{S_{c-1}}q_{c-1}(x),\ldots,2^{S_2}q_2(x),2^{S_1}q_1(x)>$ where $0<s_c<s_{c-1}<\ldots.<s_2<s_1$ and $2^{S_i}q_i(x)$ is minimal degree polynomial in *C* among all polynomials in *C* with leading coefficient less than odd multiple of $2^{S_{i-1}}$ for $1\le i\le c$ and *f(x)* is minimal degree polynomial among all monic polynomials in *C*. Moreover, $q_1(x)\,|\,q_2(x)\,|\,q_3(x)\,|\ldots|\,q_c(x)\,|\,f(x)$ which implies $C\subset\,<q_1(x)>$.

Proof: Suppose *C* is a code which contains monic polynomials. Choose a monic polynomial $f(x)=f_1(x)+2f_2(x)+2^2f_3(x)+\ldots+2^{m-1}f_m(x)$ of minimal degree *'t'* among all monic polynomials in *C*. Let *S* be set of all polynomials of *C* of degree less than *t.* Then leading coefficient of all polynomials in *S* is zero divisor, that is, of the type $2^i h_i$ for some $i<m$ and h_i is an odd integer. Let $c(x)\in C$, by division algorithm there exist unique polynomials *q(x)* and *r(x)* such that

$$c(x)=f(x)q(x)+r(x) \qquad (2)$$

where either *r(x)*=0 or $\deg(r(x))<\deg(f(x))$. Now, *C* is an ideal therefore $r(x)\in C$. If $\deg(r(x))<\deg(f(x))$ then $r(x)\in S$ Now, *S* does not contain any monic polynomial and therefore by *Lemma 3.4.* $r(x)\in\,<2^{S_c}q_c(x),2^{S_{c-1}}q_{c-1}(x),\ldots,2^{S_2}q_2(x),2^{S_1}q_1(x)>$ Thus, there exist $w_1(x),w_2(x),\ldots,w_c(x)$ such that $r(x)=2^{S_1}q_1(x)w_1(x)+2^{S_2}q_2(x)w_2(x)+\ldots+2^{S_c}q_c(x)w_c(x)$ Substituting this value in equation (2), we get $c(x)=f(x)q(x)2^{S_1}q_1(x)w_1(x)+2^{S_2}q_2(x)w_2(x)+\ldots+2^{S_c}q_c(x)w_c(x)$ This implies that $c(x)\in\,<f(x),2^{S_c}q_c(x),2^{S_{c-1}}q_{c-1}(x),\ldots,2^{S_2}q_2(x),2^{S_1}q_1(x)>$

3.6. Theorem : Cyclic Codes in *R* of length 2^k are generated by at most *m* elements.

Proof: The Theorem follows from Lemmas 3.1. to 3.5.

REFERENCES

[1]. H.Q.Dinh, A class of constacyclic codes over the Ring $F_q + uF_q + ... + u^{k-1}F_q$ J.London math. Soc. 42 (1967) 208-216.

[2]. T. Abualrub and R. Oehmke, "Cyclic codes of length 2^e over Z_4" Discrete Applied Mathematics 128 (2003) 3 – 9.

[3]. T. Abualrub. Cyclic codes and their duals over Z_m. Ann. Sci. Math. 23 (1999), no. 2, 109–118.

[4]. A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Designs Codes Cryptogr. 6 (1995) 21–35.

[5]. F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, Ninth impression, North-Holland, Amsterdam, 1977.

[6]. Steven T. Dougherty, San Ling, Cyclic Codes Over Z_4 of Even Length, Designs, Codes and Cryptography, vol 39, pp 127–153, 2006

[7]. T. Blackford, Cyclic codes over Z_4 of oddly even length, Discrete Applied Mathematics, Vol. 128 (2003) pp. 27–46.

[8]. Shi Minjia, Zhu Shixin. Cyclic Codes Over The Ring $Z_P{}^2$ Of Length p^e. Journal Of Electronics (China), vol 25, no 5,(2008), 636-640.

[9]. I.S.Luthar, I.B.S.Passi. Algebra volume 2 Rings, Narosa Publishing House, first edition,2002.

[10]. Arpana Garg, Sucheta Dutt, Cyclic codes of length 2^k over Z_8, accepted,World Congress of Engineering and Technology, Beijing, China, Oct 26-28, 2012.

[11]. T.Abualrub, I.Siap, Cyclic codes over the rings $Z_2 + uZ_2$ and $Z_2 + uZ_2 + u^2Z_2$, Design Codes and Cryptography 42 (2007) 273-287.

[12]. H.M. Kiah, K.H. Leung, S. Ling, Cyclic codes over $GR(p^2,m)$ of length p^k, Finite Fields and Their Applications 14(2008) 834-846.

[13]. S.Zhu, X.Kai, A Class of Constacyclic Codes Over Z_{p^m} Finite Fields and Their Applications 16(2010) 243-254.