Open Journal of Applied Sciences
Supplement：2012 world Congress on Engineering and Technology

Cyclic codes of length 2^k over Z_8

Arpana Garg, Sucheta Dutt*
Department of Applied Sciences
PEC University of Technology, Sector - 12
Chandigarh. India
arpana22_2005@yahoo.com
suchetapec@yahoo.co.in

Abstract - We study the structure of cyclic codes of length 2^k over Z_8 for any natural number k. It is known that cyclic codes of length 2^k over Z_8 are ideals of the ring R= $Z_8[x]/<x^{2^k}-1>$. In this paper we prove that the ring R= $Z_8[x]/<x^{2^k}-1>$ is a local ring with unique maximal ideal $M=<2,x-1>$, thereby implying that R is not a principal ideal ring. We also prove that cyclic codes of length 2^k over Z_8 are generated as ideals by at most three elements.

Keywords – Codes; Cyclic Codes; Ideal; Principal Ideal Ring.

1. 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. An element of *C* is called a codeword. 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 i.e. whenever $(c_1,c_2,c_3,...,c_n)$ is in *C* then so is $(c_n,c_1,c_2,...,c_{n-1})$. Cyclic codes of order n are ideals of the ring R^n.

Let Z_8 denote the ring of integers modulo 8. Cyclic codes over ring Z_{p^m} of length *n* such that. $(n,p)=1$ are studied by A.R. Calderbank, N.J.A. Sloane in [2] and P. Kanwar, S.R. Lopez-Permouth in [3]. Most of the work has been done on the generators of cyclic code of length *n* over Z_4 where $2 \mid n$. In [1], Abualrub and Oehmke, gave the structure of cyclic codes over Z_4 of length 2^k, in [5] Blackford classified all cyclic codes over Z_4 of length $2n$ where *n* is odd and in [6] Steven T. Dougherty & San Ling gave the generator polynomial of cyclic codes over Z_4 for arbitrary even length. The structure of cyclic codes over Z_{p^2} of length p^e is given by Shi Minjia, Zhu Shixin in [7].

*(corresponding author : phone: 172-275-3268; fax: 172-274-5175)

Cyclic codes of any length *n* over fields are principal ideals. Therefore cyclic codes over Z_2 of length *n* are principal ideals. Moreover, cyclic codes over Z_2 of length *n* are generated by polynomials of the type $(x+1)^t$ where $t \mid n$ and these generators are divisors of x^n-1. But the situation is different in case of cyclic codes over rings. In this paper we prove that the ring *R*= $Z_8[x]/<x^{2^k}-1>$ is a local ring with unique maximal ideal $M=<2,x-1>$. Thereby implying that *R* is not a principal ideal ring (there exist cyclic codes which cannot be generated by one element). Even the generators of a cyclic code need not divide x^n-1 over Z_8. We also prove that cyclic codes of length 2^k over Z_8 are generated as ideals by at most three elements.

Throughout this paper we assume that $n = 2^k$ so that $R = Z_8[x]/<x^n-1>$.

2. Preliminaries

Any codeword from a cyclic code of length *n* can be represented by polynomials modulo x^n-1. Any codeword *c* = $(c_0,c_1,c_2,...,c_{n-1})$ can be represented by polynomial $c(x)=c_0+c_1x+...+c_{n-1}x^{n-1}$ in the ring *R*.

Definition 2.1: Define a map

$$\Phi : R \rightarrow Z_2[x]/<x^n-1>$$

s.t. Φ maps 0,2,4,6 to 0; 1,3,5,7 to 1; and *x* to *x*.

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

Note that Z_2 and Z_8 are rings under different binary operations, but addition and multiplication of elements in Z_2 can be obtained from the addition and multiplication of elements of Z_8 reducing them by modulo 2. Any element *a* $\in Z_8$ can be written as $a=b+2c+4d$ s.t. $b,c,d \in Z_2$. Therefore any polynomial $f(x) \in Z_8[x]$ can be represented as $f(x)=f_1(x)+2f_2(x)+2^2f_3(x)$, where $f_i(x) \in Z_2[x]$ for every *i*.

The image of any polynomial $f(x)$ Є R, under the homomorphism Φ is $f_1(x)$.

Definition 2.2[8]: The content of the polynomial $f(x) = a_0 + a_1 x + ... + a_m x^m$ where the a_i's belong to Z_8 , is the greatest common divisor of $a_0, a_1, ..., a_m$.

Theorem 2.3[8]: The Correspondence Theorem. If $\varphi : A \to A'$ is a surjective ring homomorphism having kernel η, then $I' \to \varphi^{-1}(I')$ is a 1-1 correspondence between the totality of ideals I' of A' and the totality of those ideals of A which contain η.

Theorem 2.4[8]: The General Isomorphism Theorem. If $\varphi : A \to A'$ is a surjective ring homomorphism with kernel η, and if the ideals I, I' respectively correspond to each other as in theorem 2.3. (i.e. $I = \varphi^{-1}(I')$ or equivalently, if $I \supset \eta$ *and* $I' = \varphi(I)$, then there is a unique ring homomorphism

$\overline{\varphi} : A / I \to A' / I'$ such that $\overline{\varphi}(a + I) = \varphi(a) + I'$

for all a in A. Moreover, $\overline{\varphi}$ is an isomorphism of A/I with A' / I' .

Lemma 2.5 [1]: If R is a local ring with the unique maximal ideal M and M = (a) = ($a_1, a_2, ..., a_n$), then $M = <a_i>$ for some i.

3. Generators of Cyclic Codes Over Z8.

Consider the ring $R = Z_8[x] / <x^n - 1>$. Let C be an ideal (cyclic code) in R. Now, we prove that the ring R is a local ring but not a principal ideal ring

Lemma 3.1: R is a local ring with the unique maximal ideal $M = <2, x - 1>$.

Proof : The ring $R_1 = Z_2[x] / <x^n - 1>$ is a local ring with unique maximal ideal $I = <(x-1)>$. Now, Φ is a ring homomorphism which is onto. Therefore by theorem 2.3.,

$$M = \Phi^{-1}(I) = \Phi^{-1}(<x - 1>) = <2, x - 1>$$

is ideal of R containing kernel of Φ. By theorem 2.4, there exists a unique ring isomorphism $\eta : R/\Phi^{-1}(I) \to R_1/I$. As I is maximal ideal of R_1 therefore R_1/I is a field and η is a isomorphism therefore $R / \Phi^{-1}(I)$ is also a field. This implies that $M = \Phi^{-1}(I)$ is a maximal ideal of R.

Therefore, R is a local ring with unique maximal ideal M.

Lemma 3.2: R is not a principal ideal ring.

Proof: Suppose R is a principal ideal ring. Let us consider the maximal ideal $M = <2, x - 1>$ of R. By the lemma 2.5., $M = <2, x - 1> = <x - 1>$ or $M = <2, x - 1> = <2>$. But neither 2 Є $<x - 1>$ nor $(x - 1)$ Є $<2>$. Therefore, R is not a principal ideal ring.

Now, we prove that cyclic codes of length 2^k over Z_8 are generated as ideals by at most three elements. We have the following:

Lemma 3.3: Let C be a cyclic code of length 2^k over Z_8 . If minimal degree polynomial $g(x)$ in C is monic, then $C = <g(x)>$ where $g(x) = g_1(x) + 2 g_2(x) + 4 g_3(x)$ such that $g_1(x) \neq 0$ and $g_i(x) \in Z_2[x]$ for i = 1, 2, 3.

Proof: Suppose C is a cyclic code of length $n = 2^k$ over Z_8 . Let $g(x) = g_1(x) + 2 g_2(x) + 4 g_3(x)$ such that $g_i(x) \in Z_2[x]$ for i = 1, 2, 3; be a polynomial of minimal degree in C whose leading coefficient is a unit. Let $c(x)$ be a codeword in C, then By division algorithm ∃ $q(x)$ and $r(x)$ over Z_8 such that

$c(x) = g(x)q(x) + r(x)$

where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$

This implies $r(x) = c(x) - g(x)q(x) \in C$

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 $r(x) = 0$ i.e. every polynomial $c(x)$ in C is a multiple of $g(x)$. i.e. $C = <g(x)>$.

Lemma 3.4: Let C be a cyclic code of length 2^k over Z_8 If C contains no monic polynomial and leading coefficient of minimal degree polynomial $g(x)$ in C is 2 or 6, then $C = <g(x)> = <2q_1(x)>$ where $q_1(x)$ Є $Z_4[x] / <x^n - 1>$.

Proof: If leading coefficient of minimal degree polynomial $g(x)$ is 2 or 6 then we claim that content of $g(x)$ is 2.

Suppose this is not so. Let $g(x) = c_0 + c_1 x + ... + c_s x^s$ and there exist some t such that $c_t \neq 0$ (mod 2), then $4g(x)$ 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 $c_i \equiv 0$ (mod 2) for all i and content of $g(x)$ is 2.

So $g(x) = 2q_1(x)$ where $q_1(x)$ Є $Z_4[x] / <x^n - 1>$. Let C be a code which contains no monic polynomial. Then all polynomials in C are with leading coefficient non unit. We claim that all the elements in C are multiples of $2q_1(x)$ where $q_1(x)$ Є $Z_4[x] / <x^n - 1>$.

Suppose this is not so. Then there exists a polynomial $u(x)$ of minimal degree t_1 in C which is not a multiple of $g(x) = 2q_1(x)$

Therefore, there exists $r_2(x) (\neq 0) \in Z_8[x] / <x^n - 1>$

Such that $u(x) = 2q_1(x)\, v\, x^{t_1 - s} + r_2(x)$

where $\deg r_2(x) < \deg u(x)$ and v=1 or 2 or 3

Now, C is an ideal

Therefore $r_2(x) = u(x) - 2q_1(x)vx^{t_1-s} \in C$

if $\deg r_2(x) < \deg u(x) \& r_2(x) \in C$ then $2q_1(x) | r_2(x)$

$\Rightarrow 2q_1(x) | u(x)$

which is a contradiction.

Hence $r_2(x)=0$

$\Rightarrow$ $2q_1(x) | u(x)$. i.e. $u(x) \in <g(x)> = < 2q_1(x) >$

i.e., every codeword of C is generated by $g(x) = 2q_1(x)$. i.e. $C = <g(x)> = < 2q_1(x) >$

Lemma 3.5: Let C be a cyclic code of length 2^k over Z_8 containing monic polynomials and leading coefficient of minimal degree polynomial $g(x) = 2q_1(x)$ in C is 2 or 6, then $C = =<f(x), 2q_1(x)>$ where $f(x)$ be a monic polynomial of minimal degree t among all monic polynomials in C. Moreover, $q_1(x) | f(x)$ and any code $C =< f(x), 2q_1(x) >$ is strictly contained in the code generated by $q_1(x)$.

Proof: Suppose C is a code which contains a monic polynomial $f(x)=f_1(x)+2f_2(x)+2^2 f_3(x)$, of minimal degree t among all monic polynomials in C. Let S be the set of polynomials of C of degree less than t. Then leading coefficient of all polynomials in S is a non unit or zero divisor.

Let $c(x) \in C$, by division algorithm ∃ unique polynomials = $q_3(x)$, $r_4(x)$ s.t.

$c(x)=f(x)q_3(x)+r_4(x)$ where $r_4(x) = 0$ or $\deg r_4(x)<\deg f(x)$ (1)

As C is an ideal

$\Rightarrow r_4(x) \in C$

Now if $\deg r_4(x) < \deg f(x)$

$\Rightarrow r_4(x) \in S$

then leading coefficient of $r_4(x)$ must be a zero divisor.

Let $g(x)= 2q_1(x)$ be minimal degree polynomial in S with leading coefficient *2* or *6* . It follows as in Lemma 3.4, $r_4(x)$ is multiple of $2q_1(x)$ and

$\exists w_1(x) \in Z_8[x]/ < x^n - 1 > s.t. r_4(x) = 2q_1(x)w_1(x)$

substituting in equation (1), we get

$c(x) = f(x)q_3(x) + 2q_1(x)w_1(x)$

which implies $C =< f(x), 2q_1(x) >$

As $f(x)$ is monic, therefore $2f(x)$ is polynomials with leading coefficient *2*. Therefore $2q_1(x) | 2f(x)$

$\Rightarrow q_1(x) | f(x)$.

Lemma 3.6: Let C be a cyclic code of length 2^k over Z_8 which contains polynomials with leading coefficient 4 only. Let $g(x)$ be minimal degree polynomial in C, then $C = <g(x)> = < 4q_2(x) >$ where $q_2(x) \in Z_2[x]/ < x^n - 1 >$.

Proof: **W**e claim first that content of $g(x)$, the minimal degree polynomial in C, is 4.

If this is not so, then $2g(x)$ is a non zero polynomial of degree less than degree of $g(x)$ belong to C, which is a contradiction to the choice of *deg g(x)*.

$\Rightarrow$content of $g(x)$ =4

$\Rightarrow g(x) = 4q_2(x)$ where $q_2(x) \in Z_2[x]/< x^n - 1>$

Now, we claim that all polynomials in C are multiples of $4q_2(x)$, where $q_2(x) \in Z_2[x]/ < x^n - 1 >$. Suppose this is not so, then ∃ a polynomial in C which is not a multiple of $g(x)= 4q_2(x)$. Let $u_1(x)$ be a polynomial of minimal degree t_2 in C which is not divisible by $4q_2(x)$,

then $\exists\ r_3(x)(\neq 0) \in Z_8[x]/ < x^n - 1 >$

$s.t. u_1(x) = 4q_2(x)x^{t_2-s} + r_3(x)$ where $\deg(r_3(x)) < \deg u_1(x)$

C is an ideal

$\therefore\ r_3(x) = u_1(x) - 4q_2(x)x^{t_2-s} \in C$

Now if $r_3(x)$ is not equal to 0, then

$deg\, r_3(x) < deg\ u_1(x)$, $r_3(x) \in C$ implies $4q_2(x) | r_3(x)$

$\Rightarrow 4q_2(x) | u_1(x)$, which is a contradiction.

Therefore $r_3(x) = 0$ and $u_1(x)$ is a multiple of $4q_2(x)$.

Hence every polynomial in C is multiple of $4q_2(x)$.

Thus $C = <g(x)> = < 4q_2(x) >$, where $q_2(x)$ belongs to $Z_2[x]/< x^n - 1>$.

Lemma 3.7 Let C be a cyclic code of length 2^k over Z_8 not containing monic polynomials and let the leading coefficient of minimal degree polynomial $g(x) = 4q_2(x)$ in C be 4, then $C =< 2q_1(x), 4q_2(x) >$, where $2q_1(x)$ is a polynomial with leading coefficient 2 or 6 of minimal degree *'s'* among all polynomials with leading coefficient 2 or 6 in C. Moreover, $q_2(x) | q_1(x)$ and therefore $C =< 2q_1(x), 4q_2(x) >$ is strictly contained in the code generated by $q_2(x)$.

Proof: Let $g(x)$ be minimal degree polynomial in C with leading coefficient 4, then from Lemma 3.6 it is clear that content of $g(x)$ is 4. That is $g(x) = 4q_2(x)$. Let $v(x)$ be a polynomial with leading coefficient 2 or 6 of minimal degree *'s'* among all polynomials with leading coefficient 2 or 6 in C. It is easy to prove that content of $v(x)$ is 2. That is $v(x) = 2q_1(x)$. Here $2q_1(x)$ is not unique.

Let S be set of all polynomials with degree less than *'s'*. Therefore S contains polynomial with leading coefficient 4 only. Let $c(x) \in C$ therefore leading coefficient of $c(x)$ is 2,4 or 6. If deg$(c(x))$ > deg($2q_1(x)$) then by lemma 3.4. $2q_1(x)$ divides $c(x)$. Therefore content of $c(x)$ is 2. If deg$(c(x))$ < deg($2q_1(x)$), then $c(x) \in S$ and by lemma 3.6. $4q_2(x) | c(x)$. Therefore content of $c(x)$ is alteast *2*. i.e. $c(x)= 2u(x)$. Now divide $u(x)$ by $q_1(x)$ .As $q_1(x)$ is monic polynomial therefore there exist $Q(x)$ and $R(x)$ such that

$u(x) = q_1(x)Q(x) + R(x)$

where $R(x) = 0$ or $deg(R(x)) < deg(q_1(x))$

$c(x) = 2u(x) = 2q_1(x)Q(x) + 2R(x)$ (2)

if $deg(R(x)) < deg(q_1(x))$ then $deg(2R(x)) < deg(2q_1(x))$

this implies $2R(x) \in S$

therefore by lemma 3.6. $4q_2(x) \mid 2R(x)$

therefore there exist $w'(x)$ such that $2R(x) = 4q_2(x)w'(x)$

substitute the value in equation (2), we get

$c(x) = 2q_1(x)Q(x) + 4q_2(x)w'(x)$ this implies $2R(x) \in S$

This implies $c(x) \in < 2q_1(x), 4q_2(x) >$. That is $C = < 2q_1(x), 4q_2(x) >$.

Lemma 3.8: Let C be a cyclic code of length 2^k over Z_8 such that the leading coefficient of minimal degree polynomial $g(x) = 4q_2(x)$ in C is 4. Further, let the minimal degree polynomial among all polynomials in C with leading coefficient not equal to 4 be monic, say $f(x)$ of degree 't'. Then $C = < f(x), 4q_2(x) >$. Moreover, $q_2(x) \mid f(x)$ and therefore $C = < f(x), 4q_2(x) >$ is strictly contained in the code generated by $q_2(x)$.

Proof: Suppose C is a code which contains a monic polynomial $f(x)=f_1(x)+2f_2(x)+2^2 f_3(x)$, of minimal degree t among all polynomials with leading coefficient unit or 2 or 6. Here $f(x)$ is not unique. Let S be the set of polynomials of C of degree less than t. Then leading coefficient of all polynomials in S is 4.

Let $c(x) \in C$, by division algorithm ∃ unique polynomials $q_3(x), r_4(x)$ *s.t.*

$c(x) = f(x)q_3(x) + r_4(x)$ (3)

where $r_4(x) = 0$ or $deg\, r_4(x) < deg\, f(x)$

As C is an ideal

$\Rightarrow r_4(x) \in C$

Now if $deg\ r_4(x) < deg\ f(x)$

$\Rightarrow r_4(x) \in S$

Let $g(x) = 4q_2(x)$ be the minimal degree polynomial in S with leading coefficient 4. It follows, as in Lemma 3.6 that $r_4(x)$ is multiple of $4q_2(x)$ and

$\exists w_2(x) \in Z_8(x)/ < x^n - 1 > s.t. r_4(x) = 4q_2(x)w_2(x)$

substituting in equation (3), we get

$c(x) = f(x)q_3(x) + 4q_2(x)w_2(x)$

which implies $C = < f(x), 4q_2(x) >$

Lemma 3.9: Let C be a cyclic code of length 2^k over Z_8 such that leading coefficient of minimal degree polynomial $g(x) = 4q_2(x)$ in C is 4. Further, let the minimal degree polynomial among all polynomials in C with leading coefficient not equal to 4 be $2q_1(x)$ of degree 's' and $f(x)$ be a monic polynomial of minimal degree t among all monic polynomials in C. Then $C = < f(x), 2q_1(x), 4q_2(x) >$. Moreover, $q_2(x) \mid q_1(x) \mid f(x)$ and therefore $C = < f(x), 2q_1(x), 4q_2(x) >$ is strictly contained in the code generated by $q_2(x)$.

Proof: Suppose C is a code which contains a monic polynomial $f(x)=f_1(x)+2f_2(x)+2^2 f_3(x)$, of minimal degree t among all monic polynomials in C. Here $f(x)$ need not be unique. Let S be the set of polynomials of C of degree less than t. Then leading coefficient of all polynomials in S is either *2,4 or 6*.

Let $c(x) \in C$, by division algorithm ∃ unique polynomials $q(x)$ and $r(x)$ such that $c(x) = f(x)q(x) + r(x)$ (4)

where either $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$

If $\deg(r(x)) < \deg(f(x))$ then $r(x) \in S$, by Lemma 3.7.

$r(x) \in < 2q_1(x), 4q_2(x) >$ therefore there exist

$u(x)$ and $v(x)$ such that $r(x) = 2q_1(x)u(x) + 4q_2(x)v(x)$ where $2q_1(x)$ be a polynomial with leading coefficient 2 or 6 of minimal degree 's' among all polynomials with leading coefficient 2 or 6 in C. Substitute the value of $r(x)$ in (4), we get $c(x) = f(x)q(x) + 2q_1(x)u(x) + 4q_2(x)v(x)$. That is $C = < f(x), 2q_1(x), 4q_2(x) >$.

Theorem 3.10: Cyclic codes in R of length 2^k are generated as ideals by at most three elements.

Proof: The theorem follows from Lemmas 3.3 to 3.9.

Note: This result has also been generalised by us for cyclic codes of length 2^k over Z_{2^m} for all m.

REFRENCES

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

[2] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Designs Codes Cryptogr. 6 (1995) 21–35. [3] P. Kanwar, S.R. Lopez-Permouth, Cyclic codes over the integers modulo p, Finite Fields Appl. 3 (4) (1997) 334–1352.

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

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

[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] 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.

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