Skew Codes over Rings

Taher Abualrub, and Padmapani Seneviratne

***Abstract*—In this paper we study skew cyclic codes over the ring $R = F_2 + vF_2 = \{0, 1, v, v+1\}$, where $v^2 = v$ and the automorphism θ on the ring $F_2 + vF_2$, where θ is defined to be $\theta(0) = 0,\ \theta(1) = 1,\ \theta(v) = v+1,\ \theta(v+1) = v$.**

Index Terms: Skew polynomial ring, skew codes

I. Introduction

One of the most important components in constructing error correcting codes is to construct codes with large Hamming distance. Different methods and techniques have been developed over the years to create error correcting codes that satisfy this property. Recently, D. Boucher, etc., in [4], and Abualrub, etc. in [1] studied an interesting class of linear codes using a non commutative ring $F[x, \theta]$ where F is a finite field and θ is a field automorphism from F to F. These codes are linear codes with a structure similar to the structure of cyclic and quasi cyclic codes. They were called skew cyclic and skew quasi cyclic codes respectively. [3] generalized the idea of skew cyclic codes using the non-commutative algebra $F[x, \theta]$ and studied skew constacyclic codes over Galois Rings.

In this paper we are interested in studying skew cyclic codes using the ring

$$R = F_2 + vF_2 = \{0, 1, v, v+1\}$$

where

$$v^2 = v$$

with ring automorphism

$$\theta : R \to R$$

defined by

$$\theta(0) = 0,\ \theta(1) = 1,\ \theta(v) = v+1,\ \theta(v+1) = v.$$

II. The Skew Polynomial Ring R$[x, \theta]$ and Skew Cyclic Codes

A. The Skew Polynomial Ring R$[x, \theta]$

In this section we construct the non commutative ring $R[x, \theta]$. The structure of this non commutative ring depends on the elements of the commutative ring

$$R = F_2 + vF_2 = \{0, 1, v, v+1\},$$

where

$$v^2 = v$$

and the automorphism θ on the ring R, where

$$\theta : R \to R$$

T. Abualrub and P. Seneviratne are with The Department of Mathematics and Statistics, American University of Sharjah, Sharjah, U.A.E. E-mail: abualrub(pseneviratne)@aus.edu .

defined by

$$\theta(0) = 0,\ \theta(1) = 1,\ \theta(v) = v+1,\ \theta(v+1) = v.$$

Note that

$$\theta^2(a) = \theta(\theta(a)) = a$$

for all $a \in R$. This implies that θ is a ring automorphism of order 2.

Definition 1: Define the skew polynomial ring

$$\begin{aligned} R[x, \theta] &= \{f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \mid \\ a_i &\in R \text{ for all } i = 0, \ldots, n\}. \end{aligned}$$

The addition in the ring $R[x, \theta]$ is the usual polynomial addition and the multiplication is defined using the following rule

$$(ax^i) * (bx^j) = a\theta^i(b)x^{i+j}.$$

B. Skew Cyclic Codes

Definition 2: Consider the ring $R = F_2 + vF_2 = \{0, 1, v, v+1\}$ where $v^2 = v$ and the automorphism θ defined as above. A subset C of R^n is called a skew cyclic code of length n if C satisfies the following conditions:

1) C is a submodule of R^n and
2) If

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C$$

then

$$\theta(c) = (\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in C.$$

Let $(f(x) + (x^n - 1))$ be an element in the set $R_n = R[x, \theta]/(x^n - 1)$, and let $r(x) \in R[x; \theta]$. Define multiplication from left as:

$$r(x) * (f(x) + (x^n - 1)) = r(x) * f(x) + (x^n - 1) \qquad (1)$$

for any $r(x) \in R[x; \theta]$.

Theorem 3: R_n is a left $R[x; \theta]-$module where multiplications is defined as in Equation 1.

Proof: The proof is similar to the proof of Theorem 9 in [5]. ■

Theorem 4: A code C in R_n is a skew cyclic code if and only if C is a left $R[x; \theta]-$submodule of the left $R[x; \theta]-$module R_n.

Proof: See [2] . ■

Theorem 5: Let C be a skew cyclic code in $R_n = R[x, \theta]/(x^n - 1)$ and let $f(x)$ be a polynomial in C of minimal degree. If $f(x)$ is monic polynomial then $C = ((f(x))$ where $f(x)$ is a right divisor of $(x^n - 1)$.

Proof: See [2]. ■

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

III. Examples

Definition 6: Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of R^n.Then we define the Euclidean inner product in R^n as

$$< x, y >= x_1y_1 + x_2y_2 + \ldots + x_ny_n,$$

and the Hermitian inner product as

$$[x, y] = x_1\overline{y_1} + x_2\overline{y_2} + \ldots + x_n\overline{y_n},$$

where $\overline{0} = 0$, $\overline{1} = 1$, $\overline{v} = v + 1$ and $\overline{v+1} = v$ in R^n.

Definition 7: The dual code $C^\perp$ with respect to the Euclidean inner product of C is defined as

$$C^\perp = \{x \in R^n \mid < x, c >= 0 \text{ for all } c \in C\}$$

and the dual code C^* with respect to the Hermitian inner product of C is defined as

$$C^* = \{x \in R^n \mid [x, c] = 0 \text{ for all } c \in C\}.$$

C is called Euclidean self dual if $C = C^\perp$ and is called Hermitian self dual if $C = C^*$.

Example 8: The polynomial $g(x) = x^6 + (v+1)x^5 + x^4 + vx^3 + x^2 + (v+1)x + 1$ generates a Hermitian self dual code of length $n = 12$ with the optimum minimum distance $d = 4$.

Example 9: The polynomial $g(x) = x^4 + vx^3 + x^2 + (v + 1)x + 1$ generates an Euclidean self dual code of length $n = 8$ with the optimum minimum distance $d = 4$.

References

[1] T. Abualrub, A. Ghrayeb, I. Siap, and N. Aydin, "On the Construction of Skew Quasi-Cyclic Codes", Accepted to appear, *IEEE transaction on Information Theory*, June 2009.

[2] T. Abualrub, and P. Seneviratne, "Skew Cyclic Codes over $F_2 + vF_2$", submitted.

[3] D. Boucher, P. Sole, and F. Ulmer, "Skew Constacyclic Codes over Galois Rings," Advances of Mathematics of Communications, vol.2 Number 3, 2008, pp. 273-292.

[4] D. Boucher, W. Geiselmann, and F. Ulmer, "Skew-Cyclic Codes," *Applicable Algebra in Engineering, Communication and Computing*, Vol. 18, Issue 4, July 2007, p. 379-389.

[5] I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne, "Skew Cyclic Codes of Arbitrary Length", submitted.

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)