Skew polynomial codes over $\mathbb{F}_2 + v\mathbb{F}_2$

Pani Seneviratne

Department of Mathematics & Statistics

American University of Sharjah

April 15, 2010

Abstract

We study skew cyclic codes over the ring

$R = \mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, v+1\}$, where $v^2 = v$. and the

automorphism θ on the ring $\mathbb{F}_2 + v\mathbb{F}_2$, where θ is defined to be

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

Note

This is a joint work with Taher Abualrub.

Introduction

- Skew cyclic codes were introduced by D. Boucher, et al. in [4], where they generalized the notion of cyclic codes by using generator polynomials of (non commutative) skew polynomial rings.
- Since skew polynomial rings are left and right Euclidean, the obtained codes share most properties of cyclic codes.
- Since there are much more skew-cyclic codes, this new class of codes allow us to systematically search for codes with good properties.

Introduction

- The skew polynomial ring $F[x, \theta]$ is not a unique factorization domain.
- Hence polynomials in general do not have unique factorization as a product of irreducible polynomials.

Example

Consider the finite field $GF(4) = \{0, 1, w, w^2\}$, where $w^2 + w + 1 = 0$. Define the automorphism

$$\begin{aligned} \theta : \quad GF(4) \quad &\rightarrow \quad GF(4) \\ \theta(w) \quad &= \quad w^2 \end{aligned}$$

Example

Then we have the following factorizations of $x^4 - 1$ in $F[x,\theta]$.

$$\begin{aligned} x^4 - 1 &= (x-1)^4 \\ &= (x+w)(x+w^2)(x+w)(x+w^2) \\ &= (x+w)(x+w)(x+w^2)(x+w^2) \\ &= (x+w)(x+w^2)(x+1)(x+1) \end{aligned}$$

Introduction

- Abualrub, et al. in [1] generalized the idea to skew quasi-cyclic codes.
- The codes studied above use a non commutative ring $F[x, \theta]$, where F is a finite field and θ is a field automorphism from F to F.
- The results in both cases produced optimal codes over $GF(4)$ with regard to the Hamming distance.
- D. Boucher, et al. in [3] generalized the idea of skew cyclic codes using the non-commutative algebra $F[x, \theta]$ and studied skew constacyclic codes over Galois Rings.

Introduction

- An ideal generalization of studying skew cyclic codes over $GF(4)$ is to study skew cyclic codes over the ring Z_4.
- But skew cyclic codes depend on a ring automorphism θ.
- Unfortunately, the only ring automorphism $\theta : Z_4 \to Z_4$ is the identity map.

Introduction

- The other two commutative rings of size 4 other than $GF(4)$ and Z_4 are the rings $F_2 + uF_2 = \{0, 1, u, u + 1\}$ where $u^2 = 0$ and $R = F_2 + vF_2 = \{0, 1, v, v + 1\}$ where $v^2 = v$.
- Again as in the case of Z_4, the ring $F_2 + uF_2 = \{0, 1, u, u + 1\}$ where $u^2 = 0$ has only the identity automorphism. So, these two rings (Z_4 and $F_2 + uF_2$) will not produce any codes that are different from normal cyclic codes.

Introduction

- The ring $R = F_2 + vF_2 = \{0, 1, v, v+1\}$ where $v^2 = v$ is more interesting than that of the other two rings.
- The ring automorphism θ, where $\theta(0) = 0,\ \theta(1) = 1,\ \theta(v) = v + 1,\ \theta(v+1) = v$ is a non-trivial automorphism.
- The ring $R = F_2 + vF_2 = \{0, 1, v, v+1\}$ is isomorphic to the ring $F_2 \times F_2$.

Skew polynomial codes

Notation

Let $R = F_2 + vF_2 = \{0, 1, v, v+1\}$ where $v^2 = v$.

with ring automorphism

$$\theta : R \to R$$

defined by

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

Note

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.

Skew polynomial codes

Definition

Define the skew polynomial ring

$$\begin{aligned} R[x,\theta] &= \{f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \mid \\ a_i &\in R \text{ for all } i = 0,\ldots,n\}. \end{aligned}$$

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

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

Skew polynomial codes

Definition

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

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

Skew polynomial codes

Definition

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

$$r(x) * (f(x) + (x^n - 1)) = r(x) * f(x) + (x^n - 1) \tag{1}$$

Skew polynomial codes

Theorem

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

Skew polynomial codes

Theorem

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.

Generators

Theorem

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 a monic polynomial then $C = ((f(x))$ where $f(x)$ is a right divisor of $(x^n - 1)$.

Generators

Proof

Let $c(x) \in C$. Then by the left division algorithm, there exist unique polynomials $q(x)$ and $r(x)$ such that $c(x) = q(x) * f(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$. Since C is linear $c(x) - q(x) * f(x) \in C$. Hence $r(x) \in C$ and since $f(x)$ is of minimal degree, we have $r(x) = 0$, $c(x) = q(x) * f(x)$ and $C = ((f(x))$.

Generators

In the case of non-monic polynomial in C of minimal degree, we have the following:

Lemma

Let $f(x)$ be a non-monic polynomial in C of minimal degree then $f(x) = vf_1(x)$ or $f(x) = (v+1)f_1(x)$, where $f_1(x)$ is a binary polynomial.

Division Algorithm

- Left and right division algorithms are not applicable unless the divisor polynomial is monic or its leading coefficient is a unit.
- Because of the structure of our ring R we have the following Lemma that will help us in our division if the leading coefficient is not a unit.

Division Algorithm

Lemma

Let $f(x)$, and $g(x)$ be two non-monic polynomials in $R[x,\theta]$ with $\deg f(x) > \deg g(x)$. Then there are polynomials $q(x)$, and $r(x)$ such that

$$f(x) = q(x) * g(x) + r(x),$$

where $r(x) = 0$, or $\deg r(x) < \deg g(x)$ or $r(x)$ is a monic polynomial of degree equal at most the degree of $f(x)$.

Generators

Theorem

Let C be a skew cyclic code in $R_n = R[x, \theta]/(x^n - 1)$. Suppose that the polynomial of minimal degree in C is not monic say $f(x) = vf_1(x)$ is a polynomial of minimal degree in C. Then $C = (vf_1, g)$ where g is a monic polynomial of lowest degree among monic polynomial in C.

Generators

Corollary

Let C be a skew cyclic code in $R_n = F[x,\theta]/(x^n - 1)$. Suppose that the polynomial of minimal degree in C is not monic say $f(x) = (v+1)\, f_1(x)$ is a polynomial of minimal degree in C. Then $C = ((v+1)\, f_1, g)$ where g is a monic polynomial of lowest degree among monic polynomial in C.

Self Dual Codes

Now we will focus our attention to self-dual codes with respect to Euclidean and Hermitian inner products.

- Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of R^n.
- The Euclidean inner product in R^n is defined by $< x, y >= x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$.
- The Hermitian inner product is defined to be $[x, y] = x_1 \overline{y_1} + x_2 \overline{y_2} + \ldots + x_n \overline{y_n}$, where $\overline{0} = 0$, $\overline{1} = 1$, $\overline{v} = v + 1$ and $\overline{v+1} = v$ in R.

Sel-dual codes

Definition

- The dual code $C^{\perp}$ with respect to the Euclidean inner product of C is defined as $C^{\perp} = \{x \in R^n \mid < x, c >= 0 \text{ for all } c \in C\}$.
- The dual code C^* with respect to the Hermitian inner product of C is defined as $C^* = \{x \in R^n \mid [x, c] = 0 \text{ for all } c \in C\}$.

Self Dual Codes

- C is called Euclidean self dual if $C = C^{\perp}$ and is called Hermitian self dual if $C = C^{*}$.
- If $C = (g(x))$ is a skew cyclic code of length n and dimension k, then $C^{\perp}$ and C^{*} are skew cyclic codes of dimension $n - k$.
- This implies that C is self-dual (w.r.t. Euclidean or Hermitian) iff n is even.

Self Dual Codes

Theorem

Let $C = (g(x))$ be a skew cyclic codes of even length n and dimension k where k is odd, and let $x^n - 1 = h(x) * g(x)$, and

$$\begin{aligned} h(x) &= 1 + h_1 x + \ldots + x^k \text{ and} \\ g(x) &= 1 + g_1 x + \ldots x^{n-k}. \end{aligned}$$

Let

$$\overline{h(x)} = 1 + \theta\left(h_{k-1}\right)x + h_{k-2}x^2 + \ldots + h_1 x^{k-1} + x^k.$$

Then $\overline{h(x)}$ is a right divisor of $x^n - 1$.

Self Dual Codes

Corollary

Let $C = (g(x))$ be a skew cyclic codes of even length n and dimension k where k is odd and $x^n - 1 = h(x) * g(x)$, where $h(x)$ and $g(x)$ are defined as above, Then the dual, $C^{\perp} = \left(\overline{h(x)}\right)$, where

$$\overline{h(x)} = 1 + \theta\left(h_{k-1}\right)x + h_{k-2}x^2 + \ldots + h_1 x^{k-1} + x^k.$$

- 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.
- T. Abualrub, and P. Seneviratne, "Skew Cyclic Codes over $F_2 + vF_2$", Preprint.
- 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.
- 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.

I. Siap, T. Abualrub, N. Aydin, and P. Seneviratne, "Skew Cyclic Codes of Arbitrary Length", To appear.