# DOCTORATE
# THESIS MONITORING COMMITTEE PERIODIC EVALUATION REPORT

| Student's | |
|---|---|
| **Institute Registered** | **Graduate School of Natural and Applied Sciences** |
| **Department** | **Mathematics (English)** |
| **Program** | **PhD** |
| **Student ID Number** | **13565006** |
| **Full Name** | **Sümeyra BEDİR** |

| | |
|---|---|
| **TMC meeting place-date** | **25.05.2017** |
| **Periodic Evaluation Term** | ☒ **May-June 2017** ☐ **Nov-Dec 201..** |
| **Periodic Evaluation Number** | ☐ 1 ☐ 2 ☒ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 |
| **THESIS TITLE** | **Vectorial Cyclic Codes And Their Structure** |
| **Does the content correspond to the Thesis proposal?** | ☐ **YES** ☐ **NO** |
| **EVALUATION OF THE THESIS STUDY** | ☐ **Successful** ☐ **Unsuccessful**<br>☐ **by unanimious votes** ☐ **by majority of votes** |

**THESIS MONITORING COMMITTEE MEMBERS**

| | Appellation, Full Name | Department/ University | Date-Signature |
|---|---|---|---|
| **Thesis Advisor** | **Prof. Dr. Bayram Ali ERSOY** | **Department of Mathematics/ Yıldız Technical University** | |
| **Committee Member** | **Prof. Dr. A. Göksel AĞARGÜN** | **Department of Mathematics/ Yıldız Technical University** | |
| **Committee Member** | **Prof. Dr. Ünsal TEKİR** | **Department of Mathematics/ Marmara University** | |

**Additional Document: Student's Report**

**NOTE: The thesis committee members who have additional personal remarks may specify them with a report.**

**PROPOSAL FOR OUTLINE OF THE THESIS**

**Skew Polynomial Rings**

- The theory of noncommutative polynomial rings was first introduced by Oystein Ore (1933), Nathan Jacobson (1943) and Bernard R. McDonald (1974).

- Let $F$ be a finite field with characteristic $p$ and let $\theta$ be an automorphism of $F$ with $|\langle\theta\rangle| = m$. If $K$ is the fixed subfield of $F$ under $\theta$, then $[F: K] = m$.

**Example.** Consider $F_4 = \{0,1,\alpha,\alpha^2\}$ with the Frobenius automorphism $\theta: F_4 \to F_4$ where $\theta(\alpha) = \alpha^2$. We have $\theta(0) = 0, \theta(1) = 1, \theta(\alpha) = \alpha^2, \theta(\alpha^2) = \alpha$. Therefore $|\langle\theta\rangle| = 2$ and $F_2$ is the fixed subfield of $F_4$ under $\theta$.

**Definition. (B.R. McDonald, 1974)** The set of skew polynomials

$$F[x;\theta] = \{a_0 + a_1x + \cdots + a_nx^n : a_i \in F\}$$

becomes a ring with the usual polynomial addition and the multiplication defined below;

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

**Example.** Let $F_4 = \{0,1,\alpha,\alpha^2\}$ with the Frobenius automorphism $\theta: F_4 \to F_4$ where $\theta(\alpha) = \alpha^2$.

$$(\alpha x) * (\alpha^2 x) = \alpha\theta(\alpha^2)x^2 = \alpha\alpha x^2 = \alpha^2 x^2$$

$$(\alpha^2 x) * (\alpha x) = \alpha^2\theta(\alpha)x^2 = \alpha^2\alpha^2 x^2 = \alpha x^2$$

Note that, $F_4[x;\theta]$ is a noncommutative ring.

**Important Notes on Skew Polynomial Rings**

- Skew polynomial rings are noncommutative and non UFD.

- Right division algorithm holds in skew polynomial rings.

- Every right/left ideal of $F[x;\theta]$ is a principal ideal.

- $I$ is a two sided ideal of $F[x;\theta]$, if there exist polynomials $f, g \in F[x;\theta]$ such that $I = f * F_4[x;\theta]$ and $I = F_4[x;\theta] * g$.

- If $|\langle\theta\rangle| = m$ and K is the fixed subfield of F under $\theta$, the center of $F[x;\theta]$ is defined as $Z(F[x;\theta]) = \{a_0 + a_1x^m + \cdots + a_rx^{mr} : a_i \in K\}$.

- Any two sided ideal of $F[x;\theta]$ is generated by a polynomial in $Z(F[x;\theta])$.

**Skew Cyclic Codes**

**Definition. (Boucher et al., 2007)** Let $F$ be a finite field with automorphism $\theta$. A subspace $C$ of $F^n$ is considered as a skew cyclic code if for any vector $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, $(\theta(c_{n-1}), \theta(c_0), \cdots, \theta(c_{n-2})) \in C$.

**Skew Pseudo-Cyclic Codes**

**Definition.** Let $F$ be a finite field with automorphism $\theta$, and let $\tau_v$ be a pseudo-cyclic shift defined on $F^n$. A subspace $C$ of $F^n$ is considered as a skew pseudo-cyclic code, if for any $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, $(\theta \circ \tau_v(c_{n-1}), \theta \circ \tau_v(c_0), \cdots, \theta \circ \tau_v(c_{n-2})) \in C$.

**Quasi-cyclic Codes**

**Theorem.** Let C be a 1-generator quasi-cyclic code. Then C is generated by an element $g(x) = (p_1(x)g_1(x), \cdots, p_r(x)g_r(x))$ where $p_i(x), g_i(x) \in F[x]/\langle (x^{m_i} - 1) \rangle$ and $g_i(x) | x^{m_i} - 1 \ \forall i$. Let $h_i(x) = (x^{m_i} - 1)/g_i(x)$ and $gcd(p_i(x), h_i(x)) = 1 \ \forall i$. Then, $dimC = \deg(lcm(h_1(x), \cdots, h_r(x)))$ and $d(C) \geq \sum_i d(\langle g_i(x) \rangle)$.

**Quasi-pseudo-cyclic Codes**

**Theorem.** Let C be a 1-generator quasi pseudocyclic code. Then C is generated by an element $g(x) = (p_1(x)g_1(x), \cdots, p_r(x)g_r(x))$ where $p_i(x), g_i(x) \in F[x]/\langle f_i(x) \rangle$ and $g_i(x) | f_i(x) \ \forall i$. Let $h_i(x) = f_i(x)/g_i(x)$ and $gcd(p_i(x), h_i(x)) = 1 \ \forall i$. Then, $dimC = \deg(lcm(h_1(x), \cdots, h_r(x)))$ and $d(C) \geq \sum_i d(\langle g_i(x) \rangle)$.

**Skew Quasi-pseudo-cyclic Codes**

**Theorem.** Let C be a 1-generator skew quasi pseudocyclic code over . Then C is generated by an element $g(x) = (p_1(x)g_1(x), \cdots, p_r(x)g_r(x))$ where $p_i(x), g_i(x) \in F[x; \theta]/\langle f_i(x) \rangle$ and $g_i(x)$ is a right divisor of $f_i(x) \ \forall i$ . Let $h_i(x) = f_i(x)/g_i(x)$ and $rgcd(p_i(x), h_i(x)) = 1 \ \forall i$. If $f_i(x) \in Z(F[x; \theta])$, then $dimC = \deg(llcm(h_1(x), \cdots, h_r(x)))$ and $d(C) \geq \sum_i d(\langle g_i(x) \rangle)$.

## Code Snippet and an example of Skew quasi-pseudo-cyclic codes

```
R1<t>:=PolynomialRing(GF(2));
p:=t^2+t+1;
F<a> := ext< GF(2) | p >;
R2<y> := PolynomialRing(F);
R<X>:=TwistedPolynomials(F:q:= 2);  // teta maps a to a^t
teta:= hom< F -> F | a^2 >;

n1:=29;
V1:=VectorSpace(F,n1);

g1s:=[a^2,a,a^2,0,a^2,a,1,a,1,1,1,a,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0]; // coefficient sequence for g1
g1v:=V1!g1s; // coefficient vector for g1
g1:=R!g1s; // g1 as a skew polynomail

h1s:=[1,1,a,0,1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0]; // coefficient sequence for h1
h1:=R!h1s; // h1 as a skew polynomial

f1:=h1*g1;
f1s:=ElementToSequence(f1);


//p1
p1s:=[1,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0];
p1:=R!p1s;
q1,r1:=Quotrem(p1*g1,f1); "r1=", r1; u1s:=ElementToSequence(r1) cat [0:x in [1..n1-1-Degree(r1)]];

//p2
p2s:=[1,0,1,0,0,0,0,0];
p2:=R!p2s;
q2,r2:=Quotrem(p2*g1,f1); "r2=",r2; u2s:=ElementToSequence(r2) cat [0:x in [1..n1-1-Degree(r2)]];


T1:=CompanionMatrix(R2!f1s);
"T1=",T1;

// 1st part
G1:=Matrix(F,n1,n1,[]);
G1[1]:=V1!u1s;
for i in [1..n1-1] do
G1[i+1]:=(V1!([teta(G1[i,j]): j in [1..n1]]))*T1;
end for;
"G1=",G1;
MinimumDistance(LinearCode(EchelonForm(G1)));

// 2nd part
G2:=Matrix(F,n1,n1,[]);
G2[1]:=V1!u2s;
for i in [1..n1-1] do
G2[i+1]:=(V1!([teta(G2[i,j]): j in [1..n1]]))*T1;
end for;
"G2=",G2;
MinimumDistance(LinearCode(G2));

G:=HorizontalJoin(G1,G2);G;
C:=LinearCode(G); C;
MinimumDistance(C);
```

1st Part;

$$f1 = X^{29} + X^{28} + X^{27} + a^2X^{26} + X^{25} + X^{24} + X^{23} + a^2X^{22} + X^{21} + a^2X^{20} + aX^{19} + X^{18} + a^2X^{17} + a^2X^{15} + a^2X^{14} + aX^{13} + X^{12} + a^2X^{11} + a^2X^{10} + X^9 + a^2X^8 + aX^5 + X^4 + X^3 + X^2 + a^2$$

$$g1 = X^{14} + X^{13} + X^{12} + aX^{11} + X^{10} + X^9 + X^8 + aX^7 + X^6 + aX^5 + a^2X^4 + a^2X^2 + aX + a^2$$

$$h1 = X^{15} + X^4 + aX^2 + X + 1$$

$$p1 = X^{12} + X^8 + X^4 + 1$$

$f1 = h1 * g1, rgcd(p1, h1) = 1,$

$$p1 * g1 \; mod \; f1 = X^{26} + X^{25} + X^{24} + aX^{23} + X^{18} + aX^{17} + a^2X^{16} + aX^{14} + a^2X^{10} + X^9 + X^8 + aX^7 + aX^6 + a^2X^2 + aX + a^2$$

1st Part → [29,15,8] code

2nd Part; $f1, g1, h1$ same with part 1

$$p2 = X^2 + 1$$

$$p2 * g1 \; mod \; f1 = X^{16} + X^{15} + a^2X^{13} + a^2X^{11} + a^2X^9 + aX^6 + aX^5 + aX^3 + aX + a^2$$

2nd Part → [29,15,8] code

$C1|C2$ →[58,15,23] code