Vectorial Cyclic Codes and Their Structure

Sümeyra Bedir
Thesis Supervisor: Assoc. Prof. Dr. Bayram Ali ERSOY

Yıldız Technical University
Department of Mathematics

PhD Thesis Report - II
30.12.2016

Introduction

- Pseudo-cyclic codes over finite fields were first introduced in (Peterson, 1972).

Introduction

- Pseudo-cyclic codes over finite fields were first introduced in (Peterson, 1972).
- Although every pseudo-cyclic code corresponds to a shortened cyclic code over finite fields, researches have showned that the method not only provides a direct construction for many linear codes but also may be a fruitful way to construct many good codes over different algebraic structures for which a construction is not introduced yet (Lopez et al., 2009; Alahamdi et al.,2016).

Introduction

- Pseudo-cyclic codes over finite fields were first introduced in (Peterson, 1972).
- Although every pseudo-cyclic code corresponds to a shortened cyclic code over finite fields, researches have showned that the method not only provides a direct construction for many linear codes but also may be a fruitful way to construct many good codes over different algebraic structures for which a construction is not introduced yet (Lopez et al., 2009; Alahamdi et al.,2016).
- In the first section we give the definitions for the pseudo-cyclic shift and pseudo-cyclic codes.

Introduction

- Pseudo-cyclic codes over finite fields were first introduced in (Peterson, 1972).
- Although every pseudo-cyclic code corresponds to a shortened cyclic code over finite fields, researches have showned that the method not only provides a direct construction for many linear codes but also may be a fruitful way to construct many good codes over different algebraic structures for which a construction is not introduced yet (Lopez et al., 2009; Alahamdi et al.,2016).
- In the first section we give the definitions for the pseudo-cyclic shift and pseudo-cyclic codes.
- In the second section we mention about our previous studies briefly.

Introduction

- Pseudo-cyclic codes over finite fields were first introduced in (Peterson, 1972).
- Although every pseudo-cyclic code corresponds to a shortened cyclic code over finite fields, researches have showned that the method not only provides a direct construction for many linear codes but also may be a fruitful way to construct many good codes over different algebraic structures for which a construction is not introduced yet (Lopez et al., 2009; Alahamdi et al.,2016).
- In the first section we give the definitions for the pseudo-cyclic shift and pseudo-cyclic codes.
- In the second section we mention about our previous studies briefly.
- Finally, we introduce our recent study on pseudo-cyclic code constructions over different metric spaces.

Pseudo-cyclic Shift

Let $F = GF(q)$ be a finite field with q elements and let F^n be the $n-$dimensional vector space over F.
Let $c = (c_0, c_1, \dots, c_{n-1})$ be any vector in F^n . We fix a shift vector $v = (v_0, v_1, \dots, v_{n-1})$ and define the following transformation

$$\begin{array}{rl} \tau_v: \ F^n & \rightarrow F^n \\ (c_0, c_1, \dots, c_{n-1}) & \mapsto (v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \dots, c_{n-2} + v_{n-1} c_{n-1}) \end{array}$$

- It has the following representation matrix as $\tau_v(c) = T_v c$, and T_v is exactly the companion matrix for $f(x) = x^n - v(x)$.

$$T_v = \begin{bmatrix} 0 & \cdots & \cdots & 0 & v_0 \\ 1 & 0 & \cdots & 0 & v_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & v_{n-1} \end{bmatrix}_{nxn}$$

Example

Let $c = (c_0, c_1, c_2)$ be a vector in some vector space F^3. Let $v = (v_0, v_1, v_2)$ be the shift vector.
Thus we have the following shift representation matrix;

$$T_v = \begin{bmatrix} 0 & 0 & v_0 \\ 1 & 0 & v_1 \\ 0 & 1 & v_2 \end{bmatrix}$$

And the transformation τ_v moves $c = (c_0, c_1, c_2)$ to the vector $\tau_v(c) = (v_0c_2, c_0 + v_1c_2, c_1 + v_2c_2)$ as follows;

$$\tau_v(c) = T_v c = \begin{bmatrix} 0 & 0 & v_0 \\ 1 & 0 & v_1 \\ 0 & 1 & v_2 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} v_0c_2 \\ c_0 + v_1c_2 \\ c_1 + v_2c_2 \end{bmatrix}$$

- T_v is the companion matrix for $f(x) = x^3 - (v_0 + v_1x + v_2x^2)$.

Different Notations of the shift and Related Structures

- Pseudo-cyclic shift, Pseudo-cyclic codes
- Polycyclic shift, Polycyclic codes
- $p(x)-$circulants, Generalized cyclic codes
- $v-$vector cyclic shift, $v-$vector based codes

Pseudo-cyclic Codes

Definition

A linear code C with length n over a finite field F is called $pseudo-cyclic$ with respect to the polynomial $v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$, if whenever $c = (c_0, c_1, \ldots, c_{n-1})$ is in C, so is its $v-$pseudo-cyclic shift $(v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \ldots, c_{n-2} + v_{n-1} c_{n-1})$.

- A pseudo-cyclic code with respect to v is invariant under τ_v.

Pseudo-cyclic Codes

Definition

A linear code C with length n over a finite field F is called $pseudo-cyclic$ with respect to the polynomial $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$, if whenever $c = (c_0, c_1, \ldots, c_{n-1})$ is in C, so is its $v-$pseudo-cyclic shift $(v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \ldots, c_{n-2} + v_{n-1} c_{n-1})$.

- A pseudo-cyclic code with respect to v is invariant under τ_v.
- Any cyclic code is $pseudo-cyclic$ with respect to $v = (1, 0, \ldots, 0).(v(x) = 1)$

Pseudo-cyclic Codes

Definition

A linear code C with length n over a finite field F is called $pseudo-cyclic$ with respect to the polynomial $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$, if whenever $c = (c_0, c_1, \ldots, c_{n-1})$ is in C, so is its $v-$pseudo-cyclic shift $(v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \ldots, c_{n-2} + v_{n-1}c_{n-1})$.

- A pseudo-cyclic code with respect to v is invariant under τ_v.
- Any cyclic code is $pseudo-cyclic$ with respect to $v = (1, 0, \ldots, 0).(v(x) = 1)$
- Any constacyclic code with respect to α, is $pseudo-cyclic$ with respect to $v = (\alpha, 0, \ldots, 0).(v(x) = \alpha)$

- In terms of the usual correspondance to the polynomial ring $F[x]/(x^n - v(x))$, multiplying a polynomial by x corresponds to a pseudo-cyclic shift with respect to v, therefore a $pseudo-cyclic$ code over F^n corresponds to an ideal in $F[x]/(x^n - v(x))$.

Example

Consider $c(x) = c_0 + c_1 x + c_2 x^2$. Let $v(x) = v_0 + v_1 x + v_2 x^2$, and we are in $F_q[x]/(x^3 - v(x))$.
Multiplying $c(x)$ by x, we get;

$$\begin{aligned}(c_0 + c_1 x + c_2 x^2).x &= c_0 x + c_1 x^2 + c_2 x^3 \\ &= c_0 x + c_1 x^2 + c_2 (v(x)) \\ &= c_0 x + c_1 x^2 + c_2 (v_0 + v_1 x + v_2 x^2) \\ &= c_2 v_0 + (c_0 + c_2 v_1) x + (c_1 + c_2 v_2) x^2\end{aligned}$$

So this gives us the pseudo-cyclic shift,

$$(c_0, c_1, c_2) \rightarrow (c_2 v_0, c_0 + c_2 v_1, c_1 + c_2 v_2)$$

Pseudo-cyclic Codes as Invariant Submodules

- Pseudo-cyclic codes over finite chain rings are recently studied by (Lopez, et al., 2009).

Pseudo-cyclic Codes as Invariant Submodules

- Pseudo-cyclic codes over finite chain rings are recently studied by (Lopez, et al., 2009).
- Let $f(x) = x^n - v(x) = f_1.f_2.....f_t$ be the factorization of a regular polynomial $f(x)$ over a finite chain ring R into pairwise coprime, monic, basic irreducible polynomial factors. In this case, we can apply the generalization of the Sun Zi Theorem;

$$R/(f(x)) = R/(f_1(x)) \oplus \cdots \oplus R/(f_t(x))$$

- Consider the submodules $f_i(T_v)x = 0$, where $x \in R^n$. Denoting $U_i = Kerf_i(\tau_v)$, the results in and are genralized to the pseudo-cyclic case as follows

Lemma

(1) Each U_i is a free τ_v-invariant submodule of R^n.
(2) If W is a τ_v-invariant submodule of R^n and $W_i = W \cap U_i$ for $i = 1, 2, \ldots, r$, then W_i is τ_v-invariant and $W = \bigoplus_{i=1}^{t} W_i$.
(3) $R^n = \bigoplus_{i=1}^{t} U_i$
(4) $rank(U_i) = \deg(f_i)$
(5) The minimal polynomial of τ_v over U_i is $f_i(x)$
(6) U_i is a free minimal τ_v-invariant submodule of R^n
(7) If U is a free τ_v-invariant submodule of R^n, then U is a direct sum of some minimal free τ_v-invariant submodules U_i of R^n.

Theorem

Let C be a linear polycyclic code of length n over R. Then the following facts hold

(1) $C = \bigoplus_{j=1}^{s} U_{i_j}$ *for some minimal* τ_v*-invariant submodules of* R^n *and* $rank(C) = \sum_{j=1}^{s} k_{i_j}$ *where* k_{i_j} *is the rank of* U_{i_j}

(2) $h(x) = f_{i_1}(x).f_{i_2}(x).\dots.f_{i_s}(x)$ *is the minimal polynomial of* τ_v *over* C

(3) $rank(h(T_v)) = n - rank(C)$

(4) $c \in C$ *if and only if* $h(T_v)c = 0.$

- If $g(x) = f(x)/h(x)$ is the generating polynomial of a polycyclic code C, then $H = h(T_v)$ is a parity check matrix for C and $G = g(T_v^{tr})$ is a generator matrix for C. One may also notice that G is indeed a full vector-circulant matrix (Jitman, 2013) of $c = (g_0, g_1, \dots, g_{n-1})$ with respect to v.

Vector Circulant Matrices (p(x)-circulants)

The generator matrix of a pseudo-cyclic code is a vector circulant matrix.
Vector circulant matrices are obtained by applying recursively the vector cyclic shift to the generating vector in the first row.
Namely, if we have $g = (g_0, g_1, \ldots, g_{n-1})$ as the generating vector (the coefficient vector for the generating polynomial $g(x)$), then the generating matrix is obtained as follows;

$$G = \begin{bmatrix} \cdots & g & \cdots \\ \cdots & \tau_v(g) & \cdots \\ \cdots & \tau_v^2(g) & \cdots \\ & \vdots & \\ \cdots & \tau_v^{n-1}(g) & \cdots \end{bmatrix}_{nxn} = g(T_v^{tr})$$

Example

Consider the vector space F_7^4.
Fix the shift vector $v = (2,3,0,1)$ and construct the $v - vector$ circulant matrix for $g = (1,2,3,4)$.
$\tau_v((g_0, g_1, g_2, g_3)) = (v_0 g_3, g_0 + v_1 g_3, g_1 + v_2 g_3, g_2 + v_3 g_3)$.

$$
\begin{aligned}
v &= (2,3,0,1);\\
T_v &= \begin{bmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, g = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix};\\
Tg &= \begin{bmatrix} 1 \\ 6 \\ 2 \\ 0 \end{bmatrix}, T^2 g = \begin{bmatrix} 0 \\ 1 \\ 6 \\ 2 \end{bmatrix}, T^3 g = \begin{bmatrix} 4 \\ 6 \\ 1 \\ 1 \end{bmatrix};\\
G &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 6 & 2 & 0 \\ 0 & 1 & 6 & 2 \\ 4 & 6 & 1 & 1 \end{bmatrix}
\end{aligned}
$$

Our Previous Studies

Polycyclic Quaternary Codes (ICCC, 2015)

- We pointed out the algebraic structure via submodule representation of quaternary pseudo-cyclic codes and their duals.

Our Previous Studies

Polycyclic Quaternary Codes (ICCC, 2015)

- We pointed out the algebraic structure via submodule representation of quaternary pseudo-cyclic codes and their duals.
- We obtained good pseudo-cyclic codes over $\mathbb{Z}_4$, most of which are new and optimal linear codes with respect to the existing database of quaternary codes (Asamov, 2007)

Our Previous Studies

Pseudo-cyclic Codes with Applications to DNA (ICFAS, 2016)

- We introduced the construction of polycyclic reversible DNA codes generated by polynomials of 4^k-lifted form

Our Previous Studies

Pseudo-cyclic Codes with Applications to DNA (ICFAS, 2016)

- We introduced the construction of polycyclic reversible DNA codes generated by polynomials of 4^k-lifted form
- We gave some promising examples of these codes which are MDS and satisfy the Griesmer bound.

Term Rank Metric Spaces

The vector space of mxn matrices over a fixed finite field F_q of q elements become a metric space denoted by M_{TR}, with the term rank metric derived from the term rank weight defined below, given A as an mxn matrix with $\mathcal{I}(A)$ being the set of rows/columns of A which contains all the nonzero entries of A;

$$\|A\|_{TR} = \min |\mathcal{I}(A)|$$

If A and B are two mxn matrices, the term rank distance is defined as;

$$d_{TR} = \|A - B\|_{TR}$$

Examples

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \Longrightarrow \|A\|_{TR} = 1$$

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \Longrightarrow \|A\|_{TR} = 2$$

Codes over Term Rank Metric Spaces

Codes over term rank metric spaces have applications in information transmission via memoryless matrix channels which appear in the data storage systems, memory cards and some wireless communication systems.
These codes are considered as $k-$dimensional vector subspaces of F_q^{mxn}. The minimum distance of a code over term rank metric space, denoted by D_{TR}, should clearly be less than or equal to the minimum of $\{m, n\}$ and assuming without the loss of generality that $m \leq n$, we have;

$$D_{TR} = \min_{A \in C - \{0\}} \|A\|_{TR} \leq m$$

Computing Term Rank Distance

It is proved that, the term rank weight of a matrix A is equal to the maximum size of a matching of the bipartite graph for which A is the bi-adjacency matrix (Brualdi et al, 2012).

Singleton Bound

The only known bound for codes over M_{TR} is the Singleton bound, which is expressed in the following version;

$$k \leq n(m - D_{TR} + 1)$$

If we have the equality, the code is considered to be optimal.

Construction of Optimal Codes

- Gabudilin Codes (in Rank Metric Spaces)

Construction of Optimal Codes

- Gabudilin Codes (in Rank Metric Spaces)
- by considering a set of all $p(x) - circulant\ mxn$ matrices over F_q (for $D_{TR} = m$).

Construction of Optimal Codes

- Gabudilin Codes (in Rank Metric Spaces)
- by considering a set of all $p(x) - circulant\ mxn$ matrices over F_q (for $D_{TR} = m$).
- by Toeplitz-like matrices (for $D_{TR} = m$).

Construction of Optimal Codes

- Gabudilin Codes (in Rank Metric Spaces)
- by considering a set of all $p(x) - circulant\ mxn$ matrices over F_q (for $D_{TR} = m$).
- by Toeplitz-like matrices (for $D_{TR} = m$).
- ???

Example

Let $F_q = GF(2^2) = \{0, 1, a, a^2\}$.
Let $p(x) = x^4 + a$, M_{TR}; $4x4$ F_q-matrix space
In this case, $T =$ the companion matrix of $p(x)$ is considered.
And the subspace generated by the matrices $\{T, T^2, T^3, I_4\}$ constructs a $[4x4, 4]$ code over M_{TR}.

$$C =< \left\{ \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \end{bmatrix}, I_4 \right\} >$$

Code Construction and Examples

Let $p(x) = a_0 + a_1x + \cdots + x^m$ be a monic divisor of degree m of a polynomial $f = x^n - 1$ of degree n and consider the following matrix P obtained from the companion matrix (bootom format) of p horizontally joined with an $mx(n-m)$ block matrix of zeroes.

$$P = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ -a_0 & -a_1 & \cdots & -a_{m-1} & 0 & \cdots & 0 \end{bmatrix}$$

We define a cyclic shift by vertically shifting the columns of P to the right hand side. We can obtain this shift by successive operations of the companion matrix of f to the matrix P.
The F_q sub matrix space spanned by n matrices of cyclic shifts of P construct a form of a cyclic code over M_{TR}.

We generalize this to the pseudo-cyclic case as follows;

Fact (Proposition)

Let F_q *be a finite field with* q *elements and let* f *be a monic polynomial and* p *a divisor polynomial of* f *over* $F_q[x]$, *with* $\deg f = n$ *and* $\deg p = m$. *Let* P *be the matrix obtained from the companion matrix of* p *horizontally joined with an* $mx(n-m)$ *block matrix of zeroes, and* T *be the companion matrix of* f . *The* F_q-*sub matrix space spanned by the following set of* mxn *matrices;*

$$\{P, PT, PT^2, \ldots, PT^{n-1}\}$$

constructs a pseudo-cyclic code over the term rank metric space M_{TR}.

Example

Let F_q be the finite field with 4 elements; $F_4 = \{0, 1, a, a^2\}$. Consider $f(x) = x^9 - 1$ and take $p(x) = x^3 + a^2$ as a divisor of f. Therefore we have $m = 3$, $n = 9$, and

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ a^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$T = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{9x9}$$

Example

Applying T to P, constructs the desired cyclic shift;

$$
\begin{aligned}
PT &= \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & a^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \\
PT^2 &= \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & a^2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \\
&\vdots \\
PT^8 &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^2 \end{bmatrix}
\end{aligned}
$$

The subspace generated by the spanning set $\{P, PT, PT^2, \ldots, PT^8\}$ becomes a cyclic $[3x9, 9]-$code over the F_4-matrix space of $3x9$ matrices.

Future Studies

- We aim to find the restrictions and conditions for constructing optimal codes with the proposed construction method.
- New bounds (implementations of sphere packing-covering bounds) are to be explored as in the usual vector space case.

A. Alahamdi, S. Dougherty, A. Leroy, P. Sole, (2016). On the duality and the direction of polycyclic codes, Adv. in Math. of Com., 10(4):921-929.

A. Asamov, N. Aydın, (2007). The database for $\mathbb{Z}_4$ codes, http://www.asamov.com/Z4Codes/

S. Jitman, (2013). Vector-circulant matrices over finite fields and related codes, arXiv:1408.2059 [math.RA]

S.R. Lopez-Permouth, B.R. Parra-Avila, S. Szabo, (2009). Dual generalizations of the concept of cyclicity of codes, Adv. in Math. of Com. (2009) 227–234.

William Wesley Peterson, E. J. Jr Weldon, Error Correcting codes: second edition, MIT Press (1972).

D. Radkova, A.J. Van Zanten, Constacyclic codes as invariant subspaces, Linear Algebra and its Applications, 430(2009), 855-864.

M. Wu, Free cyclic codes as invariant submodules over finite chain rings, International Mathematical Forum, 8-37(2013), 1835 - 1838.

V. Gritsenko, A. Maevskiy, (2014). On a construction of optimal codes in term rank metric via p(x)-circulants. Fourteenth