# 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 | 30.12.2016 |
| Periodic Evaluation Term | ☐ May-June 201… ☒ Nov-Dec 2016 |
| 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 | Assoc. 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.**

# On The Construction of Codes over Term Rank Metric Spaces

Sümeyra Bedir

## 1 Introduction

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;

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

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.[8,9] 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;

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

The only known bound for optimality of 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.

In , authors have introduced a construction method for optimal codes over $M_{TR}$, by using the correspondence between polynomials and $p(x)$-circulants. With this method, they construct $[nxn, n]-$codes, and for the construction of $[mxn, n]-$codes, they address the shortening method. In this study, we introduce a new construction, which will guide as an analogue to the usual construction of codes over vector spaces, and will give a way for direct construction of $[mxn, n]-$codes over term rank spaces in general. We also propose a script for finding the minimum term rank distance of a given code using Pyhton packages.

## 2 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 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;

**Theorem 1** *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 2** *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*

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ a^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, T = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{9x9}$$

*Applying* $T$ *to* $P$, *constructs the desired cyclic shift;*

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

*And 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.*

## 3 Computing The Minimum Term Rank Distance

As in the case in general coding theory, computing the minimum distance and obtaining optimal codes is an important issue also for codes over term rank metric spaces. It is already known 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[9]. Currently, there is not any in-built function for computing the term rank of a matrix in commonly used computer algebra systems. As an example for codes over $F_4-$ matrix spaces, we used the following Python packages and scripts for computing the minimum term rank distance of a code over $M_{TR}$, where we print the list of all matrices in the code from MAGMA computer algebra system to a text file as follows;

```
//Magma Code for writing matrices to a file:
K<a>:=GF(2^2); F<x>:= PolynomialRing(K);
p:=; f:=;
m:=Degree(p);n:=Degree(f);
```

```
T:= CompanionMatrix(f); V:= KMatrixSpace(K,m,n);
M:=MatrixRing(K,n);
Z1 := [0:  x in [1..m*(n-m)]];
P:= HorizontalJoin(CompanionMatrix(p),Matrix(K, m,
n-m, Z1));
B := { V!P*T^i :  i in [0..n-1]};
S:=sub< V | B >;
SetOutputFile("mxn.txt");
for s in S do
for i in [1..m] do
for j in [1..n] do
print s[i,j];end for;
print "$";end for;
print "@";end for;
UnsetOutputFile();

##Python script for computing minimum term rank distance:
import numpy as np
import networkx as nx
from networkx.algorithms import bipartite
import itertools
from networkx.convert import _prep_create_using
from networkx.convert_matrix import _generate_weighted_edges
import scipy
from scipy import linalg
n = 11;m = 5
fname = "mxn.txt"
fhand = open(fname)
L = list();S = str()
for line in fhand:
 line = line.strip()
 if "a^2" in line:
 line = line.replace("a^2","1")
 elif "a" in line:
 line = line.replace("a","1")
 S = S + line
M = S.strip().split("@")
for s in M:
 s = s.split("$")
 L.append(s)
for l in L:
 if len(l) < m+1 :
```

```
 L.remove(l)
 else:
 l.remove("")
K = list()
for item in L:
 M = list()
 for i in range(m):
 M.append([int(r) for r in item[i]])
 A = scipy.sparse.csr_matrix(M)
 G = nx.bipartite.from_biadjacency_matrix(A)
 D = nx.bipartite.maximum_matching(G)
 termrank = int(len(D.items())/2)
 if termrank != 0:
 K.append(termrank)
print "D_tr = ", min(K)
```

The cyclic code in the above example has a minimum term rank distance of 3, and therefore it is optimal.

**Example 3** *Let $F_q$ be the finite field with 4 elements; $F_4 = \{0, 1, a, a^2\}$. Consider $f(x) = x^6 + a^2x^2 + a$ and take $p(x) = x^4 + x^2 + a$ as a divisor of $f$. We have $m = 4$, $n = 6$, and*

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

*Applying $T$ to $P$, constructs a pseudo-cyclic shift as follows;*

$$PT = \begin{bmatrix} 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&a&0&1&0&0 \end{bmatrix}, PT^2 = \begin{bmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \\ 0&0&a&0&1&0 \end{bmatrix}, PT^3 = \begin{bmatrix} 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \\ a&0&a^2&0&0&0 \\ 0&0&0&a&0&1 \end{bmatrix},$$

$$PT^4 = \begin{bmatrix} 0&0&0&0&0&1 \\ a&0&a^2&0&0&0 \\ 0&a&0&a^2&0&0 \\ a&0&a^2&0&a&0 \end{bmatrix}, PT^5 = \begin{bmatrix} a&0&a^2&0&0&0 \\ 0&a&0&a^2&0&0 \\ 0&0&a&0&a^2&0 \\ 0&a&0&a^2&0&a \end{bmatrix}$$

*And the subspace generated by the spanning set $\{P, PT, PT^2, PT^3, PT^4, PT^5\}$ becomes a pseudo-cyclic $[4x6, 6]-$code over the $F_4-$matrix space of $4x6$ matrices.*

# 4 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.

# 5 References

## References


[1] 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.

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

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

[4] 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.

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

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

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

[8] V. Gritsenko, A. Maevskiy, (2014). On a construction of optimal codes in term rank metric via p(x)-circulants, Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory, September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia 348–353.

[9] Richard A. Brualdi, Kathleen P. Kiernan, Seth A. Meyer, Michael W. Schroeder, (2012). On the t-Term Rank of a Matrix, Linear Algebra and its Applications, 436(6):1632-1643.