

On a pseudo-cyclic construction of codes over term rank metric spaces

Sumeyra Bedir · Bayram Ali Ersoy

Received: 11.04.2019 / Revised: 20.05.2019 / Accepted: 26.08.2019

Abstract. *Pseudo-cyclic codes are the most general form of the concept of cyclicity of codes over vector spaces in information and coding theory. As a method of construction, it provides a direct way to construct shortened codes on vector spaces over finite fields and finite chain rings. This study applies the related concepts to the matrix spaces with respect to the term rank metric.*

Keywords. Pseudo-cyclic codes · Matrix spaces · Linear codes · Term rank metric

Mathematics Subject Classification (2010): MSC 94B05

1 Introduction

In algebraic coding theory, many research has been conducted in terms of investigating codes over different algebraic structures. It has been an important problem to find out new construction methods for codes as well as obtaining new codes and new error correction and data transmission methods. The concept of optimality of codes arises in terms of transmission of data with maximum error correction capability and this has been a widely studied issue on algebraic codes [10, 12].

Codes over matrix spaces with respect to term rank or rank metric have applications in information transmission via memoryless matrix channels which appear in the data storage systems, memory cards and some wireless communication systems in addition to network coding and space-time coding [4]. Gritsenko and Maevskiy[5] have introduced a method of constructing codes involving term rank metric. Recently, Liu and Liu [8] have investigated codes over the rank metric as complementary dual codes and introduced a construction of two classes of Gabidulin LCD MRD codes by self dual basis. In this study, we first give some preliminaries about pseudo-cyclic codes and codes over matrix spaces. We propose the pseudo-cyclic construction method for codes over term rank metric spaces in the second section and we provide some examples. In the third section, we address a method to compute the minimum term rank distance of a code using computer algebra system Magma and Python programming language together, and examine the optimality conditions of codes by means of the proposed construction method.

S. Bedir
Yildiz Technical University
E-mail: sbedir@yildiz.edu.tr

B.A. Ersoy
Yildiz Technical University
E-mail: ersoya@yildiz.edu.tr

2 Preliminaries

2.1 Pseudo-cyclic Codes

Pseudo-cyclic codes over finite fields were first introduced in [11]. Although every pseudo-cyclic code over finite fields is indeed a shortened cyclic code, the method provides a direct construction for many linear codes of various parameters over both finite fields and finite chain rings and thus attracted many researchers. Pseudo-cyclic codes and their duals are defined as polycyclic codes by means of the generalization of the concept of cyclicity of codes in [9]. After that, having the notions of left/right polycyclic codes introduced, these codes are examined in terms of duality and directions in [1]. Throughout this study we consider the following definitions and notations about pseudo-cyclic codes.

Definition 2.1 *A linear code C with length n over a finite field F_q , is called right pseudo-cyclic with respect to $v = (v_0, v_1, \dots, v_{n-1}) \in F_q^n$, if, whenever $c = (c_0, c_1, \dots, c_{n-1})$ is in C , so is its v -pseudo-cyclic shift $(v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \dots, c_{n-2} + v_{n-1} c_{n-1})$.*

With the usual correspondence to the polynomial ring $F_q[x]$, C is a right pseudo-cyclic code with respect to the polynomial $v(x) = v_0 + v_1 x + \dots + v_{n-1} x^{n-1}$, for which v is the coefficient vector. The direction of a pseudo-cyclic code refers to the direction of the pseudo-cyclic shift. In this study we prefer using the right shift.

Clearly, any cyclic code is pseudo-cyclic with respect to $v = (1, 0, \dots, 0)$; $v(x) = 1$ and any constacyclic code with respect to α where $\alpha \in F_q^*$, is pseudo-cyclic with respect to $v = (\alpha, 0, \dots, 0)$; $v(x) = \alpha$.

Consider the following transformation

$$\tau_v : \begin{array}{ccc} F^n & \longrightarrow & F^n \\ (c_0, c_1, \dots, c_{n-1}) & \longmapsto & (v_0 c_{n-1}, c_0 + v_1 c_{n-1}, \dots, c_{n-2} + v_{n-1} c_{n-1}) \end{array} \quad (2.1)$$

The representation matrix of τ_v is T_v , where $\tau_v(c) = T_v c$ for $c \in F^n$, and T_v is exactly the companion matrix of $f(x) = x^n - v(x)$:

$$T_v = \begin{bmatrix} 0 & \cdots & \cdots & 0 & v_0 \\ 1 & 0 & \cdots & 0 & v_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & v_{n-1} \end{bmatrix}_{n \times n} \quad (2.2)$$

A pseudo-cyclic code with respect to v is invariant under τ_v . A matrix G in the following form, which is exactly the v -based vector circulant matrix of the vector c [7], is a generating matrix of a pseudo-cyclic code with respect to v .

$$G = \begin{bmatrix} c_0 & \cdots & c_{n-1} \\ - & T_v c & - \\ - & T_v^2 c & - \\ & \vdots & \\ - & T_v^{n-1} c & - \end{bmatrix}_{n \times n} \quad (2.3)$$

In the quotient 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 C generated by a polynomial $g(x)$ (a divisor of $f(x) = x^n - v(x)$), corresponds to an ideal in $F[x]/(x^n - v(x))$. Using the fact that C is an ideal, one can easily show that if $\deg(g(x)) = n - k$, $C = (g(x))$ has dimension k .

2.2 Codes Over Matrix Spaces Codes over matrix spaces have been studied in terms of array codes or Gabudilin codes in [4] with respect to rank metric and term rank metric instead of the usual Hamming metric defined on usual vector spaces. In matrix spaces, matrices correspond to vectors in usual vector spaces. Note that, matrices over the base field F_q are isomorphic to the vector space over the extension field F_{q^n} ;

$$F_q^{m \times n} \cong F_{q^n}^m \quad (2.4)$$

The vector space of $m \times n$ matrices over a fixed finite field F_q of q elements become a metric space denoted by M_{TR} . Given A as an $m \times n$ matrix with $\mathcal{I}(A)$ being the set of rows/columns of A which contains all the nonzero entries of A , the term rank norm is defined as

$$\|A\|_{TR} = \min |\mathcal{I}(A)| \quad (2.5)$$

If A and B are two $m \times n$ matrices, the term rank distance is defined as

$$d_{TR} = \|A - B\|_{TR} \quad (2.6)$$

Codes over matrix spaces are considered as k -dimensional subspaces of $F_q^{m \times n}$. The minimum distance of a code over a 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

$$D_{TR} = \min_{A \in C - \{0\}} \|A\|_{TR} \leq m \quad (2.7)$$

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

$$k \leq n(m - D_{TR} + 1) \quad (2.8)$$

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

Gritsenko and Maevskiy [6] have introduced a construction method for optimal codes over M_{TR} , using the correspondence between polynomials and $p(x)$ -circulants. With this method, they construct $[n \times n, n]$ -codes, and for construction of $[m \times n, n]$ -codes, they address the shortening method. In this study, we introduce a direct pseudo-cyclic construction, which will guide as an analogue to the usual construction of codes over ordinary vector spaces in general, and with this method the cyclic and constacyclic cases for codes over matrix spaces will be classified. We also propose a method for finding the minimum term rank distance of a given code using Python software.

3 Code Construction and Examples

Let $p(x) = a_0 + a_1x + \dots + x^m$ be a monic divisor of degree m of a polynomial $f(x) = x^n - 1$ of degree n and consider the following matrix P_p obtained from the companion matrix of $p(x)$ horizontally joined with an $m \times (n - m)$ block zero-matrix

$$P_p = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ -a_0 & -a_1 & \cdots & -a_{m-1} & 0 & \cdots & 0 \end{bmatrix}_{m \times n} \quad (3.1)$$

We define a *cyclic shift* by vertically shifting the columns of P_p to the right hand side. We can obtain this shift by multiplying P_p with T_f which is the companion matrix of $f(x) = x^n - 1$;

And the subspace generated by the spanning set $\{P_p T_f^i : i \in [0, 8]\}$ becomes a cyclic $[3 \times 9, 9]$ -code over the F_4 -matrix space of 3×9 matrices.

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

$$P_p = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \alpha & 0 & 1 & 0 & 0 & 0 \end{bmatrix}, T_f = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \alpha & 0 & \alpha^2 & 0 & 0 & 0 \end{bmatrix} \quad (3.9)$$

Applying T_f to P_p , constructs a pseudo-cyclic shift as follows;

$$P_p T_f = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & \alpha & 0 & 1 & 0 & 0 \end{bmatrix}, P_p T_f^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \alpha & 0 & 1 & 0 \end{bmatrix}, \quad (3.10)$$

$$P_p T_f^3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \alpha & 0 & \alpha^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 & 1 \end{bmatrix}, P_p T_f^4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ \alpha & 0 & \alpha^2 & 0 & 0 & 0 \\ 0 & \alpha & 0 & \alpha^2 & 0 & 0 \\ \alpha & 0 & \alpha^2 & 0 & \alpha & 0 \end{bmatrix}, \quad (3.11)$$

$$P_p T_f^5 = \begin{bmatrix} \alpha & 0 & \alpha^2 & 0 & 0 & 0 \\ 0 & \alpha & 0 & \alpha^2 & 0 & 0 \\ 0 & 0 & \alpha & 0 & \alpha^2 & 0 \\ 0 & \alpha & 0 & \alpha^2 & 0 & \alpha \end{bmatrix} \quad (3.12)$$

And the subspace generated by the spanning set $\{P_p T_f^i : i \in [0, 5]\}$ becomes a pseudo-cyclic $[4 \times 6, 6]$ -code over the F_4 -matrix space of 4×6 matrices.

3.1 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 which also holds for codes over term rank metric spaces. In order to compute minimum term rank distance of a code over a matrix space, graph theoretical methods are addressed [5]. It is shown 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 [3]. Currently, there was 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 Magma script for obtaining a code over a matrix space and created some Python implementations for computing the minimum term rank distance of this code. In this method, we initially retrieve the list L of all entries (we shall denote any noninteger field-specific element by an integer here) of matrices in the code to a text file and call this file from Python to compute the minimum term rank distance.

We create a code over a matrix space with the following Magma code;

```
//Set the associated polynomial p and base polynomial f
//Set the appropriate output file name
//Copy m, n and the output filepath for later use in python function
```

```
K<a>:=GF(2^2);
```

```

F<x>:= PolynomialRing(K);

p:= x^5 + a^2*x^4 + x^3 + x^2 + a*x + 1;
f:= x^11-1;

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));
P;

B := { V!P*T^i : i in [0..n-1]};
S:=sub< V | B >;
S;

SetOutputFile ("5x11.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 ();

```

Having the code constructed, we compute its minimum term rank distance with applying the following Python function;

```

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

# Given a file path of Magma file of the constructed code,
# computes the minimum term rank distance of an  $m \times n$  code over  $GF(4)^{mn}$ .

def Minimum_Term_Rank_Distance(m,n, filepath):
    fname = filepath
    fhand = open(fname)

```

```

L = list ()
S = str ()
# Denote field – specific elements by 1
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 ("@" )

# Remove irrelevant characters inserted for environmental implementations
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_biadacency_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))

```

For the cyclic code in the first example, we call the function with parameters (5,11, "5x11.txt") and we get that it has a minimum term rank distance of 3, and therefore it is optimal.

This example is taken over the field F_4 . One may change the field and then slight modifications should be applied to the scripts if there exist more field-specific non-zero and non-integer elements.

3.2 Constructing Optimal Codes

Our main theorem is pointing out the conditions for $p(x)$ and $f(x)$ at which the code becomes optimal. For cyclic $[m \times n, n]$ codes the following results are obtained. For the most general cases the optimality question remains open.

Theorem 3.1 *Let F_q be a finite field with q elements and $p(x)$ a divisor polynomial of $f(x) = x^n - 1$ over $F_q[x]$, with $\deg p(x) = m$. Let P_p and T_f be as defined above. The cyclic $[m \times n, n]$ code C associated with $p(x)$ is optimal when $p(x) = x^m - a_0$, where $a_0 \in F_q^*$.*

Proof. For any polynomial $p(x) = \sum_{i=0}^m a_i x^i$, a matrix $A \in C$, namely a $c_i \in F_q (i \in [0, n - 1])$ -linear combination of basis matrices $P_p T_f^i : i \in [0, n - 1]$, will look like

$$A = \begin{bmatrix} c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & c_{n-3} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ c_{n-m+1} & \cdots & c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} \\ -\gamma_0 & -\gamma_1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \gamma_{n-1} \end{bmatrix}_{m \times n} \quad (3.13)$$

where for $i \in [0, n-1]$ we have

$$\gamma_i = c_0 a_i + c_1 a_{i-1} + \cdots + c_i a_0 + \underbrace{0 + \cdots + 0}_{(n-m)} + c_{n-m+1+i} a_{m-1} + \cdots + c_{n-2} a_{i+2} + c_{n-1} a_{i+1}. \quad (3.14)$$

It is shown in [3] that

$$\|A\|_{TR} = \max_{\tau} |\Delta_{\tau}(A)| \quad (3.15)$$

where the diagonal

$$\Delta_{\tau} = \{(0, \tau(0)), (1, \tau(1)), \dots, (m-1, \tau(m-1))\} \quad (3.16)$$

is a set of positions in a matrix $A \in F_q^{m \times n}$, and τ is an injection from $[0, m-1]$ to $[0, n-1]$. $|\Delta_{\tau}(A)|$ denotes the number of nonzero entries in Δ_{τ} .

For the case where $p(x)$ is of the form $x^m - a_0$, ($a_0 \in F_q^*$), we have

$$A = \begin{bmatrix} c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} & \cdots & c_{n-3} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ c_{n-m+1} & \cdots & c_{n-2} & c_{n-1} & c_0 & c_1 & \cdots & c_{n-m-1} & c_{n-m} \\ -c_0 a_0 & -c_1 a_0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & -c_{n-1} a_0 \end{bmatrix}_{m \times n} \quad (3.17)$$

We know that there exists at least one nonzero coefficient in the linear combination for all $A \in C$, say $c_t \in F_q$ ($t \in [0, n-1]$). The diagonal

$$\Delta_{\tau} = \{c_t = (0, 1), c_t = (1, 2), \dots, c_t = (m-1, n-1), -c_t a_0 = (m, 0)\}$$

corresponding to the nonzero coefficient c_t , gives the desired $\max_{\tau} |\Delta_{\tau}(A)| = m$. Therefore, we have $\|A\|_{TR} = m, \forall A \in C$, which makes C optimal.

4 Conclusion and Future Work

We proposed a pseudo-cyclic method for construction of codes over matrix spaces which allows defining cyclic, constacyclic and pseudo-cyclic concepts as in codes over vector spaces. Our method, using sparse matrices, becomes memory-efficient compared to already known constructions over matrix spaces. We provided computer algebraic method to compute the term rank distance of a code and gave optimality conditions for cyclic codes over the term rank metric space. This method can be applied to any matrix-space code, and can be improved in terms of computational speed. By means of optimality, we introduced a restriction for associated polynomials that generates optimal cyclic codes over matrix spaces. More conditions may be investigated for cyclic, constacyclic and pseudo-cyclic cases referencing these concepts.

Acknowledgements A part of this study has been presented in the International Conference on Mathematics and Engineering, ICOME-2017, May 10 - 12, 2017.

References

1. Alahamdi, A., Dougherty, S., Leroy, A., Sole, P.: *On the duality and the direction of polycyclic codes*, Adv. Math. Commun. **10** (4), 921-929 (2016).
2. Bosma, W., Cannon, J., Playoust, C.: *The Magma algebra system I. The user language*, J. Symbolic Comput. **24**, 235-265 (1997).
3. Brualdi, R.A., Kiernan, K.P., Meyer, S.A., Schroeder, M.W.: *On the t -term rank of a matrix*, Linear Algebra Appl. **436** (6), 1632-1643 (2012).
4. Gabidulin, E.M.: *Optimum codes correcting lattice errors*, Probl. Peredachi Inf. **21** (2), 103-108 (1985).
5. Gritsenko, V.V., Maevskiy, A.E.: *On a construction of optimal codes in term rank metric via $p(x)$ -circulants*, Proceedings of the 14th International Workshop on Algebraic and Combinatorial Coding Theory, Svetlogorsk (Kaliningrad region, Russia, 2014) 348-353 (Sep. 12-16, 2014).
6. Gritsenko, V.V., Maevskiy, A.E.: *$p(x)$ -circulants over finite fields and probabilistic methods for its construction*, Math. Notes, **96** (5), 928-942 (2014).
7. Jitman, S.: *Vector-Circulant Matrices and Vector-Circulant Based Additive Codes over Finite Fields*, Information, **8** (3), 82-88 (2017).
8. Liu, X., Liu, H.: *Rank-metric Complementary Dual Codes*, J. Appl. Math. Comput. (2019). <https://doi.org/10.1007/s12190-019-01254-1>
9. Lopez-Permouth, S.R., Parra-Avila, B.R., Szabo, S.: *Dual generalizations of the concept of cyclicity of codes*, Adv. Math. Commun. 227-234 (2009).
10. MacWilliams, F.J., Sloane, N.J.A.: *The Theory of Error-Correcting Codes*, North-Holland (1977).
11. Peterson, W.W., Weldon, E.J.: *Error Correcting Codes. 2nd edn*, MIT Press (1972).
12. Xing, C., Ling, S.: *Coding Theory: A First Course*, Cambridge University Press, (2003).