GENERATOR MATRIX FOR TWO-DIMENSIONAL CYCLIC CODES OF ARBITRARY LENGTH

ZAHRA SEPADAR

Department of Pure Mathematics, Ferdowsi University of Mashhad,
P.O.Box 1159-91775, Mashhad, Iran

Abstract. Two-dimensional cyclic codes of length \( n = \ell s \) over the finite field \( F \) are ideals of the polynomial ring \( F[x, y]/< x^s - 1, y^\ell - 1 > \). The aim of this paper, is to present a novel method to study the algebraic structure of two-dimensional cyclic codes of any length \( n = \ell s \) over the finite field \( F \). By using this method, we find the generator polynomials for ideals of \( F[x, y]/< x^s - 1, y^\ell - 1 > \) corresponding to two dimensional cyclic codes. These polynomials will be applied to obtain the generator matrix for two-dimensional cyclic codes.

1. Introduction

One of the important generalizations of the cyclic code is two-dimensional cyclic (TDC) code.

Definition 1.1. Suppose that \( C \) is a linear code over \( F \) of length \( s\ell \) whose codewords are viewed as \( s\ell \) arrays. That is every codeword \( c \) in \( C \) has the following form

\[
\begin{pmatrix}
c_{0,0} & \cdots & c_{0,\ell-1} \\
c_{1,0} & \cdots & c_{1,\ell-1} \\
\vdots & & \vdots \\
c_{s-1,0} & \cdots & c_{s-1,\ell-1}
\end{pmatrix}
\]

If \( C \) is closed under row shift and column shift of codewords, then we call \( C \) a TDC code of size \( s\ell \) over \( F \).

It is well known that TDC codes of length \( n = \ell s \) over the finite field \( F \) are ideals of the polynomial ring \( F[x, y]/< x^s - 1, y^\ell - 1 > \).

The characterization for TDC codes, for the first time was presented by Ikai et al. in [1]. Since the method was pure, it didn’t help decode these codes. After that, Imai introduced basic theories for binary TDC codes (2). The structure of some two-dimensional cyclic codes corresponding to the ideals of \( F[x, y]/< x^s - 1, y^{2k} - 1 > \) is characterized by the present author in [3].

The aim of this paper, is to find the generator matrix for TDC codes of arbitrary length \( n = \ell s \) over the finite field \( F \). To achieve this aim, we present a new method

2010 Mathematics Subject Classification. 12E20, 94B05, 94B15, 94B60.
Key words and phrases. two dimensional cyclic code, generator matrix, generator polynomial.
E-mail addresses: zahra.sepasdar@mail.um.ac.ir and zahra.sepasdar@gmail.com.
to characterize ideals of the ring \( \mathbb{F}[x, y]/ (x^s - 1, y^\ell - 1) \) corresponding to TDC codes, and find generator polynomials for these ideals. Finally, we use these polynomials to obtain the generator matrix for corresponding TDC codes.

**Remark 1.2.** For simplicity of notation, we write \( g(x) \) instead of \( g(x)+ <a> \) for elements of \( \mathbb{F}[x]/ <a> \). Similarly, we write \( g(x, y) \) instead of \( g(x, y)+ <a, b> \) for elements of \( \mathbb{F}[x, y]/ <a, b> \).

2. **Generator polynomials**

Set \( R := \mathbb{F}[x, y]/ (x^s - 1, y^\ell - 1) \) and \( S := \mathbb{F}[x]/ (x^s - 1) \). Suppose that \( I \) is an ideal of \( R \). In this section, we construct ideals \( I_i \) of \( S \) (for \( i = 0, \ldots, \ell - 1 \)) and prove that the monic generator polynomials of \( I_i \) provide a generating set for \( I \). Since

\[
\mathbb{F}[x, y]/ (x^s - 1, y^\ell - 1) \cong (\mathbb{F}[x]/ (x^s - 1))[y]/ (y^\ell - 1),
\]

an arbitrary element \( f(x, y) \) of \( I \) can be written uniquely as \( f(x, y) = \sum_{i=0}^{\ell-1} f_i(x)y^i \), where \( f_i(x) \in S \) for \( i = 0, \ldots, \ell - 1 \). Put

\[
I_0 = \{ g_0(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=0}^{\ell-1} g_i(x)y^i \}.
\]

First, we prove that \( I_0 \) is an ideal of the ring \( S \). Assume that \( g_0(x) \) is an arbitrary element of \( I_0 \). According to the definition of \( I_0 \), there exists \( g(x, y) \in I \) such that \( g(x, y) = \sum_{i=0}^{\ell-1} g_i(x)y^i \). Now, \( xg_0(x) \in I_0 \) since \( I \) is an ideal of \( R \) and \( xg_0(x) = \sum_{i=0}^{\ell-1} xg_i(x)y^i \) is an element of \( I \). Besides, \( I_0 \) is closed under addition and so \( I_0 \) is an ideal of \( S \). It is well-known that \( S \) is a principal ideal ring. Therefore, there exists a unique monic polynomial \( p_0^0(x) \) in \( S \) such that \( I_0 = < p_0^0(x) > \) and \( p_0^0(x) \) is a divisor of \( x^s - 1 \). So there exists a polynomial \( p_0^0(x) \) in \( \mathbb{F}[x] \) such that \( x^s - 1 = p_0^0(x)p_0^0(x) \). Now, consider the following equations

\[
\begin{align*}
f(x, y) &= f_0(x) + f_1(x)y + \cdots + f_{\ell-1}(x)y^{\ell-1} \\
yf(x, y) &= f_0(x)y + f_1(x)y^2 + \cdots + f_{\ell-1}(x)y^{\ell} \\
&= f_{\ell-1}(x) + f_0(x)y + f_1(x)y^2 + \cdots + f_{\ell-2}(x)y^{\ell-1}.
\end{align*}
\]

Since \( I \) is an ideal of \( R \), \( yf(x, y) \in I \). So according to the definition of \( I_0 \), \( f_{\ell-1}(x) \in I_0 \). A similar method can be applied to prove that \( f_i(x) \in I_0 = < p_0^0(x) \> \) for \( i = 1, \ldots, \ell - 2 \). So

\[
f_i(x) = p_i^0(x)q_i(x)
\]

for some \( q_i(x) \in S \). Now, \( p_0^0(x) \in I_0 \) so according to the definition of \( I_0 \), there exists \( p_0(x, y) \in I \) such that

\[
p_0(x, y) = \sum_{i=0}^{\ell-1} p_i^0(x)y^i.
\]

Again since \( I \) is an ideal of \( R \), \( y^i p_0(x, y) \in I \) for \( i = 1, \ldots, \ell - 1 \). So according to the definition of \( I_0 \), \( p_0^0(x) \in I_0 = < p_0^0(x) \> \). Therefore,

\[
p_i^0(x) = p_0^0(x)q_i^0(x)
\]
for some \( t_i^0(x) \in S \), and so
\[
p_0(x, y) = p_0^0(x) + \sum_{i=1}^{\ell-1} p_0^0(x) t_i^0(x) y^i.
\]

Set
\[
h_1(x, y) := f(x, y) - p_0(x, y)q_0(x) = \sum_{i=0}^{\ell-1} f_i(x)y^i - q_0(x) \sum_{i=0}^{\ell-1} p_i^0(x)y^i
\]
\[
= f_0(x) + \sum_{i=1}^{\ell-1} f_i(x)y^i - p_0^0(x)q_0(x) - q_0(x) \sum_{i=1}^{\ell-1} p_i^0(x)y^i
\]
\[
= \sum_{i=1}^{\ell-1} f_i(x)y^i - q_0(x) \sum_{i=1}^{\ell-1} p_i^0(x)y^i.
\]
(by equation [1])

Since \( f(x, y) \) and \( p_0(x, y) \) are in \( I \) and \( I \) is an ideal of \( R \), \( h_1(x, y) \) is a polynomial in \( I \). Also note that \( h_1(x, y) \) is in the form of \( h_1(x, y) = \sum_{i=1}^{\ell-1} h_i^1(x)y^i \) for some \( h_i^1(x) \in S \). Now, put
\[
I_1 = \{ g_1(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=1}^{\ell-1} g_i(x)y^i \}.
\]

By the same method being applied for \( I_0 \), it can be proved that \( I_1 \) is an ideal of \( S \). Thus, there exists a unique monic polynomial \( p_1^1(x) \) in \( S \) such that \( I_1 = < p_1^1(x) > \) and \( p_1^1(x) \) is a divisor of \( x^s - 1 \). Therefore, there exists a polynomial \( p_1^1(x) \) in \( F[x] \) such that \( x^s - 1 = p_1^1(x)p_1^1(x) \). Now, \( h_1(x, y) \in I_1 \) so according to the definition of \( I_1 \), \( h_i^1(x) \in I_1 = < p_1^1(x) > \), and so
\[
\begin{align*}
(2) & \quad h_i^1(x) = p_i^1(x)q_1(x) \\
& \text{for some } q_1(x) \in S. \end{align*}
\]

And now, \( p_1^1(x) \in I_1 \) so according to the definition of \( I_1 \), there exists \( p_1(x, y) \in I \) such that
\[
p_1(x, y) = \sum_{i=1}^{\ell-1} p_1^1(x)y^i.
\]

Again since \( I \) is an ideal of \( R \), \( y^i p_1(x, y) \in I \). So according to the definition of \( I_0 \), \( p_i^1(x) \in I_0 = < p_0^0(x) > \) for \( i = 1, \ldots, \ell - 1 \). Therefore,
\[
p_1^1(x) = p_0^0(x)t_i^1(x)
\]
for some \( t_i^1(x) \in S \), and so
\[
p_1(x, y) = \sum_{i=1}^{\ell-1} p_0^0(x)t_i^1(x)y^i.
\]
Set
\[ h_2(x, y) : = h_1(x, y) - p_1(x, y)q_1(x) = \sum_{i=1}^{\ell-1} h^1_i(x)y^i - q_1(x) \sum_{i=1}^{\ell-1} p^1_i(x)y^i \]
\[ = h^1_1(x)y + \sum_{i=2}^{\ell-1} h^1_i(x)y^i - p^1_1(x)q_1(x)y - q_1(x) \sum_{i=2}^{\ell-1} p^1_i(x)y^i \]
\[ = \sum_{i=2}^{\ell-1} h^1_i(x)y^i - q_1(x) \sum_{i=2}^{\ell-1} p^1_i(x)y^i. \] (by equation 2)

Since \( h_1(x, y) \) and \( p_1(x, y) \) are in \( I \) and \( I \) is an ideal of \( R \), \( h_2(x, y) \) is a polynomial in \( I \) in the form of \( h_2(x, y) = \sum_{i=2}^{\ell-1} h^2_i(x)y^i \) for some \( h^2_i(x) \in S \). Put
\[ I_2 = \{ g_2(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=2}^{\ell-1} g_i(x)y^i \}. \]

Again \( I_2 \) is an ideal of \( S \), and so there exists a unique monic polynomial \( p^2_2(x) \) in \( S \) such that \( I_2 = \langle p^2_2(x) \rangle \). Also \( p^2_2(x) \) is a divisor of \( x^s - 1 \), and so there exists a polynomial \( p^2_2(x) \) in \( \mathbb{F}[x]\) such that \( x^s - 1 = p^2_2(x)p^2_2(x) \). Now, \( h_2(x, y) \in I \) so according to the definition of \( I_2 \), \( h^2_2(x) \in I_2 = \langle p^2_2(x) \rangle \). So
\[ (3) \quad h^2_2(x) = p^2_2(x)q_2(x) \]
for some \( q_2(x) \in S \). Besides, \( p^2_2(x) \in I_2 \) so by definition of \( I_2 \), there exists \( p_2(x, y) \in I \) such that
\[ p_2(x, y) = \sum_{i=2}^{\ell-1} p^2_i(x)y^i. \]

Again since \( I \) is an ideal of \( R \), \( y^t p_2(x, y) \in I \). So according to the definition of \( I_0 \), \( p^2_0(x) \in I_0 = \langle p^0_0(x) \rangle \). Therefore,
\[ p^2_0(x) = p^0_0(x)t^2(x) \]
for some \( t^2(x) \in S \), and so
\[ p_2(x, y) = \sum_{i=2}^{\ell-1} p^0_0(x)t^2_i(x)y^i. \]

Set
\[ h_3(x, y) : = h_2(x, y) - p_2(x, y)q_2(x) = \sum_{i=2}^{\ell-1} h^2_i(x)y^i - q_2(x) \sum_{i=2}^{\ell-1} p^2_i(x)y^i \]
\[ = h^2_2(x)y^2 + \sum_{i=3}^{\ell-1} h^2_i(x)y^i - p^2_2(x)q_2(x)y^2 - q_2(x) \sum_{i=3}^{\ell-1} p^2_i(x)y^i \]
\[ = \sum_{i=3}^{\ell-1} h^2_i(x)y^i - q_2(x) \sum_{i=3}^{\ell-1} p^2_i(x)y^i. \] (by equation 3)
Therefore, \( h_3(x, y) \) is a polynomial in \( I \) in the form of \( h_3(x, y) = \sum_{i=3}^{\ell-1} h_i^3(x) y^i \) for some \( h_i^3(x) \in S \). In the next step, we put

\[
I_3 = \{ g_3(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = \sum_{i=3}^{\ell-1} g_i(x)y^i \}.
\]

The same procedure is applied to obtain polynomials

\[
h_4(x, y), \ldots, h_{\ell-2}(x, y), p_3(x, y), \ldots, p_{\ell-2}(x, y)
\]

in \( I \) and polynomials \( q_3(x), \ldots, q_{\ell-2}(x) \) in \( S \) and construct ideals \( I_4, \ldots, I_{\ell-2} \). Finally, we set

\[
h_{\ell-1}(x, y) := h_{\ell-2}(x, y) - p_{\ell-2}(x, y)q_{\ell-2}(x).
\]

Thus, \( h_{\ell-1}(x, y) \) is a polynomial in \( I \) in the form of \( h_{\ell-1}(x, y) = h_{\ell-1}^0(x)y^{\ell-1} \). Set

\[
I_{\ell-1} = \{ g_{\ell-1}(x) \in S : \text{there exists } g(x, y) \in I \text{ such that } g(x, y) = g_{\ell-1}(x)y^{\ell-1} \}.
\]

Clearly \( I_{\ell-1} \) is an ideal of \( S \). Thus, there exists a unique monic polynomial \( p_{\ell-1}^{\ell-1}(x) \) in \( S \) such that \( I_{\ell-1} = p_{\ell-1}^{\ell-1}(x) > 0 \) and \( p_{\ell-1}^{\ell-1}(x) \) is a divisor of \( x^s - 1 \) (there exists \( p_{\ell-1}^{\ell-1}(x) \) in \( \mathbb{F}[x] \) such that \( x^s - 1 = p_{\ell-1}^{\ell-1}(x)p_{\ell-1}^{\ell-1}(x) \)). Now, \( h_{\ell-1}(x, y) \in I \) so according to the definition of \( I_{\ell-1} \), \( h_{\ell-1}^{\ell-1}(x) \in I_{\ell-1} = p_{\ell-1}^{\ell-1}(x) > 0 \). So

\[
h_{\ell-1}^{\ell-1}(x) = q_{\ell-1}(x)p_{\ell-1}^{\ell-1}(x)
\]

for some \( q_{\ell-1}(x) \in S \). And now, \( p_{\ell-1}^{\ell-1}(x) \in I_{\ell-1} \) so according to the definition of \( I_{\ell-1} \), there exists \( p_{\ell-1}(x, y) \in I \) such that \( p_{\ell-1}(x, y) = p_{\ell-1}^{\ell-1}(x)y^{\ell-1} \). Therefore, by equation (4)

\[
h_{\ell-1}(x, y) = h_{\ell-1}^{\ell-1}(x)y^{\ell-1} = q_{\ell-1}(x)p_{\ell-1}^{\ell-1}(x)y^{\ell-1} = q_{\ell-1}(x)p_{\ell-1}(x, y).
\]

Again since \( I \) is an ideal of \( R \), \( yp_{\ell-1}(x, y) \in I \). So according to the definition of \( I_0 \), \( p_{\ell-1}^{\ell-1}(x) \in I_0 = p_{\ell-1}^{\ell-1}(x) > 0 \). Thus,

\[
p_{\ell-1}^{\ell-1}(x) = p_0^{\ell-1}(x)t_{\ell-1}^{\ell-1}(x)
\]

for some \( t_{\ell-1}^{\ell-1}(x) \in S \), and so

\[
p_{\ell-1}(x, y) = p_0^{\ell-1}(x)t_{\ell-1}^{\ell-1}(x)y^{\ell-1}.
\]

Therefore, for an arbitrary element \( f(x, y) \in I \) we show that

\[
h_1(x, y) := f(x, y) - p_0(x, y)q_0(x)
\]

\[
h_2(x, y) := h_1(x, y) - p_1(x, y)q_1(x)
\]

\[
h_3(x, y) := h_2(x, y) - p_2(x, y)q_2(x)
\]

\[
\ldots
\]

\[
h_{\ell-1}(x, y) := h_{\ell-2}(x, y) - p_{\ell-2}(x, y)q_{\ell-2}(x)
\]

\[
h_{\ell-1}(x, y) = q_{\ell-1}(x)p_{\ell-1}(x, y).
\]

So

\[
f(x, y) = p_0(x, y)q_0(x) + p_1(x, y)q_1(x) + p_2(x, y)q_2(x)
\]

\[
+ \cdots + p_{\ell-2}(x, y)q_{\ell-2}(x) + p_{\ell-1}(x, y)q_{\ell-1}(x).
\]
Since $p_i(x, y) \in I$ for $i = 0, \ldots, \ell - 1$ and $f(x, y)$ is an arbitrary element of $I$ and $I$ is an ideal of $R$, we conclude that

$$I = \langle p_0(x, y), \ldots, p_{\ell-1}(x, y) \rangle,$$

where $p_j(x, y) = \sum_{i=j}^{\ell-1} p_0^j(x) l_i^j(x) y^i$. So $\{p_0(x, y), p_1(x, y), \ldots, p_{\ell-1}(x, y)\}$ is a set of generating polynomials for $I$.

In the next theorem, we introduce the generator matrix for TDC codes.

**Theorem 2.1.** Suppose that $I$ is an ideal of $F[x, y]/ < x^s - 1, y^\ell - 1 >$ and is generated by $\{p_0(x, y), \ldots, p_{\ell-1}(x, y)\}$, which obtained from the above method. Then the set

$$\{p_0(x, y), xp_0(x, y), \ldots, x^{s-a_0-1}p_0(x, y),$$

$$p_1(x, y), xp_1(x, y), \ldots, x^{s-a_1-1}p_1(x, y),$$

$$\vdots$$

$$p_{\ell-1}(x, y), xp_{\ell-1}(x, y), \ldots, x^{s-a_{\ell-1}-1}p_{\ell-1}(x, y)\}$$

forms an $F$-basis for $I$, where $a_i = \deg(p_i^j(x))$.

**Proof.** Assume that $l_0(x), \ldots, l_{\ell-1}(x)$ are polynomials in $F[x]$ such that $\deg(l_i(x)) < s - a_i$ and

$$l_0(x)p_0(x, y) + \cdots + l_{\ell-1}(x)p_{\ell-1}(x, y) = 0.$$

These imply the following equation in $S$

$$l_0(x)p_0^0(x) = 0.$$

Therefore, $l_0(x)p_0^0(x) = s(x)(x^s - 1)$ for some $s(x) \in F[x]$. Now, the degree of $x$ in the right side of this equation is at least $s$ but since $\deg(p_0^0(x)) = a_0$ and $\deg(l_0(x)) < s - a_0$, the degree of $x$ in the left side of this equation is at most $s - 1$. So we get $l_0(x) = 0$. Similar arguments yield $l_i(x) = 0$ for $i = 1, \ldots, \ell - 1$. \hfill \qed

3. Conclusion

In this paper, we present a novel method for studying the structure of TDC codes of length $n = s\ell$. This leads to studying the structure of ideals of the ring $F[x, y]/ < x^s - 1, y^\ell - 1 >$. By using the novel method, we obtain generating sets of polynomials and generator matrix for TDC codes.

**References**

[1] T. Ikai, H. Kosako, Y. Kojima, *Two-Dimensional Cyclic Codes*, Electronics and Communications in Japan 57-A (1975), pp. 27-35.

[2] H. Imai, *A Theory of Two-Dimensional Cyclic Codes*, Information and Control 34 (1977), pp. 1-21.

[3] Z. Sepasdar, K. Khashyarmanesh, *Characterizations of some two-dimensional cyclic codes correspond to the ideals of $F[x, y]/ < x^s - 1, y^2 - 1 >$*, Finite Fields and Their Applications 41 (2016), pp. 97-112.