CYCLIC CODES

Biljana Radičić

Singidunum University,
Belgrade, Serbia

Abstract:
In this paper, we consider cyclic codes and their extensions: quasi-cyclic codes and double cyclic codes. We show how their generator matrices can be obtained. The obtained results are illustrated by examples.

Keywords:
Circulant matrices, cyclic codes, quasi-cyclic codes, double cyclic codes, generator matrices.

1. INTRODUCTION

Let m and n be positive integer numbers, F be a field of characteristic 0 or its characteristic is coprime to n, and ω is a primitive n-th root of unity.

First, we give the definition of a circulant matrix.

Definition 1. (**A circulant matrix**) ([1]) A $n \times n$ matrix $C[c(x)]$ over the field F is called a circulant matrix associated with the polynomial

$$c(x) = \sum_{i=0}^{n-1} c_i x^i, \tag{1}$$

if $C[c(x)]$ has the following form:

$$C[c(x)] = \begin{bmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_1 \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \dots & c_0 \end{bmatrix}. \blacklozenge \tag{2}$$

As we can see, the matrix $C[c(x)]$ of the form (2) has the following property: the second row of the matrix $C[c(x)]$ is the right cyclic shift of its first row, the third row of the matrix $C[c(x)]$ is the right cyclic shift of its second row and so on. Namely, the i-th row of the matrix $C[c(x)]$ is the right cyclic shift of its $(i-1)$-th row. Thus, the matrix $C[c(x)]$ of the form (2) is completely determined by its first row. Circulant matrices have a very wide applications in numerical analysis, cryptography and

Correspondence:
Biljana Radičić

e-mail:
bradicic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2019-465-471

coding theory. In this paper, we present their applications in coding theory. It should be also pointed out that circulant matrices belong to the class of Toeplitz matrices - matrices having constant diagonals. More information about Toeplitz matrices can be found in the following papers: [2] and [3].

Example 1. *Let* $c(x)=1-x$. Then,

$$C[c(x)]=\begin{bmatrix}1 & -1\\ -1 & 1\end{bmatrix}.\ \Diamond$$

Example 2. *Let* $c(x)=3+x+2x^3$. Then,

$$C[c(x)]=\begin{bmatrix}3 & 1 & 0 & 2\\ 2 & 3 & 1 & 0\\ 0 & 2 & 3 & 1\\ 1 & 0 & 2 & 3\end{bmatrix}.\ \Diamond$$

The following definition is *a generalization* of Definition 1.

Definition 2. (**A generalized circulant matrix**) A $m\times n$ matrix $C_g[c(x)]$ over the field F is called a generalized circulant matrix associated with the polynomial (1) if $C_g[c(x)]$ has the following form:

$$C_g[c(x)]=\begin{bmatrix}c_0 & c_1 & \dots & c_{n-1}\\ c_{n-1} & c_0 & \dots & c_{n-2}\\ \vdots & \vdots & \ddots & \vdots\\ c_{n-m+1} & c_{n-m+2} & \dots & c_{n-m}\end{bmatrix} \quad (3)$$

where all the subscripts j of c_j are modulo n. ♦

Remark 1. A generalized circulant matrix becomes a circulant matrix provided that $m = n$. ▼

Example 3. Let $c(x)=1-x$ and $m=4$. Then,

$$C_g[c(x)]=\begin{bmatrix}1 & -1\\ -1 & 1\\ 1 & -1\\ -1 & 1\end{bmatrix}.\ \Diamond$$

Example 4. *Let* $c(x)=3+x+2x^3$ and $m=3$. Then,

$$C_g[c(x)]=\begin{bmatrix}3 & 1 & 0 & 2\\ 2 & 3 & 1 & 0\\ 0 & 2 & 3 & 1\end{bmatrix}.\ \Diamond$$

Let us recall that ω is a primitive n-th root of unity.

Theorem 1. ([1], [4]) The eigenvalues of the matrix $C[c(x)]$ are:

$$\lambda_j(C[c(x)])=c(\omega^j),\ \ j=\overline{0,n-1}, \quad (4)$$

and the eigenvectors of the matrix $C[c(x)]$ are:

$$v_n(\omega^j)=\begin{bmatrix}1 & \omega^j & \dots & \omega^{(n-1)j}\end{bmatrix}^T,\ \ j=\overline{0,n-1}, \quad (5)$$

where $[\ ]^T$ is the symbol for the transpose of a matrix. ∇

Therefore,

$$C[c(x)]\,v_n(\omega^j)=c(\omega^j)\ v_n(\omega^j),\ \ j=\overline{0,n-1}. \quad (6)$$

Similar to the equality (6) (in relation to a circulant matrix), it can be obtained the following equality (in relation to a generalized circulant matrix):

$$C_g[c(x)]\,v_n(\omega^j)=c(\omega^j)\ v_m(\omega^j),\ \ j=\overline{0,n-1}. \quad (7)$$

Using the previous equality, it can be obtained the following equality:

$$C_g[c(x)]\,\Phi_{n,n}(\omega)=\Phi_{m,n}(\omega)\ diag(c(1),c(\omega),\dots,c(\omega^{n-1})), \quad (8)$$

where $diag(c(1),c(\omega),\dots,c(\omega^{n-1}))$ is a diagonal $n\times n$ matrix with the elements $c(\omega^j), j=\overline{0,n-1}$, on the main diagonal, $\Phi_{n,n}(\omega)$ is the $n\times n$ Fourier matrix i.e.

$$\Phi_{n,n}(\omega)=\begin{bmatrix}1 & 1 & \dots & 1\\ 1 & \omega & \dots & \omega^{n-1}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & \omega^{n-1} & \dots & \omega^{(n-1)(n-1)}\end{bmatrix}, \quad (9)$$

and $\Phi_{m,n}(\omega)$ is its $m\times n$ generalization.

Remark 2. Let $r=\min\{m,n\}$. Any $k\times k$ submatrix of the matrix $\Phi_{m,n}(\omega)$ formed by its first k rows, where k is a positive integer number such that $k\le r$, is a Vandermonde matrix ([5], a French mathematician, musician and chemist Alexandre-Théophile Vandermonde) formed by k different elements, therefore it is a non-degenerate matrix. From that, we conclude that the rank

of the matrix $\Phi_{m,n}(\omega)$ is equal to r and the first r rows of the matrix $\Phi_{m,n}(\omega)$ are linearly independent. ▼

As we stated at the beginning of the paper, m and n are positive integer numbers and ω is any primitive n-th root of unity. Let n' be also a positive integer number, ω' be any primitive n'-th root of unity and F be a field of characteristic 0 or its characteristic is coprime to both n and n'.

Let $C_g[c(x)]$ and $C_g[c'(x)]$ be generalized circulant matrices associated, respectively, with the polynomials:

$$c(x)=\sum_{i=0}^{n-1}c_i x^i \text{ and } c'(x)=\sum_{j=0}^{n'-1}c'_j x^j. \tag{10}$$

Definition 3. (***A double circulant matrix***) A $m\times(n+n')$ matrix $C_g[c(x),c'(x)]$ over the field F is called a double circulant matrix associated with the polynomials (10) if $C_g[c(x),c'(x)]$ has the following form:

$$C_g[c(x),c'(x)]=\left[C_g[c(x)]\ \middle|\ C_g[c'(x)]\right]. \blacklozenge \tag{11}$$

Example 5. Let F be the field of complex numbers, $n=3$, $n'=2$, $c(x)=1-2x-x^2$ and $c'(x)=-1+2x$.

Then, for $m=6$,

$$C_g[c(x),c'(x)]=\begin{bmatrix}1&-2&-1&-1&2\\-1&1&-2&2&-1\\-2&-1&1&-1&2\\1&-2&-1&2&-1\\-1&1&-2&-1&2\\-2&-1&1&2&-1\end{bmatrix}. \lozenge$$

Example 6. Let F be the field of complex numbers, $n=4$, $n'=2$, $c(x)=1-2x-x^2$ and $c'(x)=-1+2x$.

Then, for $m=5$,

$$C_g[c(x),c'(x)]=\begin{bmatrix}1&-2&-1&0&-1&2\\0&1&-2&-1&2&-1\\-1&0&1&-2&-1&2\\-2&-1&0&1&2&-1\\1&-2&-1&0&-1&2\end{bmatrix}. \lozenge$$

Remark 3. (**in relation to Example 5.**) Using the elementary operations to the matrix $C_g[c(x),c'(x)]$, we obtain:

$$C_g[c(x),c'(x)]\approx\begin{bmatrix}1&-2&-1&-1&2\\0&-1&-3&1&1\\0&0&14&-8&1\\0&0&0&1&1\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}.$$

From that, we conclude that the matrix $C_g[c(x)\ c'(x)]$ has rank 4, and its first 4 rows are linearly independent. ▼

Remark 4. (**in relation to Example 6.**) Using the elementary operations to the matrix $C_g[c(x)\ c'(x)]$, we obtain:

$$C_g[c(x),c'(x)]\approx\begin{bmatrix}1&-2&-1&0&-1&2\\0&1&-2&-1&2&-1\\0&0&-2&-2&1&1\\0&0&0&2&1&-2\\0&0&0&0&0&0\end{bmatrix}.$$

From that, we conclude that the matrix $C_g[c(x),c'(x)]$ has rank 4, and its first 4 rows are linearly independent. ▼

2. CYCLIC CODES AND THEIR GENERATOR MATRICES

In this section, we consider cyclic codes and show how their_generator matrices can be obtained.

In coding theory:

- any $(c_0,c_1,\ldots,c_{n-1})\in F^n$, where F is a finite field whose characteristic is coprime to n, is called *a word over F*,
- any subspace C of F^n is called *a linear code over F*,
- the words in C are called *code words*,
- if $(c_{0,0},c_{0,1},\ldots,c_{0,n-1})$, $(c_{1,0},c_{1,1},\ldots,c_{1,n-1})$, … ,
- $(c_{r-1,0},c_{r-1,1},\ldots,c_{r-1,n-1})$ is a basis of the linear code C, then the $r\times n$ matrix

$$C_g=\begin{bmatrix}c_{0,0}&c_{0,1}&\cdots&c_{0,n-1}\\c_{1,0}&c_{1,1}&\cdots&c_{1,n-1}\\\vdots&\vdots&\ddots&\vdots\\c_{r-1,0}&c_{r-1,1}&\cdots&c_{r-1,n-1}\end{bmatrix} \tag{12}$$

is called *a generator matrix of the linear code C*.

The generator matrices are useful for *encoding* and *decoding*.

Let us consider the quotient ring $F_n[X]=F_{n-1}[X]/\langle x^n-1\rangle$ and point out that any polynomial $f(x)=\sum f_i x^i \in F_n[X]$ can be identified with a word $(f_0,f_1,\overset{i=0}{\ldots},f_{n-1})\in F^n$. Therefore, any ideal C of $F_n[X]$ can be observed as a linear code over F, called a *cyclic code over F*. Thus, any polynomial $c(x)=\sum_{i=0}^{n-1} c_i x^i$ generates *a cyclic code*:

$$C_{c(x)}=\{f(x)c(x)\bmod(x^n-1)\,|\,f(x)\in F[x]\}. \quad (13)$$

It is easy to see that the row vectors of the matrix (2) generate the linear code (13).

Remark 5. (***in relation to the matrix (2)***) In the general case, the row vectors of the matrix (2) are linearly dependent, so the matrix (2), in the general case, is not a generator matrix of a cyclic code (13). ▼

In the paper [6] the authors proved the following theorem (*in relation to a generalized circulant matrix*). Before we present the result from the paper [6], let us mention that the degree of a polynomial $f(x)$ is denoted by $\deg f(x)$.

Theorem 2. (Theorem 2.4. [6]) Let $C_g[c(x)]$ be the matrix of the form (3), $d=\deg d(x)$, where $d(x)=\gcd(c(x),x^n-1)$ and $r=\min\{m,n-d\}$. Then, the rank of the matrix $C_g[c(x)]$ is equal to r and the first r rows of the matrix $C_g[c(x)]$ are linearly independent.

Proof. The matrix $\Phi_{m,n}(\omega)\ diag(c(1),c(\omega),\ldots,c(\omega^{n-1}))$ has exactly $n-d$ non-zero columns because there are exactly d indexes j $(j=\overline{0,n-1})$ such that $c(\omega^j)=0$. Suppose that $j_t,(t=\overline{1,n-d})$ are the indexes such that $c(\omega^{j_t})\neq 0$. Then, the rank of the matrix $C_g[c(x)]\ \Phi_{n,n}(\omega)$ is equal to the rank of the following matrix:

$$\Phi_{m,n-d}(\omega)\ diag(c(\omega^{j_1}),\ldots,c(\omega^{j_{n-d}})), \quad (14)$$

where

$$\Phi_{m,n-d}(\omega)=\begin{bmatrix}1 & \ldots & 1\\ \omega^{j_1} & \ldots & \omega^{j_{n-d}}\\ \vdots & \ddots & \vdots\\ \omega^{j_1(m-1)} & \ldots & \omega^{j_{n-d}(m-1)}\end{bmatrix}. \quad (15)$$

Similar to Remark 2, we conclude that the rank of the matrix (15) is equal to $r=\min\{m,n-d\}$ and the first r rows of the matrix (15) are linearly independent. Since the matrix $diag(c(\omega^{j_1}),\ldots,c(\omega^{j_{n-d}}))$ is non-degenerate, it follows that the rank of the matrix (14) is equal to r and the first r rows of the matrix (14) are linearly independent. Therefore, based on (8), it follows that the rank of the matrix $C_g[c(x)]\Phi_{n\times n}(\omega)$ is equal to r and the first r rows of the matrix $C_g[c(x)]\Phi_{n\times n}(\omega)$ are linearly independent. Bearing in mind that the matrix (9) is a non-degenerate, it follows that the rank of the matrix $C_g[c(x)]$ is equal to r and the first r rows of the matrix $C_g[c(x)]$ are linearly independent. ∇

Remark 6. If follows, based on Theorem 2, that the first $r=n-\deg\gcd(c(x),x^n-1)$ rows of the matrix $C[c(x)]$ form a basis of the cyclic code $C_{c(x)}$. ▼

Therefore, based on Remark 6, we obtain the following results:

For Example 3, Since $c(x)=1-x$ i.e. $n=2$, it follows that $d=\deg\gcd(1-x,x^2-1)=\deg(x-1)=1$. So, $r=n-d=1$ i.e. the generator matrix of $C_{c(x)}$ is

$$C_g=[1\quad -1]. \ \Diamond \quad (16)$$

For Example 4, Since $c(x)=3+x+2x^3$ i.e. $n=4$, it follows that $d=\deg\gcd(3+x+2x^3,x^4-1)=\deg(x+1)=1$. So, $r=n-d=3$ i.e. the generator matrix of $C_{c(x)}$ is, in this case, the same as $C_g[c(x)]$. Thus,

$$C_g=\begin{bmatrix}3 & 1 & 0 & 2\\ 2 & 3 & 1 & 0\\ 0 & 2 & 3 & 1\end{bmatrix}. \ \Diamond \quad (17)$$

In coding theory, the question:

Whether or not the cyclic codes are asymptotically good?

is still open. ([7])

In the paper [8], Berman proved that cyclic codes are asymptotically bad if only finitely many primes are involved in the lengths of the codes.

Now, we consider the matrix $C_g[c(x),c'(x)]$ of the form (11) i.e. a double circulant matrix associated with the polynomials (10) and give the answer how to determine the rank of that matrix.

Similar to the equality (7), it can be obtained the following equalities:

$$C_g[c(x),c'(x)]\begin{bmatrix}v_n(\omega^i)\\ 0_{n'\times 1}\end{bmatrix}=c(\omega^i)v_m(\omega^i),\ i=\overline{0,n-1}, \quad (18)$$

$$C_g[c(x),c'(x)]\begin{bmatrix}0_{n\times 1}\\ v_{n'}(\omega'^j)\end{bmatrix}=c'(\omega'^j)v_m(\omega'^j),\ j=\overline{0,n'-1} \quad (19)$$

Also, similar to the equality (8), using the equalities (18) and (19), it can be obtained the following equality:

$$C_g[c(x),c'(x)]\cdot diag(\Phi_{n,n}(\omega),\Phi_{n',n'}(\omega'))=\Phi_{m,n+n'}(\omega,\omega')\,diag(c(1),c(\omega),\ldots,c(\omega^{n-1}),c'(1),c'(\omega'),\ldots,c'(\omega'^{n'-1}))\ .$$

Similar to Theorem 2, using the previous equality, in the paper [6], the authors also proved the following theorem.

Theorem 3. (Theorem 3.6. [6]) Let $C_g[c(x),c'(x)]$ be the matrix of the form (11), $l=\gcd(n,n')$,

$$d=\deg\frac{\gcd(c(x),x^n-1)\gcd(c'(x),x^{n'}-1)(x^l-1)}{\gcd(c(x)c'(x),x^l-1)} \qquad (21)$$

and $r=\min\{m,n+n'-d\}$. Then, the rank of the matrix $C_g[c(x),c'(x)]$ is equal to r and the first r rows of the matrix $C_g[c(x),c'(x)]$ are linearly independent. ∇

In the next section, we extend the definition of the cyclic codes.

3. THE QUASI-CYCLIC CODES OF INDEX $1\frac{1}{2}$

Let n be a positive integer number and F be a finite field whose characteristic is coprime to n. Let us recall that the quotient ring $F[X]/\langle x^n-1\rangle$ is denoted by $F_n[X]$.

The product

$$F_n[X]\times F_n[X] \qquad (22)$$

is a free $F_n[X]$ - modul of rank 2 and any $F_n[X]$ - submodule C of (22) is called *a quasi-cyclic code of index 2.* In general, any $F_n[X]$-submodule C of the free $F_n[X]$ - modul of rank m is said to be *a quasi-cyclic code of index m.*

Remark 7. Cyclic codes are just quasi-cyclic codes of index 1. ▼

In the paper [9], C. L. Chen, W. W. Peterson and E. J. Weldon showed that the quasi-cyclic codes of index 2 are asymptotically good. Moreover, for any integer $m>1$, the quasi-cyclic codes of index m are asymptotically good (see [10] and [11]) .

In the paper [6] (see also [12]), Yun Fan and Hualu Liu considered the quasi-cyclic codes of index $1\frac{1}{2}$ Namely, they considered, provided that n is a positive even integer number, the following $F_n[X]$ - modul:

$$F_n[X]\times F_{\frac{n}{2}}[X] \qquad (23)$$

Any submodule C of $F_n[X]$ - modul (23) is called a quasi-cyclic code of index $1\frac{1}{2}$.

Let

$$c(x)=\sum_{i=0}^{n-1}c_ix^i \text{ and } c'(x)=\sum_{j=0}^{\frac{n}{2}-1}c_jx^j\ . \qquad (24)$$

Then, any element ($c(x),c'(x)$) of the modul (23) generates a quasi-cyclic code $C_{c(x),c'(x)}$ of index $1\frac{1}{2}$ which is called a quasi-cyclic code of index $1\frac{1}{2}$ generated by ($c(x),c'(x)$). Namely,

$$C_{c(x),c'(x)}=\left\{\begin{matrix}(f(x)c(x)\bmod(x^n-1),f(x)c'(x)\\ \bmod(x^{\frac{n}{2}}-1))\end{matrix}\middle|\ f(x)\in F[x]\right\} \qquad (25)$$

The question is:

How to get a generator matrix of $C_{c(x)\,c'(x)}$)?

Namely, the $n\times(n+\frac{n}{2})$ matrix:

$$C_g[c(x),c'(x)]=\begin{bmatrix} c_0 & c_1 & \ldots & c_{n-1} & c'_0 & c'_1 & \ldots & c'_{\frac{n}{2}-1}\\ c_{n-1} & c_0 & \ldots & c_{n-2} & c'_{\frac{n}{2}-1} & c'_0 & \ldots & c_{\frac{n}{2}}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ c_{\frac{n}{2}+1} & c_{\frac{n}{2}+2} & \ldots & c_{\frac{n}{2}} & c'_1 & c'_2 & \ldots & c'_0\\ c_{\frac{n}{2}} & c_{\frac{n}{2}+1} & \ldots & c_{\frac{n}{2}-1} & c'_0 & c'_1 & \ldots & c'_{\frac{n}{2}-1}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ c_1 & c_2 & \ldots & c_0 & c'_1 & c'_2 & \ldots & c'_0 \end{bmatrix} \qquad (26)$$

is a double circulant matrix associated with the polynomials (24).

Remark 8. (***in relation to the matrix*** (26)) In the general case, the row vectors of the matrix (26) are linearly dependent. So, in the general case, the matrix (26) is not a generator matrix of the quasi-cyclic code (25). ▼

Before we continue, let us recall that n is a positive even integer number and F is a finite field whose characteristic is coprime to n.

In relation to the matrix $C_g[c(x),c'(x)]$ of the form (26), in the paper [6], the authors proved the following theorem.

Theorem 4. Theorem 4.1. [6]) Let $C_g[c(x),c'(x)]$ be the matrix of the form (26), $d_1=\gcd(c(x),x^{\frac{n}{2}}+1)$ and $d_2=\gcd(c(x),c'(x),x^{\frac{n}{2}}-1)$. Then, the rank of the matrix $C_g[c(x),c'(x)]$ is equal to $r=n-\deg(d_1\cdot d_2)$

and the first r rows of the matrix $C_g[c(x),c'(x)]$ are linearly independent i.e. the first r rows of the matrix $C_g[c(x),c'(x)]$ form a generator matrix of the quasi-cyclic code (25). ∇

The following example illustrates the result of Theorem 4.

Example 7. Let $F = Z_5$, $n = 6$, $c(x) = c'(x) = 1 + x + x^2$

Then,

$$C_g[c(x)\ c'(x)] = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Since,

$$d_1 = \gcd(1 + x + x^2, x^3 + 1) = 1$$

and

$$d_2 = \gcd(1 + x + x^2, 1 + x + x^2, x^3 - 1) = 1 + x + x^2,$$

it follows that

$$r = 6 - \deg(1 + x + x^2) = 4.$$

Therefore,

$$C_g = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

is a generator matrix of the quasi-cyclic code $C_{1+x+x^2,\ 1+x+x^2}$ of index $1\frac{1}{2}$. ◊

4. DOUBLE CYCLIC CODES

In this section, n and n' are positive integer numbers and F is a field whose characteristic is coprime to both n and n'.

Now, we consider the product:

$$F_n[X] \times F_{n'}[X] \qquad (27)$$

as an $F[X]$- module. Any $F[X]$ - submodule C of that modul is called *a double cyclic code.*

Remark 9. (***in relation to the product*** (27)) Let us point out that the product (27) is neither an $F_n[X]$ - module nor an $F_{n'}[X]$ - module. Namely, the product (27) can be viewed as $F_k[X]$ - module, where $k = lcm(n, n')$.

Let $c(x)$ and $c'(x)$ be polynomials (10) and $C_g[c(x),c'(x)]$ be the matrix of the form (11). Then, any element ($c(x),c'(x)$) of the modul (27) generates a double cyclic code $C_{c(x),c'(x)}$ which is called a double cyclic generated by ($c(x),c'(x)$). Namely,

$$C_{c(x),c'(x)} = \left\{ \begin{matrix} (f(x)c(x) \bmod (x^n - 1), f(x)c'(x) \bmod \\ (x^{n'} - 1)) \end{matrix} \middle| f(x) \in F[x] \right\}. \qquad (28)$$

The question is:

How to get a generator matrix of $C_{c(x)\,c'(x)}$)?

From Theorem 3, it can be proved the following theorem.

Theorem 5. (Theorem 4.3. [6]) Let $k = lcm(n, n')$ and $C_g[c(x),c'(x)]$ be the $k \times (n + n')$ matrix of the form (11). Let $l = \gcd(n, n')$,

$$d = \deg \frac{\gcd(c(x), x^n - 1)\gcd(c'(x), x^{n'} - 1)(x^l - 1)}{\gcd(c(x)c'(x), x^l - 1)} \qquad (29)$$

and $r = n + n' - d$. Then, the rank of the matrix $C_g[c(x),c'(x)]$ is equal to r and the first r rows of the matrix $C_g[c(x),c'(x)]$ are linearly independent. ∇

The following example illustrates the result of Theorem 5.

Example 8. Let $F = Z_5$, $n = 3$, $n' = 2$, $c(x) = -x + x^2$ and $c'(x) = -1 + x$. Then, $k = lcm(3,2) = 6$ and $l = \gcd(3,2) = 1$;

$\gcd(-x + x^2, x^3 - 1) = x - 1$;
$\gcd(-1 + x, x^2 - 1) = x - 1$ and
$\gcd((-x + x^2)(-1 + x), x - 1) = x - 1$ i.e.

$d = \deg(x^2 - 1) = 2$.

So, based on Theorem 5, the rank of the following double circulant matrix

$$C_g\left[c(x),c'(x)\right]=\begin{bmatrix}0&-1&1&-1&1\\1&0&-1&1&-1\\-1&1&0&-1&1\\0&-1&1&1&-1\\1&0&-1&-1&1\\-1&1&0&1&-1\end{bmatrix}$$

is $r=3+2-2=3$ i.e. the first 3 rows of $C_g\left[c(x),c'(x)\right]$ are linearly independent. Thus, the first 3 rows of $C_g\left[c(x),c'(x)\right]$ form a generator matrix of the double cyclic code $C_{-x+x^2,\ -1+x}$ i.e.

$$C_g=\begin{bmatrix}0&-1&1&-1&1\\1&0&-1&1&-1\\-1&1&0&-1&1\end{bmatrix}$$

is a generator matrix of the double cyclic code $C_{-x+x^2,\ -1+x}$. ◊

REFERENCES

[1] P. J. Davis, Circulant matrices, Wiley, New York, 1979.

[2] R. M. Gray, Toeplitz and circulant matrices: A review, Found. Trends Commun. Inf. Theory 2(3) (2006), 155-239.

[3] I. S. Iohvidov, Hankel and Toeplitz matrices and forms: Algebraic Theory, Birkhäuser, Boston, 1982.

[4] R. S. Varga, Eigenvalues of circulant matrices, Pacific J. Math., 4(1) (1954), 151-160.

[5] Wikipedia, Vandermonde matrix, https://en.wikipedia.org/wiki/ Vandermonde_matrix.

[6] Y. Fan, H. Liu, Double circulant matrices, arXiv:1601.06872v1, January, 2016.

[7] C. Martínez-Pérez, W. Willems, Is the class of cyclic codes asymptotically good? IEEE Trans. Inform. Theory, 52 (2006), 696-700.

[8] S. D. Berman, Semisimple cyclic and Abelian codes II, Cybernetics, 3 (1967), 17-23.

[9] C. L. Chen, W. W. Peterson, E. J. Weldon, Some results on quasi-cyclic codes, Information and Control, 15 (1969), 407-423.

[10] Y. Fan, L. Lin, Thresholds of random quasi-Abelian codes, IEEE Trans. Inform. Theory, 61(1) (2015), 82-90.

[11] S. Ling, P. Solé, Good self-dual quasi-cyclic codes exist, IEEE Trans. Inform. Theory, 49 (2003), 1052-1053.

[12] Y. Fan, H. Liu, Quasi-cyclic codes of index , arXiv:1505.02252, May 2015.