ON QUASI-CYCLIC CODES OF INDEX 1½

Biljana Radičić*

Singidunum University,
Belgrade, Serbia

Abstract:

Quasi-cyclic codes of index 1½ are considered in this paper. Our main aim is to show how we can obtain generator matrices of such codes. It should be emphasized that generator matrices are not uniquely determined. The method of obtaining generator matrices will be illustrated with examples.

Keywords:

A quasi-cyclic code; a circulant matrix; generator matrices of a code.

INTRODUCTION

In the introduction section of this paper we give some important definitions which are necessary for understanding the text. Suppose that F is a finite field (i.e. a field that have a finite number of elements). The examples of finite fields which are the most common in the literature are the rings $(Z_p, +_p, \bullet_p)$, where p is a prime number. Suppose that n is a natural number. A word (of length n) over F is any $(f_0, f_1, \ldots, f_{n-1})$, where $f_i \in F, i = 0, n-1$. A linear code (of length n) is any subspace C of F^n. If $dim(C)=r$ (i.e. $(c_{0,0},c_{0,1},\ldots c_{0,n-1})$, $(c_{1,0},c_{1,1},\ldots c_{1,n-1})$,...., $(c_{r-1,0},c_{r-1,1},\ldots c_{r-1,n-1})$ is a basis of a linear code C) then the following $r \times n$ matrix

$$\begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{r-1,0} & c_{r-1,1} & \cdots & c_{r-1,n-1} \end{bmatrix} \quad (1)$$

is a generator matrix of a linear code C.

In the paper [1] the author proved that linear codes are asymptotically good.

Correspondence:
Biljana Radičić

e-mail:
bradicic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2022-44-48

The question is:

"When we say that codes are asymptotically good? "

In order to give the answer to that question we need to define *the rate of C* (the symbol - R(C)) and the *relative minimum distance of C* (the symbol – Δ(C)). Namely,

$$R(C)=\frac{\dim(C)}{n} \quad \text{and} \quad \Delta(C)=\frac{d}{n} \tag{2}$$

where d is the minimum Hamming distance of C (an American mathematician *Richard Wesley Hamming*, 1915 - 1998). Before we continue, let us recall the following: *The Hamming distance* between $c=(c_0,c_1,\ldots,c_{n-1})\in C$ and $c'=(c'_0,c'_1,\ldots,c'_{n-1})\in C$ is the number of positions at which c and c' are different.

Example 1. (*The Hamming distance*) In this example we will determine the Hamming distance between

a) **00000** and **11111**. In this case the Hamming distance is 5;

b) 2564318 and 2769378. In this case the Hamming distance is 3;

c) tara and tama. In this case the Hamming distance is 1. ◊

If the sequence $C_1, C_2, \ldots$ of codes (of length $n_i, i=1,2,\ldots$, going to infinity) over the field F satisfies:

$$R(C_i) \text{ and } \Delta(C_i) \text{ are positively bounded from below} \tag{3}$$

then for such sequence of codes we say that it is a asymptotically good. If inside of some class of codes there exist asymptotically good sequences of codes then for such class of codes we say that it is a asymptotically good class of codes.

Suppose that Π_n is a permutation group on the index set $\{1,2,\ldots,n\}$ of coordinates of F^n. For a linear code C (in F^n) we say that it *is invariant* by the Π_n- action if : $\forall \pi\in\Pi_n$, $\forall c\in C,\ \pi(c)\in C$.

If $\Pi_n=\langle(12\ldots n)\rangle$ is a cyclic group generated by the cycle (12 ... n) and C is invariant by the Π_n- action (in F^n), then C is called *a cyclic code of length n.*

The answer to the question:

„Are the cyclic codes asymptotically good?" (4)

has not been given yet [2].

If $\Pi_n=\langle(12\ldots n)(n+1,n+2,\ldots,2n)\rangle$ is a cyclic group generated by the product of the corresponding two cycle (12 ... n) and (n+1, n+2,..., 2n) and C is invariant by the Π_n - action (in $F^n\times F^n$), then C is called *a quasi-cyclic code of index 2 and co-index n*.

Generaly, if Π_n is a permutation which is the product of m disjoint cycles of length n and C is invariant by the Π_n - action (in $\underbrace{F^n\times\cdots\times F^n}_{m}$), then C is called a *quasi-cyclic code of index m and co-index n.*

2. A QUASI-CYCLIC CODE OF INDEX $1\frac{1}{2}$

The product

$$F_{2n}[X]\times F_n[X] \tag{5}$$

is considered, where $F[X]/\langle x^n-1\rangle$ is denoted by $F_n[X]$ (i.e. $F[X]/\langle x^{2n}-1\rangle$ is denoted by $F_{2n}[X]$).

Each element of (5) is represented (uniquely) as $(g(x),g'(x))$, where

$$g(x)=\sum_{i=0}^{2n-1}g_ix^i \quad \text{and} \quad g'(x)=\sum_{j=0}^{n-1}g'_jx^j \tag{6}$$

and $g_i,g'_j\in F, i=\overline{0,2n-1}, j=\overline{0,n-1}$.

The element $(g(x),g'(x))$ can be identified with the word

$$(g_0,\ldots,g_{2n-2},g_{2n-1},g'_0,\ldots,g'_{n-1})\in F^{2n}\times F^n. \tag{7}$$

Suppose that π is a permutation of the coefficients of $F^{2n}\times F^n$ which is the product of 2 disjoint cycles of length $2n$ and n such that

$$\begin{aligned}&\pi(g_0,\ldots,g_{2n-2},g_{2n-1},g'_0,\ldots,g'_{n-2},g'_{n-1})=\\&(g_{2n-1},g_0,\ldots,g_{2n-2},g'_{n-1},g'_0,\ldots,g'_{n-2})\end{aligned} \tag{8}$$

Hence, the permutation π (on $F^{2n}\times F^n$) is corresponding to the operation by multiplying X (on $F_{2n}[X]\times F_n[X]$).

$$X(g(x),g'(x))=(Xg(x)(\mathrm{mod}\,x^{2n}-1),Xg'(x)(\mathrm{mod}\,x^n-1)) \tag{9}$$

If a linear subspace C of $F_{2n}[X]\times F_n[X]$ is invariant by the permutation π i.e.

$$\forall(g(x),g'(x))\in C \qquad X(g(x),g'(x))\in C \tag{10}$$

then C is *called a quasi-cyclic code over F of index* $1\frac{1}{2}$ *and co-index* $2n$.

The operation by multiplying X (on $F_{2n}[X]\times F_n[X]$). can be extended as follows:

For any $f(x)\in F[X]$ and any $(g(x),g'(x))\in F_{2n}[X]\times F_n[X]$

$$\begin{aligned}&f(x)(g(x),g'(x))=\\&(f(x)g(x)(\mathrm{mod}\,x^{2n}-1),f(x)g(x)(\mathrm{mod}\,x^n-1)).\end{aligned} \tag{11}$$

The previous operation can be abbreviated (on $F_{2n}[X]\times F_n[X]$) as follows:

$$f(x)(g(x),g'(x))=(f(x)g(x),f(x)g'(x)) \tag{12}$$

The product (5) is an $F_{2n}[X]$ - module and its $F_{2n}[X]$ - submodules are just the quasi-cyclic codes of index $1\frac{1}{2}$ and co-index $2n$. An $F_{2n}[X]$ - submodule of (5) is generated by at most two elements.

Let $(g(x),g'(x))$ be any element of the product (5), then the set

$$\{(f(x)g(x),f(x)g'(x))\in F_{2n}[X]\times F_n[X] \mid f(x)\in F_{2n}[X]\} \quad (13)$$

is a quasi-cyclic code of index $1\frac{1}{2}$ and co-index n generated by $(g(x),g'(x))$ and will be denoted by $C_{g(x),g'(x)}$.

We will deal with the following question:

How to get a generator matrix of $C_{g(x),g'(x)}$? (14)

The generator matrix of $C_{g(x),g'(x)}$ will be denoted by $\hat{G}[g(x),g'(x)]$.

Let

$$g(x)=g_0+g_1x+\ldots+g_{2n-1}x^{2n-1} \text{ and}$$
$$g'(x)=g'_0+g'_1x+\ldots+g'_{n-1}x^{n-1}. \quad (15)$$

Using the coefficients $g_i, i=\overline{0,2n-1}$ i.e. a word $(g_0,g_1,\ldots,g_{2n-1})$ (of length $2n$) and the coefficients $g'_j, j=\overline{0,n-1}$ i.e. a word $(g'_0,g'_1,\ldots,g'_{n-1})$ (of length n) the following matrices of the order $2n$ and n, respectively, are constructed:

$$G[g(x)]=\begin{bmatrix} g_0 & g_1 & \cdots & g_{2n-1} \\ g_{2n-1} & g_0 & \cdots & g_{2n-2} \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \cdots & g_0 \end{bmatrix} \text{ and}$$

$$G'[g'(x)]=\begin{bmatrix} g'_0 & g'_1 & \cdots & g'_{n-1} \\ g'_{n-1} & g'_0 & \cdots & g'_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ g'_1 & g'_2 & \cdots & g'_0 \end{bmatrix}. \quad (16)$$

As we can see the matrices $G[(g(x)]$ and $G'[g'(x)]$ are constructed such that they have the following property: its *i*-th row is the right cyclic shift of its (*i* -1)-th row. The matrices with such property are called *circulant matrices.* We will single out just some of the most important information in relation to these matrices: 1. If A, B are circulant matrices then AB=BA; 2. If A is a circulant matrix A^{-1} then is also a circulant matrix. For more information about these matrices we suggest the following papers: [3] and [4]. Circulant matrices belong to the class of *Toeplitz matrices* (a German mathematician *Otto Toeplitz,* 1881-1940) which have the following form:

$$T=\begin{bmatrix} t_0 & t_1 & \cdots & t_{n-2} & t_{n-1} \\ t_{-1} & t_0 & \ddots & t_{n-3} & t_{n-2} \\ t_{-2} & t_{-1} & \ddots & \ddots & t_{n-3} \\ \vdots & \vdots & \ddots & \ddots & t_1 \\ t_{1-n} & t_{2-n} & \cdots & t_{-1} & t_0 \end{bmatrix} \quad (17)$$

Example 2. (The examples of Toeplitz matrices)

$$T_1=\begin{bmatrix} 1 & 8 & 0 & 2 & 4 \\ 5 & 1 & 8 & 0 & 2 \\ 3 & 5 & 1 & 8 & 0 \\ 7 & 3 & 5 & 1 & 8 \\ 9 & 7 & 3 & 5 & 1 \end{bmatrix} \text{ and } T_2=\begin{bmatrix} 1 & 3 & 0 & 2 & 4 \\ 4 & 1 & 3 & 0 & 2 \\ 2 & 4 & 1 & 3 & 0 \\ 0 & 2 & 4 & 1 & 3 \\ 3 & 0 & 2 & 4 & 1 \end{bmatrix}. \Diamond \quad (18)$$

More information about Toeplitz matrices can be found in [5], [6] and [7].

Using the matrices (16) the following $2n\times 3n$ matrix is constructed:

$$G[g(x),g'(x)]=\begin{bmatrix} g_0 & g_1 & \cdots & g_{2n-1} & g'_0 & g'_1 & \cdots & g'_{n-1} \\ g_{2n-1} & g_0 & \cdots & g_{2n-2} & g'_{n-1} & g'_0 & \cdots & g'_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{n+1} & g_{n+2} & \cdots & g_n & g'_1 & g'_2 & \cdots & g'_0 \\ g_n & g_{n+1} & \cdots & g_{n-1} & g'_0 & g'_1 & \cdots & g'_{n-1} \\ g_{n-1} & g_n & \cdots & g_{n-2} & g'_{n-1} & g'_0 & \cdots & g'_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \cdots & g_0 & g'_1 & g'_2 & \cdots & g'_0 \end{bmatrix}. \quad (19)$$

Namely, it is easy to see that:

$$C_{g(x),g'(x)}=\{(f_0,f_1,\ldots,f_{2n-1})G[g(x),g'(x)] \mid (f_0,f_1,\ldots,f_{2n-1})\in F^{2n}\}. \quad (20)$$

The matrix (19) does not have to be a generator matrix of $C_{g(x),g'(x)}$ because its rank does not have to be equal to *2n*. In order to give the answer to the question (14) we need the following theorem presented and proved in the paper [8] by *Y. Fan and H. Liu.*

Theorem 1. (Theorem 2.4. [8]) Suppose that the polynomials $p_{g(x),g'(x)}(x)$ and $r_{g(x),g'(x)}(x)$, for any, $(g(x),g'(x))\in F_{2n}[X]\times F_n[X]$ are defined as follows:

$$p_{g(x),g'(x)}(x)=\gcd(g(x),x^n+1)\cdot\gcd(g(x),g'(x),x^n-1) \text{ and}$$
$$r_{g(x),g'(x)}(x)=\frac{x^{2n}-1}{p_{g(x),g'(x)}(x)}. \quad (21)$$

Then, $(g(x),g'(x))$ induces an $F_{2n}[X]$ -homomorphism $h_{g(x),g'(x)}: F_{2n}[X]\to F_{2n}[X]\times F_n[X]$ such that:

$$f(x)\xrightarrow{h_{g(x),g'(x)}}(f(x)g(x),f(x)g'(x)) \quad (22)$$

and

$$Ker(h_{g(x),g'(x)})=\left\langle r_{g(x),g'(x)}(x)\right\rangle_{F_{2n}[x]} \quad (23)$$

i.e.

$$\dim(C_{g(x),g'(x)})=\deg(r_{g(x),g'(x)}(x)) \quad (24)$$

Proof.

Namely,

$$q(x)\in Ker\left(h_{g(x),g'(x)}\right)$$

if and only if

$$q(x)g(x) \equiv 0 \,(\mathrm{mod}\, x^{2n}-1) \text{ and } q(x)g'(x) \equiv 0 \,(\mathrm{mod}\, x^{n}-1)$$

if and only if

$$q(x)g'(x) \equiv 0 \,(\mathrm{mod}\, x^{n}+1),\ q(x)g'(x) \equiv 0 \,(\mathrm{mod}\, x^{n}-1)$$

and $q(x)g'(x) \equiv 0 \,(\mathrm{mod}\, x^{n}-1)$

If and only if

$$q(x)g(x) \equiv 0 \,(\mathrm{mod}\, x^{n}+1) \text{ and}$$
$$q(x)\gcd(g(x),g'(x)) \equiv 0 \,(\mathrm{mod}\, x^{n}-1)$$

if and only if

$$q(x) \equiv 0 \ (\mathrm{mod}\frac{x^{n}+1}{\gcd(g(x),x^{n}+1)}) \text{ and}$$
$$q(x) \equiv 0 \ (\mathrm{mod}\frac{x^{n}-1}{\gcd(g(x),g(x),x^{n}-1)})$$

if and only if

$$q(x) \equiv 0 \ (\mathrm{mod}\frac{x^{n}+1}{\gcd(g(x),x^{n}+1)} \cdot \frac{x^{n}-1}{\gcd(g(x),g'(x),x^{n}-1)})$$

i.e.

$$q(x) \in \left\langle r_{g(x),g'(x)}(x) \right\rangle_{F_{2n}[x]}$$

Especially,

$$\dim(C_{g(x),g'(x)}) = \dim(F_{2n}[X]) - \dim(Ker(h_{g(x),g'(x)}))$$
$$= 2n - \deg(p_{g(x),g'(x)}(x)) = \deg(r_{g(x),g'(x)}(x)) \,.\ \blacklozenge$$

Finally, we shall give the two examples and in these examples we shall illustrate the method of obtaining a generator matrix of $C_{g(x),g'(x)}$.

Example 3. Let $n=2$, $F=(Z_{2.}+_2,\bullet_2)$, $g(x)=1+x^3$ and $g'(x)=x$.

Then,

$$C[1+x^3] = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ and } C'[x] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (25)$$

i.e.

$$C[1+x^3,x] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}. \quad (26)$$

Since,

$$p_{1+x^3,x}(x) = \gcd(1+x^3,x^2+1)\cdot\gcd(1+x^3,x,x^2-1) = 1$$

and

$$r_{1+x^3,x}(x) = \frac{x^4-1}{p_{1+x^3,x}(x)} = \frac{x^4-1}{1} = x^4-1\,,$$

based on Theorem 1, it follows that

$$\dim(C_{1+x^3,x}) = \deg(r_{1+x^3,x}(x)) = 4 \quad (27)$$

i.e. the generator matrix of $C_{1+x^3,x}$ is equal to the matrix (26). ◊

Example 4. Let $n=2$, $F=(Z_{3.}+_3,\bullet_3)$, $g(x)=1+x+x^2+x^3$ and $g'(x)=2+x$.

Then,

$$C[1+x+x^2+x^3] = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \text{ and } C'[2+x] = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \quad (28)$$

i.e.

$$C[1+x+x^2+x^3,2+x] = \begin{bmatrix} 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 \\ 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 \end{bmatrix}. \quad (29)$$

Since,

$$p_{1+x+x^2+x^3,2+x}(x) = \gcd(1+x+x^2+x^3,x^2+1)\cdot$$
$$\gcd(1+x+x^2+x^3,2+x,x^2-1) = x^2+1$$

and

$$r_{1+x+x^2+x^3,2+x}(x) = \frac{x^4-1}{p_{1+x+x^2+x^3,2+x}(x)} = \frac{x^4-1}{x^2+1} = x^2-1\,,$$

based on Theorem 1, it follows that

$$\dim(C_{1+x+x^2+x^3,2+x}) = \deg(r_{1+x+x^2+x^3,2+x}(x)) = 2$$

i.e. the generator matrix of $C_{1+x+x^2+x^3,2+x}$ is

$$\hat{C}[1+x+x^2+x^3,2+x] = \begin{bmatrix} 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 \end{bmatrix}. \lozenge \quad (30)$$

3. REFERENCES

[1] R. R. Varshamov, Estimate of the number of signals in error-correcting codes (in Russian), Dokl. Acad. Nauk, vol.117, pp. 739-741, 1957.

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

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

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

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

[6] S. Serra-Capizzano, C. Garoni, Generalized Locally Toeplitz Sequences: Theory and Application - Volume I, Springer, 2017.

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

[8] Y. Fan, H. Liu, Quasi-cyclic codes of index 1.5 , arXiv:1505.02252v1, May 2015.