ADVANCED COMPUTING SESSION

ON QUASI-CYCLIC CODES OF INDEX 1⅓

Biljana Radičić

Faculty of Informatics and Computing,
Singidunum University,
Belgrade, Serbia

Abstract:
The main subject of this paper are quasi-cyclic codes of index 1⅓. We show how to obtain generator matrices of such codes. Generator matrices are not uniquely determined. At the end of this paper we illustrate the result by examples. It should be also mention that generator matrices have wide application in encoding and decoding.

Keywords:
Quasi-cyclic code; generator matrices of a code.

1. INTRODUCTION

Suppose that F is a finite field (i.e. the field with a finite number of elements) and n is a natural number.

In that case,

- *a word over F* is any $(c_0, c_1, \ldots, c_{n-1}) \in F^n$,
- *a linear code of length n over F* is any subspace C of F^n,
- *code words* are the words in C,
- *a generator matrix of the linear code C* is the $r \times n$ matrix

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

assuming that a basis of the linear code C consists of

$(c_{0,0}, c_{0,1}, \ldots, c_{0,n-1}), (c_{1,0}, c_{1,1}, \ldots, c_{1,n-1}), \ldots,$

$(c_{r-1,0}, c_{r-1,1}, \ldots, c_{r-1,n-1})$,

- the fraction $\frac{\dim(C)}{n}$, where $dimC$ is the dimension

Correspondence:
Biljana Radičić

e-mail:
bradicic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2020-307-311

of C, is called *the rate of* C and denoted by R(C).

Let us point out that the dimension of C is equal to the rank of its generator matrix i.e.

$$\dim(C) = r \tag{2}$$

The subject of our research are quasi-cyclic codes of index **1⅓**.

First, we shall recall the definition of a cyclic code.

Now, we consider the index set $\{1,2,\ldots,n\}$ of coordinates of F^n, the permutation group S_n on that set and the linear code C (in F^n) that satisfies the following:

$$\forall \sigma \in S_n, \forall c \in C, \sigma(c) \in C\ . \tag{3}$$

In that case we say that C is an S_n - *acted code* or an S_n- *permutation code* (see [1], [2], [3] and [4]).

Definition 1. (***A cyclic code***) ([5]) If S_n is a cyclic group generated by the (12...*n*) i.e. $S_n = \langle (12\ldots n) \rangle$ and C is an S_n- acted code, then C is called *a cyclic code of length n*. ∇

Suppose that m is also a natural number.

Definition 2. (***A quasi-cyclic code of index m and co-index n***) ([5]) If Π is the permutation group generated by the product of m disjoint cycles of length n. Then, the subspace C of

$$\underbrace{F^n \times \cdots \times F^n}_{m} \tag{4}$$

which is invariant by Π is called a *quasi-cyclic code of index m and co-index n*. ∇

The main result and the examples are given in the next section.

2. A QUASI-CYCLIC CODE OF INDEX 1⅓

If we do not mention otherwise, n is an odd natural number and F is the field with only two elements - 0 and 1 (i.e. the binary field). The operations + and ∘ (in F) are defined as follows:

+	0	1
0	0	1
1	1	0

∘	0	1
0	0	0
1	0	1

(5)

Let the quotient ring $F[X]/\langle x^n - 1 \rangle$ is denoted by $F_n[X]$.

We consider the product:

$$F_{3n}[X] \times F_n[X]. \tag{6}$$

Each element of (6) is represented (uniquely) as $(c(x), c'(x))$ where

$$c(x) = \sum_{i=0}^{3n-1} c_i x^i \quad \text{and} \quad c'(x) = \sum_{j=0}^{n-1} c'_j x^j. \tag{7}$$

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

$$(c_0, \ldots, c_{3n-2}, c_{3n-1}, c'_0, \ldots, c'_{n-1}) \in F^{3n} \times F^n. \tag{8}$$

Suppose that π is a permutation of the coefficients of $F^{3n} \times F^n$ which is the product of 2 disjoint cycles of length 3n and n such that

$$\pi(c_0, \ldots, c_{3n-2}, c_{3n-1}, c'_0, \ldots, c'_{n-2}, c'_{n-1}) = (c_{3n-1}, c_0, \ldots, c_{3n-2}, c'_{n-1}, c'_0, \ldots, c'_{n-2}) \tag{9}$$

Hence, the permutation π (on $F^{3n} \times F^n$) is corresponding to the operation by multiplying X (on $F_{3n}[X] \times F_n[X]$).

$$X(c(x), c'(x)) = (Xc(x) (\mathrm{mod}\, x^{3n} - 1), Xc'(x) (\mathrm{mod}\, x^n - 1)). \tag{10}$$

According to *Definition 2.* the following can be obtained:

If a linear subspace C of $F_{3n}[X] \times F_n[X]$ is invariant by the permutation π i.e.

$$\forall (c(x), c'(x)) \in C \quad X(c(x), c'(x)) \in C, \tag{11}$$

then C is called a *quasi-cyclic code over F of index 1⅓ and co-index 3n.*

The operation (10) can be extended in the following way:

For any $f(x) \in F[X]$ and any $(c(x), c'(x)) \in F_{3n}[X] \times F_n[X]$

$$f(x)(c(x), c'(x)) = (f(x)c(x) (\mathrm{mod}\, x^{3n} - 1), f(x)c'(x) (\mathrm{mod}\, x^n - 1)) \tag{12}$$

The operation (12) can be abbreviated (on $F_{3n}[X] \times F_n[X]$) as follows:

$$f(x)(c(x), c'(x)) = (f(x)c(x), f(x)c'(x)) \tag{13}$$

Remark 1. Let ($c(x),c'(x)$) be any element of (6), then the set

$$\{(f(x)c(x),f(x)c'(x))\in F_{3n}[X]\times F_n[X]\,|\,f(x)\in F_{3n}[X]\} \qquad (14)$$

is a quasi-cyclic code of index 1⅓ and co-index *n* generated by $(c(x),c'(x))$ and will be denoted by $C_{c(x),c'(x)}$.

The main question, in relation to $C_{c(x),c'(x)}$, is:

How can a generator matrix of ($C_{c(x),c'(x)}$) be obtained? (15)

The generator matrix of $C_{c(x),c'(x)}$ will be denoted $\hat{C}[c(x),c'(x)]$ by. Before we represent the answer to the previous question, let us point out that generator matrices have wide application in encoding and decoding.

Let

$$c(x)=c_0+c_1x+\ldots+c_{3n-1}x^{3n-1}$$

and

$$c'(x)=c'_0+c'_1x+\ldots+c'_{n-1}x^{n-1}.$$

Then, from $(c_0,c_1,\ldots,c_{3n-1})$ (a 3*n*-dimensional vector i.e. a word of length 3*n*) and $(c'_0,c'_1,\ldots,c'_{n-1})$ (a *n*-dimensional vector i.e. a word of length *n*) the following matrices of the order 3*n* and *n*, respectively, are constructed:

$$C[c(x)]=\begin{bmatrix} c_0 & c_1 & \ldots & c_{3n-1}\\ c_{3n-1} & c_0 & \ldots & c_{3n-2}\\ \vdots & \vdots & \ddots & \vdots\\ c_1 & c_2 & \ldots & c_0 \end{bmatrix} \qquad (16)$$

And

$$C'[c'(x)]=\begin{bmatrix} c'_0 & c'_1 & \ldots & c'_{n-1}\\ c'_{n-1} & c'_0 & \ldots & c'_{n-2}\\ \vdots & \vdots & \ddots & \vdots\\ c'_1 & c'_2 & \ldots & c'_0 \end{bmatrix}. \qquad (17)$$

Before we continue, let us mention that (16) and (17) represent *circulant matrices* – matrices having the following property: its second row is obtaned from its first row by moving one place to the right, its third row is obtaned from its second row by moving one place to the right and so on. Namely, its i-th row is obtained from its *(i -1)*-th row by moving one place to the right. Circulant matrices have a wide range of applications in many areas. Some of them are signal and image processing, communications, coding theory, probability, statistics, numerical analysis, engineering model and economy. More information about circulant matrices can be found in [6] and [7].

From (16) and (17) the following matrix is constructed:

$$C[c(x),c'(x)]=\begin{bmatrix} c_0 & c_1 & \ldots & c_{3n-1} & c'_0 & c'_1 & \ldots & c'_{n-1}\\ c_{3n-1} & c_0 & \ldots & c_{3n-2} & c'_{n-1} & c'_0 & \ldots & c'_{n-2}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ c_{2n+1} & c_{2n+2} & \ldots & c_{2n} & c'_1 & c'_2 & \ldots & c'_0\\ c_{2n} & c_{2n+1} & \ldots & c_{2n-1} & c'_0 & c'_1 & \ldots & c'_{n-1}\\ c_{2n-1} & c_{2n} & \ldots & c_{2n-2} & c'_{n-1} & c'_0 & \ldots & c'_{n-2}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ c_{n+1} & c_{n+2} & \ldots & c_n & c'_1 & c'_2 & \ldots & c'_0\\ c_n & c_{n+1} & \ldots & c_{n-1} & c'_0 & c'_1 & \ldots & c'_{n-1}\\ c_{n-1} & c_n & \ldots & c_{n-2} & c'_{n-1} & c'_0 & \ldots & c'_{n-2}\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ c_1 & c_2 & \ldots & c_0 & c'_1 & c'_2 & \ldots & c'_0 \end{bmatrix}$$

i.e. the $3n\times 4n$ matrix that has the following form:

$$C[c(x),c'(x)]=\begin{bmatrix} C[c(x)] & C'[c'(x)]\\ & C'[c'(x)]\\ & C'[c'(x)] \end{bmatrix}. \qquad (18)$$

It is easy to see that

$$C_{c(x),c'(x)}=\{(f_0,f_1,\ldots,f_{3n-1})C[c(x),c'(x)]\,|\,(f_0,f_1,\ldots,f_{3n-1})\in F^{3n}\}.$$

But, the rank of the matrix (18) does not have to be equal to 3*n* i.e. the matrix (18) does not have to be a generator matrix of $C_{c(x),c'(x)}$. The answer to the question (15) is given by the following theorem proving by *Y. Fan and H. Liu* in the paper [5].

Before we give that theorem and its proof, let us recall the following symbols:

- *Ker(f)* - the symbol for the *kernel of f*;
- *gcd(q(x),w(x))* - the symbol for the *greatest common divisor* of *q(x)* and *w(x)*.

Theorem 1. (Theorem 3. [5]) Suppose that $q_{c(x),c'(x)}(x)$ and $w_{c(x),c'(x)}(x)$, for any $(c(x),c'(x))\in F_{3n}[X]\times F_n[X]$, are defined as follows:

$$q_{c(x),c'(x)}(x)=\gcd(c(x),x^{2n}+x^n+1)\cdot\gcd(c(x),c'(x),x^n-1)$$

and

$$w_{c(x),c'(x)}(x)=\frac{x^{3n}-1}{q_{c(x),c'(x)}(x)}.$$

Then, $(c(x), c'(x))$ induces an $F_{3n}[X]$-homomorphism $h_{c(x),c'(x)} : F_{3n}[X] \to F_{3n}[X] \times F_n[X]$ such that:

$$f(x) \xrightarrow{h_{c(x),c'(x)}} (f(x)c(x), f(x)c'(x))$$

and $Ker(h_{c(x),c'(x)})$ is equal to $\left\langle w_{c(x),c'(x)}(x) \right\rangle_{F_{3n}[X]}$ i.e.

$$\dim(C_{c(x),c'(x)}) = \deg(w_{c(x),c'(x)}(x)).$$

Proof.

Namely, $\nu(x) \in Ker\left(h_{c(x),c'(x)}\right)$ if and only if

$$\begin{aligned} \nu(x)c(x) &\equiv 0 \pmod{x^{3n}-1} \\ \nu(x)c'(x) &\equiv 0 \pmod{x^n-1} \end{aligned}$$

$$\hat{C}[c(x), c'(x)]$$

if and only if

$$\begin{aligned} \nu(x)c(x) &\equiv 0 \pmod{x^{2n}+x^n+1} \\ \nu(x)c(x) &\equiv 0 \pmod{x^n-1} \\ \nu(x)c'(x) &\equiv 0 \pmod{x^n-1} \end{aligned}$$

if and only if

$$\begin{aligned} \nu(x)c(x) &\equiv 0 \pmod{x^{2n}+x^n+1} \\ \nu(x)\gcd(c(x),c'(x)) &\equiv 0 \pmod{x^n-1} \end{aligned}$$

if and only if

$$\nu(x) \equiv 0 \pmod{\frac{x^{2n}+x^n+1}{\gcd(c(x), x^{2n}+x^n+1)}}$$

$$\nu(x) \equiv 0 \pmod{\frac{x^n-1}{\gcd(c(x), c'(x), x^n-1)}}$$

if and only if

$$\nu(x) \equiv 0 \pmod{\frac{x^{2n}+x^n+1}{\gcd(c(x), x^{2n}+x^n+1)} \cdot \frac{x^n-1}{\gcd(c(x), c'(x), x^n-1}}$$

i.e.

$$\nu(x) \in \left\langle w_{c(x),c'(x)} \right\rangle_{F_{3n}[X]}$$

Especially,

$$\begin{aligned} &\dim(C_{c(x),c'(x)}) = \dim(F_{3n}[X]) - \dim(Ker(h_{c(x),c'(x)})) \\ &= 3n - \deg(q_{c(x),c'(x)}(x)) = \deg(w_{c(x),c'(x)}(x)). \Diamond \end{aligned}$$

Based on the previous theorem, we can obtain a generator matrix of $C_{c(x),c'(x)}$ in the following way:

I step: Determine (for given *c(x)* and *c'(x))* the matrices (16) and (17);

II step: Construct the matrix (18);

III step: Determine $r = \dim(C_{c(x),c'(x)})$;

IV step: Constuct the matrix $\hat{C}[c(x), c'(x)]$ using the rows of the matrix (18) i.e. using any r rows of the matrix (18) (for example, using the first *r* rows of the matrix (18)).

At the end of this paper, we shall give two examples and illustrate how to get a generator matrix of $C_{c(x),c'(x)}$.

Namely,

- in the first example: a generator matrix of $C_{c(x),c'(x)}$ *will be equal* to the matrix (18);
- in the second example: a generator matrix of $C_{c(x),c'(x)}$ *will not be equal* to the matrix (18);

Example 1. Let $c(x) = 1 + x^2$ and $c'(x) = 1$ then,

$$C[1+x^2] = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \text{ and } C'[1] = [1]$$

i.e.

$$C[1+x^2, 1] = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad (19)$$

Since,

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

and

$$w_{1+x^2,1}(x) = \frac{x^3-1}{q_{1+x^2,1}(x)} = \frac{x^3-1}{1} = x^3 - 1,$$

based on Theorem 1., it follows that

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

i.e. the generator matrix of $C_{1+x^2,1}$ is equal to the matrix (19).

Therefore,

$$\hat{C}[1+x^2,1]=\begin{bmatrix}1&0&1&1\\1&1&0&1\\0&1&1&1\end{bmatrix}. \ \Diamond$$

Example 2. Let $n=3, c(x)=x+x^2+x^3=x(1+x+x^2)$ and $c'(x)=1+x+x^2$. Then,

$$C[x+x^2+x^3]=\begin{bmatrix}0&1&1&1&0&0&0&0&0\\0&0&1&1&1&0&0&0&0\\0&0&0&1&1&1&0&0&0\\0&0&0&0&1&1&1&0&0\\0&0&0&0&0&1&1&1&0\\0&0&0&0&0&0&1&1&1\\1&0&0&0&0&0&0&1&1\\1&1&0&0&0&0&0&0&1\\1&1&1&0&0&0&0&0&0\end{bmatrix}$$

and

$$C'[1+x+x^2]=\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}$$

i,e

$$C[x+x^2+x^3,1+x+x^2]=\begin{bmatrix}0&1&1&1&0&0&0&0&0&1&1&1\\0&0&1&1&1&0&0&0&0&1&1&1\\0&0&0&1&1&1&0&0&0&1&1&1\\0&0&0&0&1&1&1&0&0&1&1&1\\0&0&0&0&0&1&1&1&0&1&1&1\\0&0&0&0&0&0&1&1&1&1&1&1\\1&0&0&0&0&0&0&1&1&1&1&1\\1&1&0&0&0&0&0&0&1&1&1&1\\1&1&1&0&0&0&0&0&0&1&1&1\end{bmatrix}$$

Since,

$$q_{x+x^2+x^3,1+x+x^2}(x)=\gcd(x^3+x^2+x,x^6+x^3+1)$$
$$\cdot\gcd(x^3+x^2+x,x^2+x+1,x^3-1)=x^2+x+1$$

and

$$w_{x+x^2+x^3,1+x+x^2}(x)=\frac{x^9-1}{q_{x+x^2+x^3,1+x+x^2}(x)}=$$
$$\frac{x^9-1}{x^2+x+1}=x^7+x^6+x^4+x^3+x+1,$$

based on Theorem 1., it follows that

$$\dim(C_{x+x^2+x^3,1+x+x^2})=\deg(w_{x+x^2+x^3,1+x+x^2}(x))=7$$

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

$$\hat{C}[x+x^2+x^3,1+x+x^2]=\begin{bmatrix}0&1&1&1&0&0&0&0&0&1&1&1\\0&0&1&1&1&0&0&0&0&1&1&1\\0&0&0&1&1&1&0&0&0&1&1&1\\0&0&0&0&1&1&1&0&0&1&1&1\\0&0&0&0&0&1&1&1&0&1&1&1\\0&0&0&0&0&0&1&1&1&1&1&1\\1&0&0&0&0&0&0&1&1&1&1&1\end{bmatrix}. \ \Diamond$$

REFERENCES

[1] P. J. Cameron, Permutation codes, European Journal of Combinatorics, vol. 31, no. 2, 2010, pp. 482-490. https://doi.org/10.1016/j.ejc.2009.03.044

[2] W. Chu, C. J. Colbourn, P. Dukes, Constructions for permutation codes in powerline communications, Designs, Codes and Cryptography, vol. 32, no 1-3, 2004, pp. 51–64.

[3] Y. Fan, Y. Yuan, On self-dual permutation codes, Acta Mathematica Scientia., vol. 28, no. 3, 2008, pp. 633-638. https://doi.org/10.1016/S02529602(08)60065-X

[4] H. Tarnanen, Upper bounds on permutation codes via linear programming, European Journal of Combinatorics, vol. 20, no. 1, 1999, pp. 101-114. https://doi.org/10.1006/eujc.1998.0272

[5] Y. Fan, H. Liu, Quasi-cyclic codes of index 1⅓, IEEE Transactions on Information Theory, vol. 62, no. 11, 2016, pp. 6342 – 6347. https://doi.org/10.1109/TIT.2016.2602842

[6] P. J. Davis, Circulant matrices, AMS Chelsea Publishing, 1994.

[7] I. Kra, S. Simanca, On circulant matrices, Notices of the American Mathematical Society, vol. 59, no. 3, 2012, pp. 369-377.