



SOME NEW TERNARY LINEAR CODES

Dr. Plamen Hristov
Assistant Professor of Mathematics,
Department of Mathematics,
Technical University of Gabrovo, Bulgaria

Abstract: Let $[n, k, d]_q$ code be a linear code of length n , dimension k and minimum Hamming distance d over $GF(q)$. One of the most important problems in coding theory is to construct codes with best possible minimum distances. In this paper new one-generator quasi-cyclic (QC) codes over $GF(3)$ are presented. Some of the results are received by construction X.

Keywords: Linear codes, Quasi - cyclic codes, Construction X.

I. INTRODUCTION

Let $GF(q)$ denote the Galois field of q elements. A linear code C over $GF(q)$ of length n , dimension k and minimum Hamming distance d is called an $[n, k, d]_q$ - code.

A code C is said to be quasi-cyclic (QC) if a **cyclic shift** of a codeword by p positions results in another codeword. A cyclic shift of an m -tuple $(x_0, x_1, \dots, x_{m-1})$ is the m -tuple $(x_{m-1}, x_0, \dots, x_{m-2})$.

The blocklength, n , of a QC code is a multiple of p , so that $n = mp$.
A matrix B of the form

$$\begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \cdots & b_{m-3} & b_{m-2} \\ b_{m-2} & b_{m-1} & b_0 & \cdots & b_{m-4} & b_{m-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ b_1 & b_2 & b_3 & \cdots & b_{m-1} & b_0 \end{pmatrix}$$

is called a **circulant matrix**. A class of QC codes can be constructed from $m \times m$ circulant matrices. In this case, the generator matrix G can be represented as

$$G = [B_1, B_2, \dots, B_p], \quad (1)$$

where $B_i, 1 \leq i \leq p$, are circulant matrices.

The algebra of $m \times m$ circulant matrices over $GF(q)$ is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^m - 1)$ if B is mapped onto the polynomial,

$$b(x) = b_0 + b_1x + b_2x^2 + \dots + b_{m-1}x^{m-1},$$

formed from the entries in the first row of B . The $b^i(x)$ associated with a QC code are called the **defining polynomials**.

If the defining polynomials $b_i(x)$ contain a common factor, which is also a factor of $x^m - 1$, then the QC code is called **degenerate**. The dimension k of the QC code is equal to the degree of $h(x)$, where

$$h(x) = (x^m - 1) / \gcd\{x^m - 1, b_0(x), \dots, b_p(x)\}$$

If the polynomial $h(x)$ has degree m , the dimension of the code is m , and (1) is a generator matrix. If $\deg(h(x)) = k < m$, a generator matrix for the code can be constructed by deleting $m - k$ rows of (1).

Theorem 1 [2]: Let C be a one-generator QC code over $GF(q)$ of length $n = mp$. Then, a generator $g(x) \in GF(q)[x]/(x^m - 1)^p$ of C has the following form

$$g(x) = (f_1(x)g_1(x), f_2(x)g_2(x), \dots, f_p(x)g_p(x)), \text{ where } g_i(x) \mid (x^m - 1) \\ \text{and } (f_i(x), (x^m - 1)/g_i(x)) = 1 \text{ for all } 1 \leq i \leq p.$$

Let the defining polynomials of the code C be in the next form

$$d_1(x) = g(x), d_2(x) = f_2(x)g(x), \dots, d_p(x) = f_p(x)g(x),$$

$$\text{where } g(x) \mid (x^m - 1) \text{ and } g(x), f_i(x) \in GF(q)[x]/(x^m - 1), \\ (f_i(x), (x^m - 1)/g(x)) = 1$$

$$\text{and } \deg(f_i(x)) < m - \deg(g(x))$$

for all $1 \leq i \leq p$. Then C is a degenerate QC code, which is one-generator QC code and for this code $n = mp$, and $k = m - \deg(g(x))$.

Theorem 2: (Construction X)

Let $C_2 = [n, k - l, d + s]_q$ code be a subcode of the code $C_1 = [n, k, d]_q$ and let $C_3 = [a, l, s]_q$ be a third code. Then there exists an $C = [n + a, k, d + s]_q$ code.

In this paper, one-generator QC codes ($p > 1$) are constructed, using an algebraic-combinatorial computer search, similar to that in [2], [3].

The codes presented here, improve the respective lower bounds on the minimum distance in [1].

II. THE METHOD

We have restricted our search to one-generator QC codes with a generator of the form as in Theorem 1. with one generator polynomial $g(x)$ and $f_1(x) = 1$. Let $q = 3$, $m = 32$.

Let us consider $[32p, 17]_3$, $p = 2, \dots, 4$, one-generator QC linear codes. First, using Berlekamp's algorithm, we factorize $x^{32} - 1$. There are nine multipliers:

$$x^{32} - 1 = (x^8 + 2x^4 + 2)(x^8 + x^4 + 2)(x^4 + x^2 + 2)(x^4 + 2x^2 + 2)(x^2 + x + 2)(x^2 + 2x + 2)(x^2 + 1) \\ (x + 1)(x + 2).$$

For $k = 17$ has 30 possibilities to obtain $g(x)$ of degree 15. We checked for these possibilities consecutively, using nonexhaustive search, and when

$$g(x) = x^{15} + 2x^{14} + x^{13} + x^{12} + 2x^{10} + x^9 + 2x^8 + x^7 + x^6 + 2x^5 + x^3 + 2,$$

$$f_1(x) = x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + 2x^2 + 2,$$

$$f_2(x) = x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + x + 1 \text{ and}$$

$$f_3(x) = x^{10} + x^9 + 2x^8 + x^7 + 2x^6 + x^5 + 2x^4 + x + 1,$$

$$[128, 17, 63]_3 \text{ code is obtained.}$$

By same way, we consider all other one-generator QC linear codes.

III. NEW QC CODES

Theorem 3 There exist new one-generator quasi-cyclic codes with parameters (Table 1) [1]:

Table 1

$[66,12,33]_3$	$[168,15,90]_3$	$[60,17,24]_3$	$[128,17,63]_3$
$[112,21,48]_3$	$[170,21,81]_3$	$[182,21,88]_3$	$[160,22,75]_3$
$[182,22,87]_3$	$[112,24,45]_3$	$[138,24,60]_3$	

Proof: The defining polynomials of the new codes are:

1. $[66,12,33]_3$:

2122122211100000000000,1001002021011121100000,1201001220201000121000;

2. $[168,15,90]_3$:

10012001110120000201202221011222010122000100000000000000,
21012001100021202121022002210212220111120201101110000000,
22011002201122012011101020222012022211100001112110000000;

3. $[60,17,24]_3$:

21210000000000000000,20100110112210000000,21210101021021100000;

4. $[128,17,63]_3$:

20010211212011210000000000000000,10120022202220122010220011122100,
20121020211001121010210100000000,22012110221222222121111201000000;

5. $[112,21,48]_3$:

11122002110022011220010011220220011100000000000000000000,
222122202200011112212010200112221212200220100000000000000;

6. $[170,21,81]_3$:

12202111111201110001002002012000002122210002201011222001111221111000000000
000000000000 ,
10100020202112110001112200120202011020012102020221202101002102002110111210
0000 0000000;

7. $[182,21,88]_3$:

111102120021011012021001212220200122012100010002202011000110200012200010000000
0000000000000,
210100000100201102210002002111112020002002120212021212022121100012101201211100
0 000 0000000000;

8. $[160,22,75]_3$:

2022012111111201012002011021010111002121120110111112100010000000000000000000,
21220221211022211011211011011201102201211012021221110212111022210210000000000000;

9. $[182,22,87]_3$:

2020001211100102101020222000201001010011022101210010121122212100221011000000000000000000
0,
11021012121200102220211100222010000112221121000110121220020200120202010102100000000000000
0;

10. $[112,24,45]_3$:

200102100210022221210121210222100000000000000000000000000,

$$\left(\begin{array}{c|c} G_2 & \mathbf{0} \\ \hline * & G_3 \end{array} \right)$$

where G_2 and G_3 are generator matrices of codes C_2 and C_3 , respectively, and $(*)$ denotes k_3 linear independent codewords of code C_1 .

V. NEW DERIVED CODES

There are trivial constructions. Given a linear code with parameters $[n, k, d]_3$, we can obtain some other codes as follows: through shortening $[n-1, k-1, d]_3$ code, through puncturing $[n-1, k, d-1]_3$ code and extendcode $[n+1, k, d]_3$.

For example, by $[112, 24, 45]_3$ code, there exist $[111, 23, 45]_3$, $[111, 24, 44]_3$ and $[113, 24, 45]_3$ codes.

VI. REFERENCES

- [1] M. Grassl, Linear code bound [electronic table; online], { <http://www.codetables.de>}.
- [2] I. Siap, N. Aydin and D. Ray-Chaudhury, "New Ternary Quasi-Cyclic Codes with Better Minimum Distances", Designs, Codes and Cryptography, vol. 24, (2001), 313–326.
- [3] R.Daskalov, Pl.Hristov, "One-Generator Quasi-Cyclic Ternary Linear Codes.", In Proceedings of Ninth International Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, June 16-22, (2004), 101-106.