Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 96-101*

Some new linear codes over GF(4)

Plamen Hristov plhristov@tugab.bg
Department of Mathematics, Technical University of Gabrovo, 5300 Gabrovo, BULGARIA

Dedicated to the memory of Professor Stefan Dodunekov

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, thirty two codes over $GF(4)$ are constructed, which improve the best known lower bounds on minimum distance. Some codes are quasi-cyclic and other are obtained by Construction X.

1 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 or p-QC) if a cyclic shift of a codeword by p positions results in another codeword. A cyclic shift of an m-tuple $(x_0, x_1, \ldots, x_{m-1})$ is the m-tuple $(x_{m-1}, x_0, \ldots, x_{m-2})$. The blocklength, n, of a p-QC code is a multiple of p, so that $n = pm$.

A matrix B of the form

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \cdots & b_{m-3} & b_{m-2} \\ b_{m-2} & b_{m-1} & b_0 & \cdots & b_{m-4} & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ b_1 & b_2 & b_3 & \cdots & b_{m-1} & b_0 \end{bmatrix}, \quad (1)$$

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

$$G = [B_1,\ B_2,\ \ldots,\ B_p], \quad (2)$$

where B_i is a circulant matrix.
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, $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{m-1} x^{m-1}$, 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 [4]

$$h(x) = \frac{x^m - 1}{\gcd\{x^m - 1, b_0(x), b_1(x), \cdots, b_{p-1}(x)\}}. \quad (3)$$

If the polynomial $h(x)$ has degree m , the dimension of the code is m , and (2) 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 (2).

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

$$d_1(x) = g(x),\ d_2(x) = f_2(x)g(x),\ \cdots\ ,\ d_p(x) = f_p(x)g(x), \quad (4)$$

where $g(x)|(x^m - 1), g(x), f_i(x) \in GF(q)[x]/(x^m - 1), \quad (f_i(x), (x^m - 1)/g(x)) = 1$ and $\deg f_i(x) < m - \deg g(x)$ for all $1 \le i \le p$. Then C is a degenerate QC code, which is one-generator QC code (see [4],[2]) and for this code $n = mp$, and $k = m - \deg g(x)$.

In this paper we consider one-generator QC codes. A well-known result regarding the one-generator QC codes is:

Theorem 1 [4],[2]: Let C be a one-generator QC code over $GF(q)$ of length $n = pm$. Then, a generator $\mathbf{g(x)} \in (GF(q)[x]/(x^m - 1))^p$ of C has the following form

$$\mathbf{g(x)} = (f_1(x)g_1(x), f_2(x)g_2(x), \cdots, f_p(x)g_p(x))$$

where $g_i(x)|(x^m - 1)$ and $(f_i(x), (x^m - 1)/g_i(x)) = 1$ for all $1 \le i \le p$.

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, new one-generator QC codes ($p \ge 2$) are constructed using a algebraic-combinatorial computer search, similar to that in [3] and [5]. For convenience, the elements of $GF(4)$ are given as integers: $2 = \alpha, 3 = \alpha^2$ where α is a root of the binary primitive polynomial $y^2 + y + 1$. The codes presented here improve the respective lower bounds on the minimum distance in [1].

2 The New QC Codes

We have restricted our search to one-generator QC codes with a generator of the form as in Theorem 1, where $g_1(x) = g_2(x) = \ldots = g_p(x) = g(x)$ and

Table 1: A search for $[102, 8, 68]_4$ quasi-cyclic code

p	$17p$	f_p	d	d_{gr}	p	$17p$	f_p	d	d_{gr}
2	34	1013	18	19	5	85	300301	54	56
3	51	1133	30	32	6	102	1120101	68	66
4	68	121312	42	44	7	119	22201	78	79

Table 2: A search for $[119, 8, 80]_4$ quasi-cyclic code

p	$17p$	f_p	d	d_{gr}	p	$17p$	f_p	d	d_{gr}
2	34	1013	18	19	5	85	3310101	54	56
3	51	1133	30	32	6	102	11231	66	66
4	68	121312	42	44	7	119	300301	80	79

$f_1(x) = 1$. The main aim in our search is to find good $g(x)$, which gives better minimum distance for $p = 2$. After that with the given m and $g(x)$ we search for $f_p(x), p = 3, 4, \dots$. Depending of the degree of $g(x)$, we obtain improvements on minimum distances for some dimensions.

We illustrate the search method in the following example.
Let $m = 17$ and $q = 4$. Then the $\gcd(m, q) = 1$ and the splitting field of $x^m - 1$ is $GF(q^l)$ where l is the smallest integer such that $m|(q^l - 1)$. In our case $l = 4$ and so splitting field is $GF(4^4)$. Using Berlekamp's algorithm we factorize

$$x^{17} - 1 = (x^4 + x^3 + 2x^2 + x + 1)(x^4 + x^3 + 3x^2 + x + 1)(x^4 + 2x^3 + x^2 + 2x + 1)$$

$$(x^4 + 3x^3 + x^2 + 3x + 1)(x + 1)$$

Let now k=8. There are six possibilities to obtain $g(x)$ of degree nine. By this reason, we can use exhaustive search. By $g(x) = x^9 + 3x^8 + 3x^7 + 2x^5 + 2x^4 + 3x^2 + 3x + 1$, we obtain $f_2(x) = x^3 + x + 3$ and quasi-cyclic code $[34, 8, 18]_4$. After that we make search for $f_p(x), p = 3, 4 \dots, 7$. It should be noticed, there is a possibility to go one or more steps back. The results are given in Table 1 and Table 2.

Theorem 3: There exist new one-generator quasi-cyclic codes with parameters:

$[102,8,68]_4$	$[105,8,69]_4$	$[119,8,80]_4$	$[76,9,28]_4$	$[95,9,60]_4$
$[36,10,18]_4$	$[60,10,34]_4$	$[66,10,26]_4$	$[140,10,90]_4$	$[36,11,17]_4$
$[115,11,70]_4$	$[161,11,102]_4$	$[51,12,26]_4$	$[69,12,38]_4$	$[184,12,116]_4$
$[189,12,120]_4$	$[60,14,29]_4$			

Proof. The coefficients of the defining polynomials of the codes are as follows:

A $[105, 8, 69]_4$**-code:**
11231011220231000000O,20310012230322132100O,30212333033111112211O,
30300211230121321100O,22103102021023020100O;

A $[76, 9, 48]_4$**-code:**
1233010223100000000,2133021210332100000,3113332321211133100,1331133011331130310;

A $[140, 10, 90]_4$**-code:**
1022022113013302232222310310000000000,2333303213232302120301203222011000O,
1132211101031321222030321031231100O,2322201133300132033001132303222100O;

A $[184, 12, 116]_4$**-code:**
11000111010100000000000,31102023222223102100000,21332320311011032221000,
20213001211023021010000,23322210221021323010000,31310230032031323320100,
23230111212332313100000,21332103103203023310000;

Remark: The defining polynomials of the QC codes, which are missing in Theorem 3, are given in [1]. All defining polynomials, generator matrices and weight enumerators are available on request from the author.

In process of search for new quasi-cyclic codes, we obtain many good codes. Some of these codes are extendable. Below are given the parameters of new linear codes, which are constructed using extension. The same codes are presented by trivial construction X in [1].

Theorem 4: There exist new linear codes with parameters:

$$[32{,}10{,}16]_4 \quad [51{,}10{,}28]_4 \quad [43{,}11{,}22]_4 \quad [31{,}12{,}13]_4 \quad [72{,}12{,}40]_4$$
$$[143{,}12{,}88]_4 \quad [43{,}13{,}19]_4 \quad [46{,}13{,}21]_4 \quad [52{,}13{,}25]_4 \quad [43{,}15{,}18]_4$$

Proof. The coefficients of defining polynomials of good quasi-cyclic codes are presented. The column vectors, which are added to the generator matrices, are given.

A $[30, 10, 14]_4$**-code:**
3230131101,3100211331,1002010101;
$(1010101010)^T, (0101010101)^T$;

A $[50, 10, 27]_4$**-code:**
3313300021,1311103311,1211120310,2100232231,3303010001;
$(1111111111)^T$;

A $[42, 11, 21]_4$**-code:**
101010110010000000000,302311022031322310100З;
$(32132132132)^T$;

A $[30, 12, 12]_4$**-code:**
203100000000000,221120300331000;
$(231231231231)^T$;

A $[70, 12, 38]_4$**-code:**

Table 3: New linear codes obtained by Construction X

C_1	C_2	C_3	C
$[45,10,24]_4$	$[45,8,26]_4$	$[3,2,2]_4$	$[48,10,26]_4$
$[140,10,90]_4$	$[140,7,92]_4$	$[4,3,2]_4$	$[144,10,92]_4$
$[126,11,78]_4$	$[126,8,82]_4$	$[6,3,4]_4$	$[132,11,82]_4$
$[126,16,70]_4$	$[126,10,78]_4$	$[15,6,8]_4$	$[141,16,78]_4$

1312002031003103002321010000000000000,10221132220100010222330312331010000;
$(111111111111)^T, (222222222222)^T$;
A $[140, 12, 85]_4$**-code:**
1312002031003103002321010000000000000,23113101211132303001120113110000000,
11201021102123032223023302320100000,20303101202202301233022112323030100;
Three columns $(111111111111)^T$;
A $[42, 13, 18]_4$**-code:**
210233331000000000000,310330322333310110000;
$(3213213213213)^T$;
A $[45, 13, 20]_4$**-code:**
221000000000000,211220312100000,200110031221000;
$(1111111111111)^T$;
A $[51, 13, 24]_4$**-code:**
11211000000000000,23130230332301000,31103133122210000;
$(1111111111111)^T$;
A $[42, 15, 17]_4$**-code:**
122322100000000000000,322023230031012100000;
$(321321321321321)^T$
The code $[105, 8, 69]_4$(see Theorem 3) is triple extendable. The respective columns are $(10110110)^T, (01101101)^T, (11011011)^T$.

Theorem 5: There exist new linear codes with parameters:

$$[48,10,26]_4 \quad [144,10,92]_4 \quad [132,11,82]_4 \quad [141,16,70]_4$$

Proof. In Table 3 is showed the connection between the codes C_1, C_2, C_3 and C, according to Theorem 2. For clearness, the defining polynomials of codes C_1 and C_2 are given:
1.A $[45, 10, 24]_4$**-code:**
301021000000000,202232032013100,122011101030310;
1.B $[45, 8, 26]_4$**-code:**
220302110000000,113011203211001,221310122332110;
2.A $[140, 10, 90]_4$**-code:** (see Theorem 3)
2.B $[140, 7, 92]_4$**-code:**

331310121010301323212202023230000000,13012001232012000201330112020213330,
301030110002211101303321213221211133,13312021133021132012210100031023213;
3.A $[126, 11, 78]_4$**-code:**
130203303031312233132012112013223210331030020213212310000000000,
310003311132300021300020111031231220113332302120312331112100000;
3.B $[126, 8, 82]_4$**-code:**
232000230230132023322003200121130110011310203232323332010000000,
130011011010130331203333323032323103120233333202113203103321100;
4.A $[126, 16, 70]_4$**-code:**
121000001021111203322023302003121100032231222031000000000000000,
112200020302031022222210322323201031201300113223213131000000000;
4.B $[126, 10, 78]_4$**-code:**
322322132312212200203230220202100121133130221231003121000000000,
302033311022312333122110102033101300203033303020233032103021000;
One generator matrix of code C is constructed by the indicated way:

$$G = \left(\begin{array}{c} G_2 \mid 0 \\ - - - \\ * \quad \mid G_3 \end{array} \right),$$

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

References

[1] M. Grassl, Linear code bound [electronic table; online], `http://www.codetables.de`.

[2] K. Lally, P. Fitzpatrick, Construction and classification of quasi-cyclic codes, Proc. *Int. Workshop on Coding and Cryptography, WCC'99*, Paris, France, (1999), 11–20.

[3] I. Siap, N. Aydin, D. Ray-Chaudhury, New ternary quasi-cyclic codes with better minimum distances, *IEEE Trans. Inform. Theory*, vol. 46, no. 4, (2000), 1554–1558.

[4] G. E. Séguin, G. Drolet, The theory of 1-generator quasi-cyclic codes, Technical Report, Royal Military College of Canada, Kingston, ON, 1991.

[5] P. Hristov, Some new linear codes over small finite fields, In Proc. of Sixth Int. Workshop on Optimal Codes and Related Topics, White Lagoon, Balchik, Bulgaria, June 16-22, (2009), 93-102.