Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 129-133*

New linear codes over GF(8)[1]

Plamen Hristov plhristov@tugab.bg
Department of Mathematics, Technical University of Gabrovo,
5300 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. Recently, the class of quasi-cyclic (QC) codes has been proven to contain many such codes. In this paper, thirty two codes over $GF(8)$ are constructed (among them one optimal code), which improve the best known lower bounds on minimum distance.

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.*

[1] This work was partially supported by the Bulgarian National Science Fund under Contract in TU–Gabrovo.

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]

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

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

$$d_1(x) = g(x),\ d_2(x) = f_2(x)g(x),\ \cdots\ ,\ d_p(x) = f_p(x)g(x), \tag{4}$$

where $g(x)|(x^m-1), g(x), f_i(x) \in GF(q)[x]/(x^m-1)$, $(f_i(x), (x^m-1)/g(x)) = 1$ 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 $k = m - \deg\ g(x)$.

Similarly to the case of cyclic codes, an p-QC code over $GF(q)$ of length $n = pm$ can be viewed as an $GF(q)[x]/(x^m-1)$ submodule of $(GF(q)[x]/(x^m-1))^p$ [4],[2]. Then an r-generator QC code is spanned by r elements of $(GF(q)[x]/(x^m-1))^p$.

In this paper we consider one-generator QC codes. A well-known results regarding the one-generator QC codes are as follows.

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

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

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 [2]: Let C be an one-generator QC code over $GF(q)$ of length $n = pm$ with a generator of the form

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

where $g(x)|(x^m-1), g(x), f_i(x) \in GF(q)[x]/(x^m-1)$ and $(f_i(x), (x^m-1)/g(x)) = 1$ for all $1 \le i \le p$. Then

$$p.((\#\text{ of consecutive roots of } g(x)) + 1) \le d_{\min}(C)$$

and the dimension of C is equal to $m - \deg\ g(x)$.

Theorem 3 (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.

Table 1: Minimum distances of the $[17p, 8, d]_8$ quasi-cyclic codes

p	$17p$	f_p	d	d_{gr}	p	$17p$	f_p	d	d_{gr}
2	34	1025246	21	21	5	85	1003347	62	61
3	51	1536	34	35	6	102	1237534	76	75
4	68	147711	48	49	7	119	1014524	90	89

Quasi-cyclic codes form an important class of linear codes. A large number of record breaking (and optimal codes) are QC codes [1]. In this paper, new one-generator QC codes ($p \geq 2$) are constructed using a algebraic-combinatorial computer search, similar to that in [3]. For convenience, the elements of $GF(8)$ are given as integers: $2 = \beta, 4 = \beta^2, 3 = \beta^3, 6 = \beta^4, 7 = \beta^5, 5 = \beta^6$, where β is a root of the binary primitive polynomial $y^3 + y + 1$. The codes presented here (Table 2) 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 2 and $f_1(x) = 1$. The main aim in our search is to find good $g(x)$, i.e. $g(x)$ which gives better minimum distance for $p = 2$ due to Theorem 2. When choosing $g(x)$ we calculate the minimum distance of the respective quasi-cyclic code D. After that we have compared the $d_{\min}(D)$ with the minimum distance of the best known codes [1] and with the given m and $g(x)$ we search for $f_p(x), p = 3, 4, \ldots$. 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 $q = 8$. 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 $l = 8$ and so our splitting field is $GF(8^8)$. One of the generating polynomial for $GF(8^8)$ is a primitive polynomial $p(x) = x^8 + 2x^7 + 6x^6 + x^5 + x^4 + x^3 + 4^2 + 3x + 6$ and let α be a root of $p(x)$. Then

$$x^{17} - 1 = \prod_{j=0}^{16} (x - \alpha^j)$$

Let now $k = 8$. There are two possibilities to obtain $g(x)$ of degree nine. By this reason, we can use exhaustive search. Taken $g(x) = x^9 + x^8 + x^6 + x^3 + x + 1$, we obtain $f_2(x) = x^6 + 2x^4 + 5x^3 + 2x^2 + 4x + 6$ and quasi-cyclic code $D = [34, 8, 21]_8$, the best known. After that we make search for $f_p(x), p = 3, 4 \ldots, 7$. This is a sequence of six quasi-cyclic codes. The results are given in Table 1.

It seems, that there are three new results: $[85, 8, 62]_8$, $[102, 8, 76]_8$ and $[119, 8, 90]_8$ codes. We present the new quasi-cyclic codes.

Theorem 1: There exist one-generator quasi-cyclic codes with parameters:

$[28,5,20]_8$	$[35,5,26]_8$	$[42,5,32]_8$	$[49,5,38]_8$	$[78,5,63]_8$	$[81,5,65]_8$
$[90,5,73]_8$	$[105,5,86]_8$	$[120,5,100]_8$	$[38,6,28]_8$	$[42,6,30]_8$	$[84,6,66]_8$
$[95,6,75]_8$	$[42,7,29]_8$	$[84,7,63]_8$	$[90,7,68]_8$	$[95,7,72]_8$	$[105,7,81]_8$
$[36,8,23]_8$	$[42,8,28]_8$	$[85,8,62]_8$	$[91,8,67]_8$	$[102,8,76]_8$	$[105,8,78]_8$
$[119,8,90]_8$	$[39,9,24]_8$	$[91,9,65]_8$	$[102,9,74]_8$	$[105,9,76]_8$	$[93,11,62]_8$

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

A $[28, 5, 20]_8$**-code:** 2310000,7712210,4343110,1642100; Adding the columns $(63421)^t$, $(25641)^t$, $(47261)^t$ and $(52371)^t$ to the generator matrix, the above code can be extended to a $[32, 5, 24]_8$ code.

A $[35, 5, 26]_8$**-code:** 2310000,4575210,1612510,5131710,1201310; Adding the columns $(63421)^t$, $(25641)^t$ and $(52371)^t$, the above code can be extended to a $[38, 5, 29]_8$ code.

A $[49, 5, 38]_8$**-code:** 2310000,6722100,4556310,2644510,5473410,3265310,3415210; Adding the columns $(74531)^t$ and $(52371)^t$, the above code can be extended to a $[51, 5, 40]_8$ code.

A $[38, 6, 28]_8$**-code:** 1301247742103100000,6333647125776166100; Adding the columns $(130100)^t$ and $(164361)^t$, the above code can be extended to a $[40, 6, 29]_8$ code.

A $[42, 6, 30]_8$**-code:** 6432343617331251000000,5377215221334555427100; Adding the columns $(630210)^t$, $(520710)^t$, $(602301)^t$, $(703401)^t$, $(063021)^t$ and $(052071)^t$, the above code can be extended to a $[48, 6, 36]_8$ code.

A $[42, 7, 29]_8$**-code:** 255356150702751000000,506312404625072547100 ; Adding the column $(3657521)^t$, the above code can be extended to a $[43, 7, 30]_8$ code.

A $[84, 7, 63]_8$**-code:** 255356150702751000000,506312404625072547100,
442406377267775621000,354174272601230173510; Adding the columns $(0630210)^t$, $(5703401)^t$ and $(5063021)^t$, the above code can be extended to an $[87, 7, 66]_8$ code.

A $[95, 7, 72]_8$**-code:** 1223152513221000000,6454574176233563710,3251455612372474710,
3737472772015457210, 1207412747214702100 ; Adding the columns $(3273010)^t$ and $(5536010)^t$, the above code can be extended to a $[97, 7, 74]_8$ code.

A $[105, 8, 78]_8$**-code:** 553561507027510000000,506312404625072547100; Adding the column $(11326073)^t$, the above code can be extended to an $[106, 8, 79]_8$ code.

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

Theorem 2: There exist $[45, 8, 30]_8$ code.

Proof. There exist quasi-cyclic $[42, 8, 28]_8$code with defining polynomials: 126716642762710000000, 316544405114436465310. This code as a subcode a $[42, 6, 30]_8$ code with defining polynomials: 143125610365713200000, 106500266260354044710. Using auxiliary $[3, 2, 2]_8$ code and applying construction X, we obtain a $[45, 8, 30]_8$ code. The following generator matrix yields a

Table 2: Minimum distances of the new linear codes over GF(8)

code	d	d_{gr}	code	d	d_{gr}	code	d	d_{gr}	code	d	d_{gr}
[32,5]	24	23	[120,5]	100	98	[91,7]	69	68	[102,8]	76	75
[38,5]	29	28	[20,6]	13	12	[97,7]	74	73	[106,8]	79	78
[43,5]	33	32	[40,6]	29	28	[105,7]	81	80	[119,8]	90	89
[51,5]	40	39	[48,6]	36	35	[36,8]	23	22	[39,9]	24	23
[78,5]	63	62	[84,6]	66	65	[42,8]	28	27	[91,9]	65	64
[82,5]	66	65	[95,6]	75	74	[45,8]	30	29	[102,9]	74	73
[91,5]	74	73	[43,7]	30	29	[85,8]	62	61	[106,9]	77	76
[107,5]	88	87	[87,7]	66	65	[91,8]	67	66	[93,11]	62	61

$[45,8,30]_8$ code:

$$\left(\begin{array}{c} G \mid 000 \\ - \\ 065633052407003200000210044663374762421400201 \\ 600516152040504700000647072502075311376325510 \end{array}\right),$$

where G denotes the generator matrix of the $[42,6,30]_8$ code.

Theorem 3. There exist optimal $[20,6,13]_8$ code.

Proof. There exist quasi-cyclic $[18,6,11]_8$ code with defining polynomials: 232701, 213171, 510661. Adding the columns $(414141)^t$ and $(717171)^t$, this code can be extended to an optimal $[20,6,13]_8$ code with weight enumerator $0^1 13^{2898} 14^{6363} 15^{13860} 16^{39060} 17^{59010} 18^{71757} 19^{50792} 20^{18403}$.

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. Intern. Workshop WCC1999*, 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* 46, 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.