Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 93-*

Some new linear codes over small finite fields

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. In this paper,we consider quasi-twisted (QT) codes, which are generalization of the quasi-cyclic (QC) codes . Moreover, forty five codes over $GF(7)$ and $GF(9)$ are constructed, 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-twisted (QT) if a constacyclic shift of a codeword by p positions results in another codeword. A constacyclic shift of an m-tuple $(x_0, x_1, \dots, x_{m-1})$ is the m-tuple $(\alpha x_{m-1}, x_0, \dots, x_{m-2}), \alpha \in GF(q) \setminus \{0\}$. The blocklength, n , of a QT code is a multiple of p , so that $n = pm$.

A matrix B of the form

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

where $\alpha \in GF(q) \setminus \{0\}$ is called a *twistulant matrix.* A class of QT codes can be constructed from $m \times m$ twistulant matrices. In this case, the generator matrix, G , can be represented as

$$G = [B_1,\ B_2,\ \dots,\ B_p], \tag{2}$$

where B_i is a twistulant matrix[4].
The algebra of $m \times m$ twistulant matrices over $GF(q)$ is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^m - \alpha)$ 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 QT code are called the *defining polynomials.* If $\alpha = 1$, we obtain the algebra of $m \times m$ circulant matrices, and a subclass of quasi-cyclic codes[5].

If the defining polynomials $b_i(x)$ contain a common factor which is also a factor of $x^m - \alpha$, then the QT code is called *degenerate*. The dimension k of the QT code is equal to the degree of $h(x)$, where [4]

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

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

Similarly to the case of one generator quasi-cyclic codes(see[3],[2]), an p-QT code over $GF(q)$ of length $n = pm$ can be viewed as an $GF(q)[x]/(x^m - \alpha)$ submodule of $(GF(q)[x]/(x^m - \alpha))^p$ [4]. Then an r-generator QT code is spanned by r elements of $(GF(q)[x]/(x^m - \alpha))^p$.

A well-known result regarding the one-generator QT codes are as follows.

Theorem 1.1 [4]: Let C be a one-generator QT code over $GF(q)$ of length $n = pm$. Then, a generator $\mathbf{g(x)} \in (GF(q)[x]/(x^m - \alpha))^p$ 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 $(f_i(x), (x^m - \alpha)/g_i(x)) = 1$ for all $1 \leq i \leq p$.

Quasi-twisted codes form an important class of linear codes, which contains the class of quasi-cyclic codes. A large number of record breaking (and optimal codes) are QT codes [1]. In this paper, seven new one-generator QT codes and ten QC codes ($p \geq 1$) are constructed using a algebraic-combinatorial computer search, similar to that in [4]. Other codes are obtained through extension of good QC codes. The codes presented here(Table 2), improve the respective lower bounds on the minimum distance in [1].

2 The new QT codes over GF(7)

We have restricted our search to one-generator QT codes with a generator of the form as in Theorem 1.1 with one generator polynomial g(x) and $f_1(x) = 1$.

Let $q = 7$,$m = 100$ and $\alpha = 6$. Then

$$x^{100} + 1 = \prod_{i=1}^{26} h(i)$$

There are twenty four polynomials of fourth degree and two polynomials of second degree. For $k = 14$, has 4048 possibilities to obtain $g(x)$ of degree 86. We checked for these possibilities consecutively ($f_1(x) = 1$) and when g(x)=
16000134421466365353326230166335515411420613
5064054262505040503136515562066123220346161,
$[100, 14, 63]_7$ constacyclic code is obtained. Similarly we get $[100, 12, 66]_7$ code. We note, that a cyclic $[100, 12, 66]_7$ and $[100, 14, 63]_7$ codes do not exist. Moreover, the constacyclic $[100, 16, 60]_7$, $[100, 18, 58]_7$, $[100, 20, 55]_7$ and $[100, 22, 50]_7$ codes, obtained by Grassl, are being motivated by the above two results.

Theorem 2.1: There exist one-generator quasi-twisted codes of type (4) with parameters:

$[96,6,75]_7$	$[30,8,18]_7$	$[72,8,51]_7$	$[40,10,23]_7$
$[90,10,61]_7$	$[100,12,66]_7$	$[100,14,63]_7$	

Proof. The coefficients of the defining polynomials of the codes are as follows:
A $[96, 6, 75]_7$**-code:**
643062265526521044100000,502013524005412325351000,
414154314333142246666110,621156660654165143155010;
A $[30, 8, 18]_7$**-code:**
1010000000,5314421100,3241404110;
A $[72, 8, 51]_7$**-code:**
226003441603514210000000,133543432540653642461000,123260664136540214021000;
A $[40, 10, 23]_7$**-code:**
16460406461000000000,44060463136551426100;
A $[90, 10, 61]_7$**-code:**
456300553336553006351000000000,651300552164114151301033010000,
605330452255426462023426510000;
A $[100, 12, 66]_7$**-code:**
13321430144225611615316341116443230414121212120444
13335400604553563035121520443113341050100000000000;

3 The new QC codes over GF(7)

We illustrate the search method in the following example. Let $m = 25$ and $q = 7$. Then the $\gcd(25, 7) = 1$ and the splitting field of $x^{25} - 1$ is $GF(7^4)$ where 4 is the smallest integer such that $25|(7^4 - 1)$. One of the generating

Table 1: Minimum distances of the [25p,8,d] quasi-cyclic codes over GF(7).

p	$25p$	f_p	d	d_{gr}	p	$25p$	f_p	d	d_{gr}
1	25	1	12	13	3	75	1161256	53	52
2	50	10464	33	34	4	100	161123	73	72

polynomials for $GF(7^4)$ is $p(x) = x^4 + 3x^3 + x + 5$ and let β be a root of $p(x)$. Then

$$x^{25} - 1 = \prod_{j=0}^{6}(x - \beta^j) = \prod_{i=1}^{7} h(x)$$

The minimal polynomials are:

$$\begin{array}{ll} h_1(x) = x^4 + 2x^3 + 4x^2 + 2x + 1 & h_2(x) = x^4 + 6x^3 + 5x^2 + 6x + 1 \\ h_3(x) = x^4 + 4x^3 + 3x^2 + 4x + 1 & h_4(x) = x^4 + x^3 + x^2 + x + 1 \\ h_5(x) = x^4 + 5x^3 + 5x^2 + 5x + 1 & h_6(x) = x^4 + 4x^3 + 4x + 1 \\ h_7(x) = x + 6. & \end{array}$$

For k=8 we have 15 generator polynomials. Taken

$$g(x) = x^{17} + 5x^{16} + 2x^{13} + 2x^{12} + 3x^{10} + 2x^9 + 5x^8 + 4x^7 + 5x^5 + 5x^4 + 2x + 6,$$

we obtain a quasi-cyclic code $[50, 8, 33]_7$ with $f_2(x) = x^4 + 4x^2 + 6x + 4$. After that we make search for $f_p(x), p = 3, 4$. With $f_3(x) = x^6 + x^5 + 6x^4 + x^3 + 2x^2 + 5x + 6$ we find $[75, 8, 53]_7$-code and with $f_4(x) = x^5 + 6x^4 + x^3 + x^2 + 2x + 3$ we find $[100, 8, 73]_7$-code. The results are given in Table 1.

Theorem 3.1: There exist one-generator quasi-cyclic codes of type (4) with parameters:

$$\begin{array}{rrrr} [40,5,30]_7 & [56,5,43]_7 & [57,7,41]_7 & [80,7,59]_7 \\ [96,7,72]_7 & [32,8,19]_7 & [36,8,22]_7 & [64,8,44]_7 \\ [75,8,53]_7 & [96,8,70]_7 & [100,8,73]_7 & [96,9,68]_7 \\ [100,9,71]_7 & [33,10,18]_7 & [55,10,34]_7 & [96,10,66]_7 \\ [100,10,69]_7 & & & \end{array}$$

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

A $[40, 5, 30]_7$**-code:**

65210000,52123100,24636610,42222110,15343131;

Adding the columns $(15621)^t$ and $(14631)^t$, the above code can be extended to a $[42, 5, 32]_7$ code.

A $[56, 5, 43]_7$**-code:**

65210000,35543100,40446210,15226410,25642110,55552510,63540210;
Adding the columns $(16611)^t, (16161)^t$and $(11661)^t$, the above code can be extended to a $[59, 5, 46]_7$ code.
A $[57, 7, 41]_7$**-code:**
1436236116141000000,4542144052534101410,6351030314556061510;
Adding the columns $(0532100)^t$ and $(1111111)^t$, the above code can be extended to a $[59, 7, 42]_7$ code.
A $[80, 7, 59]_7$**-code:**
6463164131000000,1611110235033100,6453240365635310,3432346551321000,2323510162165410;
A $[96, 7, 72]_7$**-code:**
5316223635665410402143154131666215264030410000000,
3046444251555161564546535101253005053056133410000;
Adding the columns $(6413641)^t$ and $(6512651)^t$, the above code can be extended to a $[98, 7, 74]_7$ code.
A $[32, 8, 19]_7$**-code:**
6346013410000000,2225651306201000 ;
Adding the column $(36413641)^t$, the above code can be extended to a $[33, 8, 20]_7$ code.
A $[36, 8, 22]_7$**-code:**
610000000,312663610,623021000,521624100;
Adding the columns $(42142142)^t$ and $(24124124)^t$, the above code can be extended to a $[38, 8, 24]_7$ code.
A $[64, 8, 44]_7$**-code:**
6145261210000000,5420144154311000,6051062341331000,1055514663661000;
Adding the columns $(66116611)^t$ and $(16611661)^t$, the above code can be extended to a $[66, 8, 46]_7$ code.
Remark: The defining polynomials of the some codes, which are missing in Theorem 3.1, are given in [1]. All defining polynomials, generator matrices and weight enumerators are available on request from the author.

Theorem 3.2: There exist quasi-cyclic codes of type (2) with parameters:

$$[21,7,12]_7 \quad [24,8,13]_7 \quad [20,8,10]_7$$

Proof. The coefficients of the defining polynomials of the codes are as follows:
A $[21, 7, 12]_7$**-code:**
4030100,3453301,4554631;
Adding the column $(1111111)^t$, the above code can be extended to a $[22, 7, 13]_7$ code.
A $[20, 8, 10]_7$**-code:**
6041,5631,1221,1361,4251;
3121,2651,4100,1221,3001;
The above code has generator matrix, containing two circulants [5] with dimension four. Adding the column $(1111111)^t$, the above code can be extended to a $[21, 8, 11]_7$ code.
A $[24, 8, 13]_7$**-code:**
54346041,61136241,33612621;

Table 2: Minimum distances of the new linear codes over GF(7)

code	d	d_{gr}	code	d	d_{gr}	code	d	d_{gr}
[42,5]	32	31	[30,8]	18	17	[100,9]	71	70
[59,5]	46	45	[33,8]	20	19	[33,10]	18	17
[96,6]	75	74	[38,8]	24	23	[40,10]	23	22
[22,7]	13	12	[66,8]	46	45	[55,10]	34	33
[59,7]	42	41	[72,8]	51	50	[90,10]	61	60
[80,7]	59	58	[75,8]	53	52	[96,10]	66	65
[98,7]	74	73	[96,8]	70	69	[100,10]	69	68
[21,8]	11	10	[100,8]	73	72	[100,12]	66	65
[25,8]	14	13	[96,9]	68	67	[100,14]	63	62

Adding the column $(1111111)^t$, the above code can be extended to a $[25, 8, 14]_7$ code.

4 The new QC codes over GF(9)

For convenience, the elements of $GF(9)$ are given as integers: $2 = \beta^4$, $3 = \beta$,$4 = \beta^7$, $5 = \beta^6$, $6 = \beta^5$, $7 = \beta^2$,$8 = \beta^3$, where β is a root of the primitive polynomial y^2+y+2 over $GF(9)$. We have restricted our search to one-generator QC codes with a generator of the form as in Theorem 1.1 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 1.1. 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. All results are given in Table 4.
We illustrate the search method in the following example. Let $q = 9$ and $m = 8$. Then

$$x^8 - 1 = \prod_{j=0}^{7} (x - \beta^j)$$

Let now $k = 6$. There are 28 possibilities to obtain $g(x)$ of degree two. By this reason, we can use exhaustive search with all different codes in a given length. Taken $g_1(x) = x^2 + 2$ and $g_2(x) = x^2 + 8x + 3$ we obtained 53 quasi-cyclic $D = [16, 6, 9]_9$ codes.(The best known code[1]is $[16, 6, 10]_9$) Using these codes, we received 198 good QC $[24, 6, 16]_9$ codes. After that we checked all codes for extendability and etc. The results are given in Table 3.

Table 3: Extendibility of a good $[8p, 6, d]_9$ quasi-cyclic codes

code	*number*	*ext.code*	*code*	*number*	*ext.code*
[24,6,16]	198	[28,6,20]	[80,6,63]	104	[81,6,64]
[32,6,22]	21604	[34,6,24]	[96,6,76]	12479	[99,6,79]
[40,6,29]	4856	[43,6,32]	[104,6,83]	7026	[107,6,86]
[48,6,36]	87	[49,6,37]	[112,6,90]	2727	[114,6,92]
[56,6,42]	10861	[58,6,44]	[120,6,97]	301	[123,6,100]
[64,6,49]	18131	[66,6,51]	[128,6,104]	8	[129,6,105]

It is seen[1], that there are six new results: $[43, 6, 32]_9$, $[49, 6, 37]_9$, $[107, 6, 86]_9$, $[114, 6, 92]_9$, $[123, 6, 100]_9$ and $[129, 6, 105]_9$.

Now, we present the new quasi-cyclic codes.

Theorem 4.1: There exist one-generator quasi-cyclic codes of type (4) with parameters:

$[32,5,24]_9$	$[60,5,48]_9$	$[64,5,51]_9$	$[80,5,65]_9$	$[40,6,29]_9$	$[48,6,36]_9$
$[56,6,43]_9$	$[91,6,72]_9$	$[100,6,80]_9$	$[104,6,83]_9$	$[112,6,90]_9$	$[120,6,97]_9$
$[128,6,104]_9$	$[32,7,21]_9$	$[104,7,81]_9$	$[120,7,95]_9$	$[126,7,100]_9$	

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

A $[32, 5, 24]_9$**-code:**
80310000,14125410,57351510,16517310;
The above code can be extended to a $[34, 5, 26]_9$ code adding of the columns $(25721)^t$ and $(21751)^t$.
A $[60, 5, 48]_9$**-code:**
1877810000,7785216100,7251380810,2373417100,6662363810,5724131210;
The above code can be extended to a $[62, 5, 50]_9$ code by adding twice the column $(11111)^t$.
A $[64, 5, 51]_9$**-code:**
4763881114410000,1571085464846100,5477036336437410,8284074810411510;
The above code can be extended to a $[70, 5, 57]_9$ code by adding of the columns $(06010)^t, (70601)^t, (26541)^t, (24761)^t, (24761)^t$ and $(15271)^t$
A $[80, 5, 65]_9$ **code:**
4036617687510000,5810512125876510,7120346383881510,6482888473553100,8756161888531410;
The above code can be extended to a $[86, 5, 71]_9$ code by adding of the columns $(23611)^t, (24421)^t, (28731)^t, (26541)^t, (26541)^t$ and $(22361)^t$
A $[40, 6, 29]_9$**-code:**
38100000,58256100,63765510,87830610,77263710;

The above code can be extended to a $[43, 6, 32]_9$ code by adding of the columns $(212121)^t, (715271)^t$ and $(423581)^t$

A $[48, 6, 36]_9$**-code:**
38100000,58256100,13311510,86555610,36352410,15730710;
The above code can be extended to a $[49, 6, 37]_9$ code by adding of the column $(324761)^t$.

A $[56, 6, 43]_9$**-code:**
17270525100000,30470554833510,41832282450510,40518226278810;

A $[91, 6, 72]_9$ **code:**
2010212100000,5685456551100,7277472885510,3883436540100,
3318214727100,6174421502610,8256678158310;
The above code can be extended to a $[92, 6, 73]_9$ code by adding of the column $(351351)^t$.

A $[100, 6, 80]_9$**-code:**
74182771257878100000,28331102267186768100,51571377646037838810,
75868711326224636310,45242251813728824310;
The above code can be extended to a $[102, 6, 82]_9$ code by adding of the columns $(212121)^t$ and $(517251)^t$.

A $[104, 6, 83]_9$**-code:**
38100000,58256100,18272610,63744810,52244010,66147810,71505810,
23541210,66676710,34624410,13173810,42838110,30533610;
The above code can be extended to a $[107, 6, 86]_9$ code by adding of the columns $(212121)^t, (725172)^t$ and $(527152)^t$

A $[112, 6, 90]_9$**-code:**
38100000,58256100,18272610,63744810,52244010,66147810,71505810,
23541210,66676710,34624410,57338610,84751110,82802610,27333510;
The above code can be extended to a $[114, 6, 92]_9$ code by adding of the columns $(212121)^t$ and $(623162)^t$.

A $[120, 6, 97]_9$**-code:**
38100000,58256100,18272610,63744810,52244010,66147810,71505810,23541210,
66676710,34624410,26734110,30533610,76845510,25744410,57152610;
The above code can be extended to a $[123, 6, 100]_9$ code by adding of the columns $(628731)^t(823741)^t$ and $(426781)^t$.

A $[128, 6, 104]_9$**-code:**
38100000,58256100,18272610,63744810,52244010,66147810,71505810,23541210,
66676710,34624410,25461810,26084310,17124210,62437110,16683810,85266810;
The above code can be extended to a $[129, 6, 105]_9$ code by adding of the column $(423581)^t$.

A $[32, 7, 21]_9$**-code:**
21000000,83222100,54653100,33576810;
The above code can be extended to a $[34, 7, 23]_9$-code by adding of the columns $(2121212)^t$ and $(7826541)^t$.

A $[104, 7, 81]_9$**-code:**
1222121000000,7802383510100,1372680321310,8611364411000,
4315314163100,8315508126210,5325315184210,3347133825610;
The above code can be extended to a $[105, 7, 82]_9$-code by adding of the column $(1111111)^t$.

A $[120, 7, 95]_9$ **code:**

Table 4: Minimum distances of the new linear codes over GF(9)

code	d	d_{gr}	code	d	d_{gr}	code	d	d_{gr}
[36,4]	30	29	[49,6]	37	36	[123,6]	100	99
[34,5]	26	25	[56,6]	43	42	[129,6]	105	104
[62,5]	50	49	[92,6]	73	72	[34,7]	23	22
[70,5]	57	56	[102,6]	82	81	[105,7]	82	81
[86,5]	71	70	[107,6]	86	85	[120,7]	95	94
[43,6]	32	31	[114,6]	92	91	[126,7]	100	99

81228663510747657056138124606100710000000,28125625001671308228602213252451803100000,
4775477306678687477736251127612143632710;

A $[126, 7, 100]_9$**-code:**
16557741000000,34211427224100,77568421415100,18428267536710,43450571601000,
87560250163410,18272264722110,10505313635310,63444841424310;

Theorem 4.2: There exist **optimal** $[36, 4, 30]_9$ code.
*Proof.*There exist quasi-cyclic $[28, 4, 22]_9$ code of type (2)[5] with defining polynomials:
8721,8531,7101,8251,2621,4771,4881.
Adding the columns $(5210)^t, (5701)^t, (1111)^t, (2121)^t, (0521)^t, (7251)^t, (2071)^t$ and $(5271)^t$, the above code can be extended to an **optimal** $[36, 4, 30]_9$ code with weight enumerator $0^1 30^{2176} 31^{1024} 32^{512} 33^{1312} 34^{512} 35^{1024}$.

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 Cod. Crypt. WCC99*, Paris, France, 1999, 11-20.

[3] G. E. Séguin, G. Drolet, The theory of 1-generator quasi-cyclic codes, Techn. Rep., Royal Milit. Coll. Canada, Kingston, ON, 1991.

[4] I. Siap, N. Aydin, D. Ray-Chaudhury, The structure of 1-generator quasi-cyclic codes and new linear codes, *Des., Codes Crypt.* 24, 2001, 313-326.

[5] H. van Tilborg, On quasi-cyclic codes with rate $1/m$, *IEEE Trans. Inform. Theory* 24, 1978, 628-630.