

Some new ternary linear codes*

Research Article

Rumen Daskalov, Plamen Hristov

Abstract: Let an $[n, k, d]_q$ 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 optimal minimum distances. In this paper 22 new ternary linear codes are presented. Two of them are optimal. All new codes improve the respective lower bounds in [11].

2010 MSC: 94B05, 94B65

Keywords: Ternary linear codes, Construction X

1. Introduction

Let an $[n, k, d]_q$ code be a linear code of length n , dimension k and minimum Hamming distance d over a finite field $GF(q)$. One of the most important and fundamental problems in coding theory is to find the optimal values of the parameters of a linear code.

This optimization problem can be formulated in a couple of ways. For example, for fixed q, n and k we may wish to maximize the minimum distance d ; or for given q, k and d to minimize the block length n . Let $d_q(n, k)$ denote the largest value of d for which there exists an $[n, k, d]_q$ code, and $n_q(k, d)$ be the smallest value of n for which there exists an $[n, k, d]_q$ code. Then an $[n_q(k, d), k, d]_q$ code is called length-optimal and an $[n, k, d_q(n, k)]_q$ code is called distance-optimal. Both length-optimal and distance-optimal codes are called optimal codes.

The problem of finding the parameters of optimal codes is a very difficult one and has two aspects - one involves the construction of new codes with better minimum distances and the other is proving the nonexistence of codes with given parameters. It has been solved only over small finite fields for small dimensions and co-dimensions.

Computer search is often used in looking for codes with better minimum distances, but it is a well known fact that computing the minimum distance of a linear code is an NP-hard problem [15]. Since it is

* This work was partially supported by the Bulgarian Ministry of Education and Science under Contract in TU-Gabrovo.

Rumen Daskalov (Corresponding Author), Plamen Hristov; Department of Mathematics, Technical University of Gabrovo, Bulgaria (email: daskalov@tugab.bg, plhristov9@gmail.com).

not possible to carry out exhaustive searches for linear codes with large dimension, it is natural to focus one's effort on subclasses of linear codes, having rich mathematical structures. Quasi-cyclic (QC) codes are known to have such a structure and it has been shown in recent years that this subclass contains many new good linear codes ([1, 4–10, 12–14] and [E. Metodieva, N. Daskalova, Generating generalized necklaces and new quasi-cyclic codes, in preparation, 2017]).

Grassl [11] maintains a table with lower and upper bounds on minimum distances of linear codes over small finite fields GF(q) ($q \leq 9$). When the constructed code has a minimum distance equal to the upper bound, it is optimal and there is no place for improvement in the table. When there is a gap between the minimum distance of the best-known code and the upper bound on the minimum distance, this is indicated in the table by listing both values - d_l and d_u . Many of the best-known codes in these tables are QC codes. A code that attains a lower bound in the table is called a *good* code. A code that improves a lower bound in the table will be called a *new* code.

Another online table of linear codes is also maintained by Chen. Chen's table [3] contains only good and best-known quasi-cyclic and quasi-twisted codes ($q \leq 13$). These two databases are updated when new codes are discovered.

The remainder of the paper is organized as follows. In Section 2, some basic definitions and facts on QC codes are presented. In Section 3, sixteen good one-generator QC codes ($p \geq 2$) are constructed using an algebraic-combinatorial computer search. In Section 4 (Theorem 4.1), we use the codes presented in section 3, along with construction X, to obtain seventeen new ternary linear codes. In Theorem 4.2 five new codes are also presented.

2. Quasi-cyclic codes

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 $(x_0, x_1, \dots, x_{m-1})$ is the m -tuple $(x_{m-1}, x_0, \dots, x_{m-2})$. 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

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

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 $GF(q)[x]/(x^m - 1)$, with B being mapped to the polynomial, $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{m-1}x^{m-1}$, formed from the entries in the first row of B . The $b_i(x)$'s 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

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

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 have the following form

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

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 $1 \leq i \leq p$. Then C is a degenerate, one-generator QC code having $n = mp$, and $k = m - \deg g(x)$ (see [14]).

In our constructions we will use the following well-known theorems.

Theorem 2.1 (Construction X). [2] Given an $[n, k, d]_q$ code C_1 , and an $[n, k - l, d + s]_q$ subcode C_2 , we can construct an $[n + a, k, d + s]_q$ code C when we have an $[a, l, s]_q$ code C_3 (by appending codewords from the latter code to cosets of the second code in the first code).

Theorem 2.2 (Construction XX). [2] Let an $[n, k, d]_q$ code C have two subcodes C_1 and C_2 of dimensions $k - k_1$ and $k - k_2$ and append tails from a $[a_i, k_i, \delta_i]_q$ code to the codewords of C , where the two tails of codewords correspond to the coset of C_i ($i = 1, 2$) it is in. If C_1, C_2 and $C_1 \cap C_2$ have minimum distance d_1, d_2 and d_0 , respectively, then there exists an $[n + a_1 + a_2, k, \min(d_0, d_1 + \delta_2, d_2 + \delta_1, d + \delta_1 + \delta_2)]_q$ code.

3. Good QC codes

In this section sixteen good one-generator QC codes ($p \leq 4$) are constructed using a non-exhaustive algebraic-combinatorial computer search, similar to that in [1, 4–6, 8–10, 14]. An important feature of these codes is that they have good subcodes and can be used for construction X.

We have restricted our search to one-generator QC codes with defining polynomials of the form (4).

Example 3.1. : Let $m = 35$. The factorization of the polynomial $x^{35} - 1$ over $GF(3)$ is

$$x^{35} - 1 = \prod_{i=1}^5 p_i(x),$$

where

$$\begin{aligned} p_1(x) &= x^{12} + x^{10} + 2x^8 + x^7 + x^5 + 2x^4 + x^3 + 2x^2 + 2x + 1 \\ p_2(x) &= x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + x^7 + x^5 + 2x^4 + x^2 + 1 \\ p_3(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ p_4(x) &= x^4 + x^3 + x^2 + x + 1 \\ p_5(x) &= x + 2. \end{aligned}$$

Let the dimension $k = 17$. Then the degree of the polynomials $g(x)$ has to be 18. Taking the product of two of the polynomials above, one of degree 12 and one of degree 6, we obtain two polynomials $g(x)$ of degree 18. We choose

$$g(x) = x^{18} + x^{17} + 2x^{16} + 2x^{15} + x^{14} + 2x^{13} + 2x^{12} + 2x^{11} + x^{10} + x^9 + 2x^4 + 2x^2 + 1,$$

and then we search for $f_2(x)$. The polynomial $f_2(x) = x^9 + 2x^8 + 2x^7 + x^6 + x^4 + x^3 + 1$ yields a $[70, 17, 29]_3$ quasi-cyclic code. Afterwards, we search for $f_3(x)$ and $f_4(x)$ in succession. The polynomial $f_3(x) = x^{10} + x^8 + 2x^6 + x^5 + x^3 + 2x + 2$ leads to a $[105, 17, 48]_3$ code and $f_4(x) = x^8 + 2x^4 + 2x^3 + x^2 + 2$ gives a $[140, 17, 69]_3$ code.

In the following theorems the defining polynomials are listed with the lowest degree coefficient on the left.

4. The new codes

Let us look at an example, related to the next Theorem 4.1. We will show how the $[151, 17, 75]_3$ code C is constructed. A generator matrix of a code C has the form $G = \begin{pmatrix} G_2 & 0 \\ * & G_3 \end{pmatrix}$, where G_2 and G_3 are generator matrices of the codes C_2 and C_3 respectively, and $(*)$ denotes l linearly independent codewords of a code C_1 .

The generator matrix G_2 of the $[140, 12, 75]_3$ subcode C_2 has the same first row as the row given in Theorem 4.1. The generator matrix of the $[11, 5, 6]_3$ code is

$$G_3 = \begin{pmatrix} 10122002010 \\ 01012200201 \\ 10101220020 \\ 01010122002 \\ 20101012200 \end{pmatrix}$$

and the five independent codewords from the $[140, 17, 69]_3$ code C_1 are:

102020000112221221100000000000000001021020100121011010202100010000002211200222221002112021121000000020021202112020221122002110000100000,
010202000011222122110000000000000000001021020100121011011020210001000000221120022222100211202112100000002002120211202022112200211000010000,
00102020000112221221100000000000000000000102102010012101101102021000100000022112002222210021120211210000000200212021120202211220021100001000,
000102020000112221221100000000000000000000102102010012101101102021000100000022112002222210021120211210000000020021202112020221122002110000100,
000010202000011222122110000000000000000000010210201001210110110202100010000002211200222221002112021121000000002002120211202022112200211000010;

The weight enumerator of the $[151, 17, 75]_3$ code is $0^1 75^{784} 76^{2664} 78^{7728} 79^{20870} 81^{40824} 82^{111524}$
 $84^{175574} 85^{491414} 87^{610190} 88^{1651468} 90^{1659156} 91^{4416804} 93^{3644426} 94^{9032618} 96^{6278202} 97^{14388718} 99^{8407602}$
 $100^{17626234} 102^{8667680} 103^{16568328} 105^{6850326} 106^{11875360} 108^{4084836} 109^{6379366} 111^{1839922} 112^{2579332}$
 $114^{607642} 115^{760172} 117^{143598} 118^{162324} 120^{24976} 121^{23782} 123^{3150} 124^{2198} 126^{84} 127^{266} 132^{12} 135^8$.

Theorem 4.1. There exist new ternary linear codes, having parameters: $[168, 12, 96]_3$, $[110, 13, 57]_3$, $[114, 13, 60]_3$, $[122, 13, 64]_3$, $[157, 13, 87]_3$, $[184, 13, 104]_3$, $[225, 13, 128]_3$, $[170, 14, 93]_3$, $[49, 15, 19]_3$, $[165, 16, 86]_3$, $[53, 17, 20]_3$, $[106, 17, 49]_3$, $[124, 17, 60]_3$, $[151, 17, 75]_3$, $[112, 19, 50]_3$, $[110, 20, 48]_3$, $[171, 20, 83]_3$.

Proof. All of the codes are obtained by construction X. The parameters of the codes, related to Theorem 2.1, are given in Table 1. The defining polynomials of the subcodes C_2 are given for clearness. The coefficients of these polynomials are as follows:

A $[160, 10, 96]_3$ code:

21201222020021120202010102102221122201120020112221020002002211221112211000000000,

110110120022212110202222211210012212112220101101110101210111120002110002201100;

A $[104, 10, 57]_3$ code:

21002111121000201000000000, 2120021202100111121222100,

1112100000001011100221110, 20011221200122201101021000;

A [104, 9, 60]3 code:

Table 1. The new codes.

code C_1	subcode C_2	code C_3	new code C
[160,12,90] ₃	[160,10,96] ₃	[8,2,6] ₃	[168,12,96] ₃
[104,13,54] ₃	[104,10,57] ₃	[6,3,3] ₃	[110,13,57] ₃
[104,13,54] ₃	[104,9,60] ₃	[10,4,6] ₃	[114,13,60] ₃
[120,13,62] ₃	[120,12,64] ₃	[2,1,2] ₃	[122,13,64] ₃
[156,13,86] ₃	[156,12,87] ₃	[1,1,1] ₃	[157,13,87] ₃
[182,13,102] ₃	[182,12,104] ₃	[2,1,2] ₃	[184,13,104] ₃
[224,13,127] ₃	[224,12,128] ₃	[1,1,1] ₃	[225,13,128] ₃
[160,14,87] ₃	[160,10,93] ₃	[10,4,6] ₃	[170,14,93] ₃
[48,15,18] ₃	[48,14,19] ₃	[1,1,1] ₃	[49,15,19] ₃
[160,16,84] ₃	[160,12,86] ₃	[5,4,2] ₃	[165,16,86] ₃
[52,17,19] ₃	[52,16,20] ₃	[1,1,1] ₃	[53,17,20] ₃
[105,17,48] ₃	[105,16,49] ₃	[1,1,1] ₃	[106,17,49] ₃
[123,17,59] ₃	[123,16,60] ₃	[1,1,1] ₃	[124,17,60] ₃
[140,17,69] ₃	[140,12,75] ₃	[11,5,6] ₃	[151,17,75] ₃
[111,19,49] ₃	[111,18,50] ₃	[1,1,1] ₃	[112,19,50] ₃
[104,20,45] ₃	[104,17,48] ₃	[6,3,3] ₃	[110,20,48] ₃
[170,20,82] ₃	[170,19,83] ₃	[1,1,1] ₃	[171,20,83] ₃

21012011002110011100000000, 21210221012001202202000100, 20102202120100012001122212,
 21211221200221021211002002;
 A [120, 12, 64]₃ code:
 1022011202110010021112112222000000000000, 2101002010121022021212001111121220000000,
 2020211110002120011122112101122111012000;
 A [156, 12, 87]₃ code:
 2012002102201121122202110200200022200021000000000000,
 1111211022101012120102220001022012010102022021000000,
 102102022111220100222022110221100202222012200010000;
 A [182, 12, 104]₃ code:
 11212112011010200101211200121210200210200102100102121200122120200102022012212
 1220000000000000,
 111101102102212111101022102120020221201002221001102210110102221220111222100
 22021101220000;
 A [224, 12, 128]₃ code:
 202112002110020101002212212210212111000212022000000000000,
 22020111002220122121222102202111121100122011020222120000,
 2022202002220211210101222212020001010102220020111112000,
 11211112102222022011222021202122120111112102000201221200;
 A [160, 10, 93]₃ code:
 111222010002220222012011010002202201022121220110212201211201101221222020000000000,
 2112110120221220011102001101220021122022012020011220111112111120221012211121020;
 A [48, 14, 19]₃ code:
 2010000000000000, 2221121000211000, 2212110110100000;
 A [160, 12, 86]₃ code:
 222022212000212211012111220022210220001002110202111210212222212120101000000000000,
 10220111202202200200120011220201221200120211101221110011212112001121200212201000;
 A [52, 16, 20]₃ code:
 22021201002000000000000000, 20211122210220200101122000;
 A [105, 16, 49]₃ code:

Theorem 4.2. There exist new ternary linear codes with parameters: $[39, 12, 18]_3$, $[48, 13, 21]_3$, $[66, 18, 27]_3$ and $[106, 14, 54]_3$.

Proof. 1. There exist a $[36, 12, 15]_3$ QC code C , having the following defining polynomials: 112122201101, 222010220221, 222001010001. This code is triple extendible. By adding the next three columns $(110110110110)^\top$, $(101101101101)^\top$, $(011011011011)^\top$ to the generator matrix of C , we get a new self-orthogonal optimal $[39, 12, 18]_3$ code. The weight distribution of the new code is $0^1 18^{8034} 21^{48204} 24^{169415} 27^{204464} 30^{90090} 33^{10998} 36^{234}$. The shortened $[38, 11, 18]_3$ code is also optimal.

2. There exist a $[48, 12, 21]_3$ QC code C , having the following defining polynomials: 102100112112 , 102121001210 , 111002112002 , 111210200210 . By adding the next row $00000000000000000000000001111111111222222222222$ to the generator matrix of code C , we get a new $[48, 13, 21]_3$ code.

3. First a new $[64, 18, 25]_3$ code D of type (4) has been constructed. It has defining polynomials $d_1(x) = g(x) = (x^8 + 2x^4 + 2)(x^4 + 2x^2 + 2)(x^2 + 2x + 2)$ and $d_2(x) = g(x).f_2(x)$, where $f_2(x) = x^{13} + x^{10} + 2x^8 + x^7 + 2x^6 + x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1$, i.e. the defining polynomials are 21011021012211100000000000000000, 22011120101001120212221001110000. This code is double extendible. By adding the next columns $(1010101010101010)^T$, $(010101010101010)^T$ to the generator matrix of D we get a new $[66, 18, 27]_3$ code.

4. A new $[106, 14, 54]_3$ code has been constructed by Construction XX (Theorem 2.2), where C is a $[104, 14, 52]_3$ code, C_1 is a $[104, 13, 53]_3$ code, C_2 is a $[104, 13, 53]_3$ code, $C_1 \cap C_2$ is a $[104, 12, 54]_3$ code and $a_1 = a_2 = 1$, $k_1 = k_2 = 1$, $\delta_1 = \delta_2 = 1$.

The defining polynomials of C , C_1 , C_2 and $C_1 \cap C_2$ are as follows:

1200002002211000000000000000, 22212202200212210221000000, 20122211021022101000000000,
20101021210012001222101100;
11100021020202000000000000, 20021012010221022202200000, 2111002022220221200000000,
21121222122011101100221020;
10200022021021000000000000, 21100122120200101210100000, 2210110212012101100000000,
22111120001010201011011210;
12210020122222000000000000, 22020110211210121122120000, 20221022211112210020000000,
20200011001212211210210122;

A generator matrix of the new code has the next form $G = \begin{pmatrix} G^* & 0 \\ * & G_3 \end{pmatrix}$, where G^* is a generator

matrix of $C_1 \cap C_2$, $G_3 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ and $*$ denotes the next two linearly independent codewords of a code C :

1200002002211000000000000022212202200212210221000000201222110210221010000000002010102121001
2001222101100,
0120000200221100000000000002221220220021221022100000020122211021022101000000000201010212100
1200122210110 . \square

References

- [1] N. Aydin, I. Siap, D. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, *Des. Codes Cryptogr.* 24(3) (2001) 313–326.
- [2] A. E. Brouwer, Bounds on the Size of Linear Codes, in *Handbook of Coding Theory*, V.S. Pless, W.C. Huffman, R.A. Brualdi(eds), Elsevier Amsterdam, 1998.
- [3] E. Z. Chen, Database of quasi-twisted codes, available at <http://www.tec.hkr.se/~chen/research/codes/searchqc2.htm>
- [4] E. Z. Chen, A new iterative computer search algorithm for good quasi-twisted codes, *Des. Codes Cryptogr.* 76(2) (2015) 307–323.
- [5] E. Chen, N. Aydin, A database of linear codes over \mathbb{F}_{13} with minimum distance bounds and new quasi-twisted codes from a heuristic search algorithm, *J. Algebra Comb. Discrete Appl.* 2(1) (2015) 1–16.
- [6] E. Chen, N. Aydin, New quasi-twisted codes over \mathbb{F}_{11} —minimum distance bounds and a new database, *J. Inf. Optim. Sci.* 36(1–2) (2015) 129–157.
- [7] R. N. Daskalov, T. A. Gulliver, New good quasi-cyclic ternary and quaternary linear codes, *IEEE Trans. Inform. Theory* 43(5) (1997) 1647–1650.
- [8] R. Daskalov, P. Hristov, New one-generator quasi-cyclic codes over $GF(7)$, *Problemi Peredachi Informatsii* 38(1) (2002) 59–63. English translation: *Probl. Inf. Transm.* 38(1) (2002) 50–54.
- [9] R. Daskalov, P. Hristov, New quasi-twisted degenerate ternary linear codes, *IEEE Trans. Inform. Theory* 49(9) (2003) 2259–2263.
- [10] R. Daskalov, P. Hristov, E. Metodieva, New minimum distance bounds for linear codes over $GF(5)$, *Discrete Math.* 275(1–3) (2004) 97–110.
- [11] M. Grassl, Linear code bound [electronic table; online], available at <http://www.codetables.de>.
- [12] P. P. Greenough, R. Hill, Optimal ternary quasi-cyclic codes, *Des. Codes Cryptogr.* 2(1) (1992) 81–91.
- [13] T. A. Gulliver, P. R. J. Ostergard, Improved bounds for ternary linear codes of dimension 7, *IEEE Trans. Inform. Theory* 43(4) (1997) 1377–1381.
- [14] I. Siap, N. Aydin, D. Ray-Chaudhury, New ternary quasi-cyclic codes with better minimum distances, *IEEE Trans. Inform. Theory* 46(4) (2000) 1554–1558.
- [15] A. Vardy, The intractability of computing the minimum distance of a code, *IEEE Trans. Inform. Theory* 43(6) (1997) 1757–1766.