

## 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](mailto:daskalov@tugab.bg), [plhristov9@gmail.com](mailto: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

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

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

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

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

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

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  $C$  have the following form

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

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  $1 \leq i \leq p$ . 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.





**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:

1022011202110010021112112222200000000000, 2101002010121022021212001111112122000000, 2020211110002120011122112101122111012000;

A  $[156, 12, 87]_3$  code:

2012002102201121122202110200200022200021000000000000, 1111211022101012120102220001022012010102022021000000, 102102022111220100222022110221100202222012200010000;

A  $[182, 12, 104]_3$  code:

11212112011010200101211200121210200210200102100102121200122120200102022012212 12200000000000, 1111011021022121111010221021200202212010002221001102210110102221220111222100 22021101220000;

A  $[224, 12, 128]_3$  code:

20211200211002010100221221221021211100021202200000000000, 22020111002220122121222102202111121100122011020222120000, 20222020022202112101012222120200010101022200201111112000, 11211112102222022011222021202122120111112102000201221200;

A  $[160, 10, 93]_3$  code:

1112220100022202201201101000220220102212122011021220121120110122122202000000000, 21121101202212200111020011012200211220220120200112201111112111120221012211121020;

A  $[48, 14, 19]_3$  code:

2010000000000000,2221121000211000,2212110110100000;

A  $[160, 12, 86]_3$  code:

22202221200021221101211122002221022000100211020211121021222221212010100000000000, 10220111202202200200120011220201221200120211101221110011212112001121200212201000;

A  $[52, 16, 20]_3$  code:

22021201002000000000000000, 20211122210220200101122000;

A  $[105, 16, 49]_3$  code:



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  $C$  :  
 120000200221100000000000002221220220021221022100000020122211021022101000000002010102121001  
 2001222101100,  
 0120000200221100000000000000222122022002122102210000002012221102102210100000000201010212100  
 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  $\text{GF}(7)$ , *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  $\text{GF}(5)$ , *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-Chaudhuri, 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.