J. Algebra Comb. Discrete Appl.
2(3) • 211-216
Received: 29 May 2015; Accepted: 29 August 2015
DOI 10.13069/jacodesmath.66269

Journal of Algebra Combinatorics Discrete Structures and Applications

Some new quasi-twisted ternary linear codes*

Research Article

Rumen Daskalov[1], Plamen Hristov[1]*****

1. Department of Mathematics, Technical University of 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 basic and most important problems in coding theory is to construct codes with best possible minimum distances. In this paper seven quasi-twisted ternary linear codes are constructed. These codes are new and improve the best known lower bounds on the minimum distance in [6].

2010 MSC: 94B05, 94B65

Keywords: Ternary linear codes, Quasi-twisted codes

1. Introduction

Let $GF(q)$ denote the Galois field of q elements and let $V(n, q)$ denote the vector space of all ordered n-tuples over $GF(q)$. A q-ary linear code C of length n and dimension k, or an $[n, k]_q$ code, is a k-dimensional subspace of $V(n, q)$. An inner product (x, y) of vectors $x, y \in V(n, q)$ defines orthogonality in the space - two vectors are said to be orthogonal if their inner product is 0. The set of all vectors of $V(n, q)$ orthogonal to all codewords from C is called the orthogonal code $C^{\perp}$ to C. It is well-known that the code $C^{\perp}$ is a linear $[n, n-k]_q$ code.

A $k \times n$ matrix G whose rows form a basis of C is called a generator matrix of C. The number of nonzero coordinates of a vector $x \in V(n, q)$ is called its Hamming weight wt(x). The Hamming distance $d(x, y)$ between two vectors is defined by $d(x, y) = wt(x - y)$. The minimum distance of a linear code C is

$$d(C) = min\ \{d(x, y) \mid x, y \in C, x \neq y\} \ = \ min\ \{wt(c) \mid c \in C, c \neq 0\}.$$

A q-ary linear code of length n, dimension k and minimum distance d is said to be an $[n, k, d]_q$ code.

Let A_i denote the number of codewords of C with weight i. The weight distribution of C is the list of numbers A_i. The weight distribution $A_0 = 1$, $A_d = \alpha$, ..., $A_n = \gamma$ is expressed as $0^1 d^{\alpha} \ldots n^{\gamma}$ also.

* *This work was partially supported by the Bulgarian Ministry of Education and Science under Contract in TU–Gabrovo.*
** *E-mail: daskalov@tugab.bg (Corresponding Author)*
*** *E-mail: plhristov9@gmail.com*

If $C \subseteq C^{\perp}$, then the code C is called self-orthogonal. For a ternary linear code C the next theorem is well-known - every codeword of C has weight divisible by three if and only if C is self-orthogonal.

A central problem in coding theory is that of optimizing one of the parameters n, k and d for given values of the other two and q-fixed. Two are the basic versions:

Problem 1: Find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d]_q$ code.

Problem 2: Find $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d]_q$ code.

A code which achieves one of these two values is called *d-optimal* or *n-optimal* respectively. Both distance-optimal and length-optimal codes are called optimal codes.

The problem of finding the parameters of the optimal codes is very difficult one (see [15], [9]) and has two aspects - one is the construction of new codes with better minimum distances and the other is to prove the nonexistence of codes with given parameters. It is entirely solved only for small finite fields and dimensions (see the following table and [10], [2], [6]).

q	2	3	4	5, 7, 8, 9
$k \leq$	8	5	4	3

Many optimal linear codes are constructed when $n-k$ is also small (see [6]).

For the first aspect computer search is often used but it is well known fact that computing the minimum distance of a linear code is an NP-hard problem [16]. Since it is not possible to conduct exhaustive searches for linear codes with large dimension, a natural way is to focus our efforts on subclasses of linear codes, having rich mathematical structures. Quasi-twisted (QT) codes are known to have this structure and it has been shown in recent years that this subclass contains many new good linear codes [1,3-8,11-14].

Grassl [6] maintains a table with lower and upper bounds on minimum distances over small finite fields. For any n and k there are two numbers in the table - d_l and d_u. The former, d_l, is the best known minimum distance of an $[n,k,d]_q$ code constructed to date, whereas the latter, d_u, is the theoretical upper bound on the minimum distance of an $[n,k]_q$ code. When $d_l = d_u = d$ then the $[n,k,d]_q$ code is optimal. Many of the best-known codes in Grassl's tables are QT 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 we will call a *new* code.

Chen also maintains online tables of linear codes. Chen's table [3] contains only good and best-known QC and QT codes ($q \leq 13$). These two databases are updated when new codes are discovered.

2. Quasi-twisted codes

A code C is said to be quasi-twisted if a constacyclic shift of a codeword by p positions results in another codeword. A constacyclic shift of an m-tuple $(x_0, x_1, \ldots, x_{m-1})$ is the m-tuple $(\alpha x_{m-1}, x_0, \ldots, x_{m-2}), \alpha \in GF(q) \setminus \{0\}$. The blocklength, n, of a QT code is a multiple of p, so that $n = pm$.

A matrix B of the form

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

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

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

where B_i is a twistulant matrix [14].

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, $b(x) = b_0+b_1x+b_2x^2+\cdots+b_{m-1}x^{m-1}$, formed from the entries in the first row of B. The $b_i(x)$ associated with a QT code are called the *defining polynomials*.

If the defining polynomials $b_i(x)$ contain a common factor which is also a factor of $x^m-\alpha$, then the QT code is called *degenerate*. The dimension k of the QT code is equal to the degree of $h(x)$, where [14]

$$h(x) = \frac{x^m-\alpha}{\gcd\{x^m-\alpha, b_1(x), b_2(x), \cdots, b_p(x)\}}. \tag{3}$$

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

A p-QT code over $GF(q)$ of length $n = pm$ can be viewed as a $GF(q)[x]/(x^m-\alpha)$ submodule of $(GF(q)[x]/(x^m-\alpha))^p$ [14]. 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 is given in the next theorem.

Theorem 2.1. *[14]: 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 $1 \le i \le p$.

In this paper seven new one-generator QT codes ($p \ge 2$) are constructed, using an algebraic-combinatorial computer search similar to that in [14]. All constructed codes are self-orthogonal.

3. The new codes

We have restricted our search to one-generator QT codes with a generator of the form (4).

Example 3.1. *Let $q = 3$, $m = 52$ and $\alpha = 2$. The factorization of the polynomial $x^{52}+1$ over GF(3) is*

$$x^{52}+1 = \prod_{i=1}^{10} p_i(x),$$

where

$$\begin{array}{ll} p_1(x) = x^6+x^5+2x^4+2x^3+x^2+2x+2 & p_6(x) = x^6+x^5+2x^4+2x^3+2 \\ p_2(x) = x^6+2x^5+2x^4+x^3+x^2+x+2 & p_7(x) = x^6+2x^5+2x^4+x^3+2 \\ p_3(x) = x^6+2x^5+2x^4+2x^3+x^2+x+2 & p_8(x) = x^6+2x^3+x^2+x+2 \\ p_4(x) = x^6+x^5+2x^4+x^3+x^2+2x+2 & p_9(x) = x^2+x+2 \\ p_5(x) = x^6+x^3+x^2+2x+2 & p_{10}(x) = x^2+2x+2. \end{array}$$

Let the dimension k be 20. Then the degree of the polynomials $g(x)$ have to be 32. There are 2.$\binom{8}{3}$ = 112 possibilities to obtain a polynomial $g(x)$ of degree 32. We check these possibilities consecutively, using non-exhaustive search. When

$$g(x) = x^{32} + x^{31} + 2x^{30} + x^{28} + x^{27} + 2x^{26} + x^{25} + 2x^{24} + 2x^{23} + x^{22}$$

$$+x^{19} + 2x^{17} + x^{15} + 2x^{14} + x^{13} + x^{12} + 2x^{11} + 2x^{9} + 2x^{9} + 2x^{9} + 1$$

and

$$f_2(x) = x^8 + x^6 + 2x^5 + 2x^4 + x^3 + 2x^2 + x + 2,$$

a good $[104, 20, 45]_3$ quasi-twisted code is obtained.

Afterwards, we search for $f_3(x)$ and $f_4(x)$ in succession. The polynomial $f_3(x) = x^8 + x^7 + x^6 + x^5 + 2x^3 + x + 1$ yields a new $[156, 20, 75]_3$ code and the polynomial $f_4(x) = x^8 + 2x^2 + x + 1$ leads to a new $[208, 20, 105]_3$ code.

We conducted a similar search for other lengths. The obtained new results are presented in the next theorem.

Theorem 3.2. *There exist self-orthogonal one-generator quasi-twisted codes ($\alpha = 2$) with parameters:*

[156,14,84]$_3$, [136,18,66]$_3$, [156,18,78]$_3$, [80,20,33]$_3$
[156,20,75]$_3$, [208,20,105]$_3$, [164,24,75]$_3$.

Proof. The coefficients of the defining polynomials and the weight distributions of the codes are as follows:
A $[156, 14, 84]_3$ code ($m = 52, p = 3$):
200100111220002122221012202011222212001000000000000,
101011112210201121210220112002110000001212210000000,
101102011122002011012211210002200022210212200100000;
0^{1} 84^{4056} 87^{17992} 90^{60112} 93^{173576} 96^{384072} 99^{661024} 102^{904280} 105^{963976} 108^{789672} 111^{484120} 114^{233376} 117^{81648} 120^{20384} 123^{3952} 126^{624} 129^{104}

A $[136, 18, 66]_3$ code ($m = 34, p = 4$):
110021200022200210000000000000000,201212022220020122201201000000000,
111010110121022101221220001000000,101212002221120201100100111110000;
0^{1} 66^{4420} 69^{56712} 72^{332656} $75^{1654168}$ $78^{6230092}$ $81^{18084804}$ $84^{39732400}$ $87^{66373440}$ $90^{83286876}$ $93^{77889716}$ $96^{53790516}$ $99^{27168584}$ $102^{9809960}$ $105^{2509268}$ 108^{439892} 111^{52496} 114^{4284} 117^{204}

A $[156, 18, 78]_3$ code ($m = 52, p = 3$):
211222111110100020221010210001000010000000000000000,
200102112220110110011221000001201200021221100000000,
111121001212220010212021111110220200201020010000000;
0^{1} 78^{9568} 81^{52104} 84^{304304} $87^{1384448}$ $90^{4931680}$ $93^{13906776}$ $96^{30902040}$ $99^{53999712}$ $102^{73411312}$ $105^{77915448}$ $108^{63630008}$ $111^{39595816}$ $114^{18649384}$ $117^{6627296}$ $120^{1732224}$ 123^{321048} 126^{43056} 129^{4160} 132^{104}

A $[80, 20, 33]_3$ code ($m = 40, p = 2$):
200110001210221011001000000000000000000,
120222012221022122020120202210201000000;
0^{1} 33^{18960} 36^{359360} $39^{4063760}$ $42^{30350480}$ $45^{144118432}$ $48^{436419120}$ $51^{831804960}$ $54^{979844960}$ $57^{696755760}$ $60^{288531648}$ $63^{66176080}$ $66^{7894000}$ 69^{437440} 72^{9440}

A $[156, 20, 75]_3$ code $(m = 52, p = 3)$:
100010011002112102010012212110211000000000000000000,
122112020110220212000020221002110111211000000000000,
110212102001122201011201000220101010101211000000000;
0^{1} 75^{8216} 78^{70200} 81^{490568} $84^{2755480}$ $87^{12400856}$ $90^{44366920}$ $93^{125212568}$ $96^{278102448}$ $99^{485583176}$ $102^{661878672}$ $105^{700633856}$ $108^{572121472}$ $111^{356398640}$ $114^{168530440}$ $117^{59392328}$ $120^{15466360}$ $123^{2948400}$ 126^{387088} 129^{33904} 132^{2704} 135^{104}

A $[208, 20, 105]_3$ code $(m = 52, p = 4)$:
100010011002112102010012212110211000000000000000000,
212110000211011012102201101021120012100110000000000,
110212110202210100211120122011021001112100000000000,
112011210022102001212001001000222111021100000000000;
0^{1} 105^{6968} 108^{36816} 111^{225368} $114^{1084720}$ $117^{4490824}$ $120^{15554344}$ $123^{44887960}$ $126^{109041296}$ $129^{221353392}$ $132^{374073232}$ $135^{524057352}$ $138^{608355904}$ $141^{582839608}$ $144^{458328208}$ $147^{294288384}$ $150^{153923432}$ $153^{64968592}$ $156^{21913224}$ $159^{5855616}$ $162^{1267136}$ 165^{203736} 168^{25792} 171^{2392} 174^{104}

A $[164, 24, 75]_3$ code $(m = 82, p = 2)$:
112122211122101021202020212120222220202022201011221221222210000000000000000000000,
201112121010220021021120212001012200212100001121201101101200010201000000000000000;
0^{1} 75^{15744} 78^{172200} $81^{1673128}$ $84^{12794460}$ $87^{79656112}$ $90^{396419160}$ $93^{1584181452}$ $96^{5070823256}$ $99^{12959375940}$ $102^{26376357636}$ $105^{42571391912}$ $108^{54230847436}$ $111^{54217062252}$ $114^{42255118404}$ $117^{25471036636}$ $120^{11763022344}$ $123^{4119948304}$ $126^{1079104584}$ $129^{208391028}$ $132^{29038660}$ $135^{2892960}$ 138^{201720} 141^{10988} 144^{164}

From the constructed codes, by trivial constructions as shortening, puncturing and extension, 29 improvements on [6] are obtained. For example - from $[80, 20, 33]_3$ code it follows that there exist $[79, 19, 33]_3$, $[78, 19, 32]_3$, $[77, 19, 31]_3$, $[79, 20, 32]_3$, $[78, 20, 31]_3$ and $[81, 20, 33]_3$ codes. □

References

[1] R. Ackerman and N. Aydin, *New quinary linear codes from quasi-twisted codes and their duals*, Appl. Math. Lett., 24(4), 512–515, 2011.

[2] S. Ball, *Three-dimensional linear codes*, Online table, http://www-ma4.upc.edu/∼simeon/.

[3] E. Z. Chen, *Database of quasi-twisted codes*, available at http://moodle.tec.hkr.se/chen/research/codes/searchqt.htm

[4] E. Z. Chen, *A new iterative computer search algorithm for good quasi-twisted codes*, Des. Codes Cryptogr, 76(2), 307-323, 2014.

[5] R. Daskalov and P. Hristov, *New quasi-twisted degenerate ternary linear codes*, IEEE Trans. Inform. Theory, 49(9), 2259–2263, 2003.

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

[7] P. P. Greenough and R. Hill, *Optimal ternary quasi-cyclic codes*, Des. Codes Cryptogr., 2(1), 81–91, 1992.

[8] T. A. Gulliver and P. R. J. Ostergard, *Improved bounds for ternary linear codes of dimension 7*, IEEE Trans. Inform. Theory, 43, 1377–1388, 1997.

[9] R. Hill, *A first course in coding theory*, Oxford Applied Mathematics and Computing Sciences Series, 1992.

[10] T. Maruta, *Griesmer bound for linear codes over finite fields*, Online table, http://www.mi.s.osakafu-u.ac.jp/~maruta/griesmer.htm.

[11] T. Maruta, M. Shinohara and M. Takenaka, *Constructing linear codes from some orbits of projectivities*, Discrete Math., 308(5-6), 832–841, 2008.

[12] E. Metodieva and N. Daskalova, *Generating generalized necklaces and new quasi-cyclic codes*, Problemi Peredachi Informatsii, (submitted).
[13] I. Siap, N. Aydin and D. Ray-Chaudhury, *New ternary quasi-cyclic codes with better minimum distances*, IEEE Trans. Inform. Theory, 46(4), 1554–1558, 2000.
[14] I. Siap, N. Aydin and D. Ray-Chaudhury, *The structure of 1-generator quasi-twisted codes and new linear codes*, Des. Codes Cryptogr., 24, 313–326, 2001.
[15] S. Dougherty, J. Kim and P. Solé, *Open problems in coding theory*, Contemporary Mathematics, 634, http://dx.doi.org/10.1090/conm/634/12692, 2015.
[16] A. Vardy, *The intractability of computing the minimum distance of a code*, IEEE Trans. Inform. Theory, 43, 1757–1766, 1997.