New Quasi-Twisted Quaternary Linear Codes [1]

R.N. Daskalov, Member, IEEE
T.A. Gulliver, Senior Member, IEEE [2]

Abstract

Let $[n, k, d]_q$-codes be linear codes of length n, dimension k and minimum Hamming distance d over $GF(q)$. In this paper, thirty-one new quaternary ($q = 4$) codes are constructed which improve the respective lower bounds on minimum distance in Brouwer's tables.

Index Terms - quaternary linear codes, quasi-twisted codes.

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.

The class of quasi-twisted codes is a generalization of the class of quasi-cyclic codes over $GF(q)$, $(q > 2)$ [10]. A code is called quasi-twisted if a constacyclic[3] shift of a codeword by p positions results in another codeword.

The blocklength, n, of a QT code is a multiple of p, so that $n = mp$. A class of QT codes can be constructed from $m \times m$ twistulant matrices (with a suitable permutation of coordinates). In this case, the generator matrix, G, can be represented as

$$G = [B_1, \ B_2, \ \ldots \ , \ B_p] \, , \tag{1}$$

where the B_i are $m \times m$ *twistulant* matrices of the form

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

and $\alpha \in$GF$(q)\backslash\{0\}$.

[1] This work was partially supported by the Bulgarian National Science Fund.

[2] R.N. Daskalov is with the Department of Mathematics, Technical University, 5300 Gabrovo, Bulgaria, daskalov@tugab.bg. T.A. Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6, agullive@ece.uvic.ca.

[3] 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$(q)\backslash\{0\}$.

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* [5]. If $\alpha = 1$, we obtain the algebra of $m \times m$ circulant matrices [12], and a subclass of quasi-cyclic codes.

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* [5]. The *order* of this QT code is defined as [13]

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

where $\alpha \in$GF$(q)\backslash\{0\}$, and the code dimension, k, is equal to the degree of $h(x)$. If $h(x)$ has degree m, $k = m$, and (1) 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 (1).

Many good linear codes over $GF(4)$ have been found previously [1], [3], [4], [6], [7], [9], [11]. In this paper, new linear QT codes with $k \geq 6$ are constructed using a nonexhaustive heuristic tabu search, similar to that in [6],[7],[8]. Because the search space for these codes is very large, techniques were used to reduce the number of defining polynomials considered at each step. These were based on considering only a subset of defining polynomials, either by choosing a subset at random before starting the search, or by choosing a subset for each iteration of the search. With this approach, 31 new codes were obtained which improve the respective lower bounds on minimum distance given by Brouwer [2]. These codes are listed below. The elements of GF(4) are taken to be $\{0, 1, \beta, \beta^2\}$, where β is denoted by 2 and β^2 is denoted by 3. The weight enumerator of a code C is given by a sequence of type i^{A_i} where A_i is the number of codewords of weight i in C.

2 The New Codes

In this section, we present the new codes. The parameters of these codes are given in Table 1. The minimum distances, d_{br} [2], of the previously best known codes are given for comparison.

Theorem 1 : There exists a $[33, 8, 18]_4$-code.

Proof.

$$G = \begin{pmatrix} 100000001202320300232212201223021 \\ 010000002120232010023221120122301 \\ 001000000212023231002322012012233 \\ 000100001021202313100232201201223 \\ 000010002102120211310023120120122 \\ 000001001210212021131002112012012 \\ 000000100121021212113100311201201 \\ 000000011012102101211310031120121 \end{pmatrix}.$$

The weight enumerator of this code is

$$0^{1}18^{396}19^{1200}20^{1944}21^{3552}22^{4452}23^{7632}24^{9948}25^{10704}26^{9300}27^{7920}28^{4632}29^{2592}30^{1020}31^{144}32^{51}33^{48}.$$

Theorem 2 : There exist quasi-cyclic codes ($\alpha = 1$) with parameters:

$$\begin{array}{llll} [216,6,155]_4, & [222,6,159]_4, & [50,7,32]_4, & [112,7,76]_4, \\ [143,7,99]_4, & [150,7,104]_4, & [156,7,108]_4, & [161,7,111]_4, \\ [169,7,118]_4, & [175,7,121]_4, & [182,7,127]_4, & [190,7,132]_4, \\ [195,7,136]_4, & [200,7,140]_4, & [208,7,146]_4, & [221,7,156]_4, \\ [30,11,13]_4, & [52,12,25]_4, & [39,13,16]_4, & [45,15,18]_4, \\ [48,16,19]_4. & & & \end{array}$$

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

A $[216, 6, 155]_4$**-code:**
000132, 111323, 001231, 011313, 111322, 013122, 011323, 013032, 012103, 011132, 012232, 011222, 013312, 001233, 113212, 013321, 000131, 011312, 001303, 012121, 011112, 012212, 010123, 001313, 000101, 001211, 011033, 012211, 011211, 001112, 012302, 013212, 011302, 001133, 012222, 112212;

A $[222, 6, 159]_4$**-code:**
011322, 011311, 001023, 010113, 013112, 011313, 001211, 012132, 111313, 112132, 111122, 011121, 013233, 113232, 000112, 012232, 111223, 001011, 112122, 011323, 111232, 001322, 011122, 013131, 012122, 011212, 011112, 010133, 001022, 012323, 012233, 013322, 000133, 013022, 011123, 000102, 111332;

A $[50, 7, 32]_4$**-code:**
0212230101, 0021123131, 0210331301, 0033333131, 0030123021;

A $[112, 7, 76]_4$**-code:**
00030311, 00112031, 01213331, 02332321, 22331221, 02212131, 00311201, 02221131, 00033321, 03031331, 01311211, 02312031, 00121121, 00021201;

A $[143, 7, 99]_4$**-code:**
0013300300331, 0003103210021, 0020312013311, 0310303211201, 0022223122111, 0232331303331, 0310110302321, 0313023331211, 0003222031211, 0033223013201, 0123120131211;

A $[150,7,104]_4$**-code:**
0000112211, 0030232321, 0232331121, 0122210121, 0003211331, 0311212211, 0321231231, 0312223311, 0032013311, 0020232221, 0003013001, 0202213321, 0222323231, 0031211011, 0013310011;

A $[156,7,108]_4$**-code:**
0232113230321, 0232312313011, 0021103002101, 0201101123301, 0002021010211, 0320333213321, 0000013233231, 0111113330221, 0021222223331, 0020331003031, 0030302010121, 0231322032301;

A $[161,7,111]_4$**-code:**
0110123, 0001232, 0110302, 0113302, 0112112, 0001033, 0122103, 0012113, 0122231, 1112233, 0123311, 1122312, 0101133, 0010113, 0123322, 1111313, 0131233, 0122031, 0010223, 0101212, 1111212, 1123213, 0133221;

A $[169,7,118]_4$**-code:**
0001301130201, 0233201133311, 0233321231211, 0033022130131, 0231233310331, 0013130203131, 0031021333021, 0012103321331, 0232122210211, 0311020132301, 0323223230131, 0213210112131, 0230133023111;

A $[175,7,121]_4$**-code:**
1113313, 0133222, 0102022, 0130303, 0013112, 0011133, 0013201, 0012111, 1112112, 0130222, 0001011, 1111223, 0121133, 0113131, 0120121, 0000012, 0120122, 0133113, 0123033, 1123123, 0112332, 0012012, 0123233, 0122232, 0121332;

A $[182,7,127]_4$**-code:**
0111232111011, 0000231300221, 0031312122001, 0000303032131, 0131133331131, 0233120312121, 0022133323211, 0211111120131, 1211312222131, 0012132301201, 0002101312311, 0120231031331, 0031130011011, 0132333113021;

A $[190,7,132]_4$**-code:**
0003131101, 0033112121, 0023131301, 0333111121, 0000013031, 0211323101, 0012100121, 0133332131, 0010302231, 0012013111, 0232230301, 0213312011, 0303033321, 0231230331, 0003030321, 0232011311, 0031123031, 0230121021, 0223323221;

A $[195, 7, 136]_4$**-code:**
0002312201231, 0120332323111, 0023011123021, 0213131333301, 0310121322211, 0212102211101, 0013331320201, 0012132301201, 0313230222331, 0233230113221, 0032003022121, 0031002323301, 0031021333021, 0320333213321, 0011022322011;

A $[200, 7, 140]_4$**-code:**
0031022211, 0030302031, 0030123021, 0030333101, 0210323111, 0312322131, 0113113321, 0021302121, 0032123001, 0021022311, 0023123111, 2313211111, 0231213011, 0231011321, 0000203111, 0130332101, 0023333031, 0322212121, 0011321101, 0322322231;

A $[208, 7, 146]_4$**-code:**
0322020211131, 0023003113231, 0003031122331, 0002211113011, 0231301022021, 0002220133121, 0332121130331, 0121112312231, 0002033020001, 3132133123131, 0131332212201, 1211122321331, 0010112112031, 0023322332001, 0311131210331, 0021222223331;

A $[221, 7, 156]_4$**-code:**
0012333222131, 0232232011111, 0030302010121, 0232323333121, 0013331320201, 0023100201011, 0032123320021, 0033303311301, 0000231300221, 0022013021311, 0123213320231, 0303312113211, 0020130120301, 0121032010331, 0310320201121, 0022133323211, 0030111103001;

A $[30, 11, 13]_4$**-code:**
000000012011311, 000102130120031;

A $[52, 12, 25]_4$**-code:**
0000011231022, 0000011112233, 0000011123303, 0000011201201;

A $[39, 13, 16]_4$**-code:**
0001222301123, 0000102122121, 0000000000001;

A $[45, 15, 18]_4$**-code:**
000000101331113, 000001012113231, 000000000000001;

A $[48,16,19]_4$**-code:**
0000001102113212, 0000001011211233, 0000000000000001;

Theorem 3 : There exist quasi-twisted codes ($\alpha = 2$) with parameters:

$$[200,8,135]_4, [208,8,141]_4, [232,8,158]_4$$

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

A $[200,8,135]_4$**-code:**
00011102, 01021112, 01131322, 01210302, 01013220, 01131332, 01032212, 01233302, 01232223, 01131232, 10231231, 01332211, 01331111, 10222323, 01333031, 11311312, 00120013, 13333203, 10331212, 00130303, 01033021, 10213121, 01101322, 12203332, 01213231;

A $[208,8,141]_4$**-code:**
01213231, 00120133, 00013303, 01021112, 01131322, 01210302, 01013220, 01131332, 01032212, 01233302, 01232223, 01131232, 10231231, 01332211, 01331111, 10222323, 01333031, 11311312, 00120013, 13333203, 10331212, 00130303, 01033021, 10213121, 01101322, 12203332;

A $[232,8,158]_4$**-code:**
00000111, 00111123, 01020132, 00120133, 00013303, 01021112, 01131322, 01210302, 01013220, 01131332, 01032212, 01233302, 01232223, 01131232, 10231231, 01332211, 01331111, 10222323, 01333031, 11311312, 00120013, 13333203, 10331212, 00130303, 01033021, 10213121, 01101322, 12203332, 01213231;

Theorem 4 : There exist quasi-twisted codes ($\alpha = 3$) with parameters:

$$[204,6,146]_4, \quad [228,6,164]_4, \quad [176,8,118]_4, \quad [184,8,124]_4,$$
$$[216,8,146]_4, \quad [224,8,152]_4.$$

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

A $[204, 6, 146]_4$**-code:**
122111, 233111, 131000, 212010, 322110, 111111, 312310, 231211, 212211, 323310, 131310, 211310, 231311, 222100, 220100, 322100, 301000, 310310, 111100, 133210, 131100, 211100, 100100, 133010, 313210, 233310, 123110, 323100, 311110, 123111, 211110, 230100, 303100, 203100;

A $[228, 6, 164]_4$**-code:**
101010, 211110, 322010, 301100, 123010, 101100, 111110, 221110, 122010, 111210, 331100, 222310, 112311, 121010, 211310, 223310, 220100, 121310, 233310, 232310, 312110, 133310, 201100, 113310, 333110, 210110, 210100, 132211, 311010, 112110, 331010, 113010, 331310, 221210, 221211, 211111, 201010, 212311;

A $[176, 8, 118]_4$**-code:**
00001313, 00101111, 01222133, 00123122, 00121223, 01032212, 01211111, 00121021, 01130132, 01322332, 01233213, 00131133, 01232222, 00122313, 01023121, 01321212, 00112121, 01212021, 01102002, 13302133, 00000111, 01213013;

A $[184, 8, 124]_4$**-code:**
00132232, 01130213, 00101111, 01222133, 00123122, 00121223, 01032212, 01211111, 00121021, 01130132, 01322332, 01233213, 00131133, 01232222, 00122313, 01023121, 01321212, 00112121, 01212021, 01102002, 13302133, 00000111, 01213013;

A $[216, 8, 146]_4$**-code:**
00012313, 11210031, 00133233, 10202311, 01022113, 01003011, 11333323, 01203221, 01133203, 13020333, 10033213, 12303033, 10322202, 10033333, 11313033, 10323022, 01100332, 12130332, 10330303, 13000222, 11203032, 11321202, 10303022, 01030103, 01331222, 01131323, 01131232;

A $[224, 8, 152]_4$**-code:**
00113301, 00101212, 11210031, 00133233, 10202311, 01022113, 01003011, 11333323, 01203221, 01133203, 13020333, 10033213, 12303033, 10322202, 10033333, 11313033, 10323022, 01100332, 12130332, 10330303, 13000222, 11203032, 11321202, 10303022, 01030103, 01331222, 01131323, 01131232;

References

[1] I. Boukliev, R. Daskalov and S. Kapralov, "Optimal quaternary linear codes of dimension five," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1228-1235, 1996.

[2] A.E. Brouwer, Linear code bound (server), Eindhoven University of Technology, The Netherlands, `http://www.win.tue.nl/win/math/dw/voorlincod.html`.

[3] R.N. Daskalov and T.A. Gulliver, "New good quasi-cyclic ternary and quaternary linear codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1647–1650, 1997.

[4] P. P. Greenough and R. Hill, "Optimal linear codes over GF(4)," *Discrete Math.*, vol. 125, pp. 187-199, 1994.

[5] P.P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Des., Codes & Crypt.*, vol. 2, pp. 81–91, 1992.

[6] T. A. Gulliver, "New optimal quaternary linear codes of dimension 5," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2260-2265, 1996.

[7] T. A. Gulliver and V. K. Bhargava, "New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes," *Des. Codes Cryptogr.*, vol. 7, pp. 223-233, 1996.

[8] T.A. Gulliver and P. Östergård, "Improvements to the bounds on quaternary linear codes of dimension 6," *Applic. Algebra in Eng., Commun. & Comput.*, (to appear).

[9] N. Hamada, "The nonexistence of some quaternary linear codes meeting the Griesmer bound and the bounds for $n_4(5,d), 1 \leq d \leq 256$," *Math. Japonica*, vol. 43, pp. 7-21, 1996.

[10] R. Hill and P.P. Greenough, "Optimal quasi-twisted codes," Proc. *Int. Workshop Algebraic and Comb. Coding Theory*, Voneshta Voda, Bulgaria, pp. 92-97, June 1992.

[11] F.R. Kschischang and S. Pasupathy, Some Ternary and Quaternary Codes and Associated Sphere Packings, *IEEE Trans.Inform.Theory*, vol.38, pp. 227-246, 1992.

[12] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., New York, NY, 1977.

[13] G.E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes," Technical Report, Royal Military College of Canada, Kingston, ON, Canada, 1991.

Table 1: Minimum Distances of the New Quaternary Linear Codes.

code	d	d_{br}	code	d	d_{br}
[204,6]	146	145	[208,7]	146	144
[216,6]	155	153	[221,7]	156	153
[222,6]	159	157	[33,8]	18	17
[228,6]	164	162	[176,8]	117	116
[50,7]	32	31	[184,8]	124	123
[112,7]	76	75	[200,8]	135	134
[143,7]	99	97	[208,8]	141	140
[150,7]	104	100	[216,8]	146	144
[156,7]	108	105	[224,8]	152	151
[161,7]	111	109	[232,8]	158	156
[169,7]	118	115	[30,11]	13	12
[175,7]	121	118	[52,12]	25	24
[182,7]	127	124	[39,13]	16	15
[190,7]	132	130	[45,15]	18	17
[195,7]	136	133	[48,16]	19	18
[200,7]	140	137			

Table Captions

Table I: Minimum Distances of the New Quaternary Linear Codes.