New Ternary Linear Codes[1]

R.N. Daskalov, Member, IEEE
T.A. Gulliver, Senior Member, IEEE
and E. Metodieva[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, eighteen codes are constructed which improve the known lower bounds on minimum distance.

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

1 Introduction

Let $GF(q)$ denote the Galois field of q elements. A linear code over $GF(q)$ of length n, dimension k and minimum Hamming distance d is called an $[n, k, d; q]$-code. This paper considers the class of quasi-twisted (QT) codes, which is a generalization of the class of quasi-cyclic codes over GF(q), $(q > 2)$ [7]. A code is called quasi-twisted if a constacyclic[3] shift of a codeword by p positions results in another codeword.

The length 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

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

[1] This work was partially supported by the Bulgarian National Science Fund under Grant I-618/96.

[2] R.N. Daskalov and E. Metodieva are with the Department of Mathematics, Technical University, 5300 Gabrovo, Bulgaria, daskalov@tugab.bg. T.A. Gulliver is with the Department of Electrical and Electronic Engineering, University of Canterbury, Private Bag 4800, Christchurch, New Zealand, Gulliver@elec.canterbury.ac.nz.

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

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

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

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

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* [3]. If $\alpha = 1$, we obtain the algebra of $m \times m$ circulant matrices [8].

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* [3]. The *order* of a QT code is defined as [9]

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

where $\alpha \in \mathrm{GF}(q)\backslash\{0\}$, 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 QT codes over $GF(3)$ with $k \leq 8$ have been found previously [2]-[6]. In this paper, new linear QT codes with $k \geq 9$ are constructed using a nonexhaustive heuristic tabu search, similar to that in [4]-[6]. 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. The success of this approach is evident by the new codes presented here which improve the respective lower bounds on minimum distance given by Brouwer [1].

2 The New Codes

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

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

$$[104, 9, 60], [130, 9, 76], [143, 9, 85], [156, 9, 93], [65, 13, 30; 3],$$
$$[56,14,24;3], [60, 14, 25; 3], [60, 15, 24; 3], [64, 16, 26 : 3], [68, 17, 27; 3],$$
$$[72,17,29;3], [134, 17, 64; 3], [153, 17, 74; 3], [54, 18, 19; 3], [72, 18, 28; 3].$$

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

A [104,9,60;3]-code:

0110201222112, 0001101101121, 0000102221022, 0012222122001,
0011012122011, 0111122212101, 0000110021001, 0000122020122;

$0^{1}60^{1066}63^{2392}66^{3198}69^{5018}72^{4160}75^{2626}78^{936}81^{260}84^{26}$

A [130,9,76;3]-code:

0111221122122, 0010212212001, 0011022001212, 0010202022102,
0012012121212, 0010121022012, 0001110100212, 0121120122222,
0012122101212, 0121111021122;

$0^{1}76^{364}77^{338}78^{624}79^{702}80^{572}81^{1066}82^{1196}83^{988}84^{1118}85^{1274}86^{1560}87^{1326}88^{1014}89^{1326}90^{1430}91^{988}92^{884}$
$93^{962}94^{390}95^{442}96^{390}97^{312}98^{208}99^{104}100^{78}102^{26}$

A [143,9,84;3]-code:

0001012020021, 0012211201011, 0110120112012, 0012100102212,
0012101202012, 0000102001002, 0011011212201, 0001121211222,
0001012111002, 0012100212222, 0011101010121;

$0^{1}84^{780}87^{1768}90^{2262}93^{3822}96^{4186}99^{3120}102^{2340}105^{1066}108^{260}111^{78}$

A [156,9,93;3]-code:

0112021211121, 0001020211011, 0010201112022, 0121222010211,
0121012111101, 0012101001021, 0111110202012, 0110212212111,
0110122012212, 0000121110012, 0000011012001, 0011200102101;

$0^{1}93^{1040}96^{1664}99^{2834}102^{4030}105^{3536}108^{3094}111^{1846}114^{1118}117^{416}120^{104}$

A [65,13,30;3]-code:

0000000000001, 0000111202122, 0010011001222, 0000101110221, 0000011212022;

$0^{1}30^{1326}33^{15496}36^{78988}39^{255088}42^{466024}45^{460876}48^{245284}51^{63232}54^{7722}57^{286}$

A [56,14,24;3]-code:

00000000000001, 00100111121112, 00010120221221, 00000101222021;

$0^{1}24^{2338}27^{27384}30^{193032}33^{748916}36^{1482460}39^{1471092}42^{703256}45^{143500}48^{10794}51^{196}$

A [60,14,25;3]-code:

000001210211202, 000000111221202, 000000001002012, 000000010122021;

$0^{1}25^{90}26^{630}27^{1350}28^{3150}29^{7140}30^{15230}31^{27360}32^{49050}33^{86170}34^{134370}35^{201000}36^{278150}37^{365490}38^{444330}$
$39^{491040}40^{518136}41^{502830}42^{464050}43^{381930}44^{299760}45^{210750}46^{138660}47^{82500}48^{43000}49^{21720}50^{8820}$
$51^{4430}52^{1200}53^{450}54^{150}55^{30}60^{2}$

A [60,15,24;3]-code:

000000000000001, 000010021222111, 000001010201222, 000000011021211;

$0^{1}24^{210}25^{600}26^{1800}27^{4050}28^{8520}29^{21150}30^{43936}31^{83340}32^{149850}33^{255340}34^{406950}35^{608400}36^{834220}$
$37^{1090620}38^{1311450}39^{1482010}40^{1560720}41^{1530750}42^{1375300}43^{1159020}44^{887700}45^{627970}46^{410610}47^{249300}$

$48^{134770}49^{65310}50^{27960}51^{11830}52^{3750}53^{1140}54^{210}55^{90}56^{30}$

A [64,16,26;3]-code:

0000000000000001, 0000101101120111, 0000000100211221, 0000010112221211;

$0^{1}26^{560}27^{1632}28^{3776}29^{9056}30^{23328}31^{46048}32^{98968}33^{190752}34^{349280}35^{597472}36^{969696}37^{1461216}38^{2072400}$
$39^{2754560}40^{3448220}41^{4036992}42^{4433840}43^{4562432}44^{4324528}45^{3842112}46^{3178400}47^{2419584}48^{1720394}49^{1123616}$
$50^{682896}51^{378080}52^{183296}53^{82304}54^{33392}55^{12000}56^{4432}57^{1088}58^{304}59^{32}60^{32}64^{2}$

A [68,17,27;3]-code:

00000000000000001, 00000010220122212, 00000000111021221, 00000011202102211;

$0^{1}27^{612}28^{1088}29^{3740}30^{9010}31^{21896}32^{49368}33^{112030}34^{226372}35^{440334}36^{804406}37^{1398352}38^{2289560}39^{3523182}$
$40^{5071304}41^{6970102}42^{8882568}43^{10850046}44^{12273898}45^{13116486}46^{13097548}47^{12251696}48^{10752126}49^{8753198}$
$50^{6652882}51^{4692852}52^{3077136}53^{1860922}54^{1033430}55^{516902}56^{247962}57^{102578}58^{38352}59^{12580}60^{4250}61^{1088}$
$62^{238}63^{68}$

A [72,17,29;3]-code:

000000000112112201, 000000000111202102, 000000001111210012, 000000011112112201;

$0^{1}29^{720}30^{1134}31^{2880}32^{6192}33^{16500}34^{39492}35^{85428}36^{175524}37^{338976}38^{619164}39^{1096704}40^{1798038}41^{2798388}$
$42^{4138518}43^{5788872}44^{7625034}45^{9492064}46^{11102256}47^{12325644}48^{12839814}49^{12563856}50^{11542824}51^{9974352}52^{8053632}$
$53^{6078960}54^{4290074}55^{2811852}56^{1695726}57^{954144}58^{485280}59^{234540}60^{102708}61^{40284}62^{13950}63^{4440}64^{1620}65^{468}$
$66^{108}72^{2}$

A [136,17,64;3]-code:

00000000000000001, 00011221212201012, 00001112012110221, 00000010220122212,
00000000111021221, 00000011202102211, 00000010110121122, 00000010102121111;

$0^{1}64^{306}65^{272}66^{748}67^{1632}68^{3198}69^{6120}70^{11798}71^{21658}72^{35870}73^{65212}74^{109718}75^{182240}76^{292264}77^{458252}$
$78^{687174}79^{1021224}80^{1454180}81^{2002634}82^{2684368}83^{3507236}84^{4440128}85^{5415860}86^{6401486}87^{7378918}88^{8223342}$
$89^{8839728}90^{9253542}91^{9340344}92^{9161776}93^{8639366}94^{7915336}95^{6987340}96^{5983626}97^{4932584}98^{3944578}99^{3015596}$
$100^{2237370}101^{1591472}102^{1088408}103^{720766}104^{456246}105^{275842}106^{162962}107^{89284}108^{50252}109^{25636}110^{12444}$
$111^{5712}112^{2176}113^{1156}114^{442}115^{102}116^{136}117^{102}$

A [153,17,74;3]-code:

00000000000000001, 00011212222001111, 00011221212201012, 00001112012110221,
00000010220122212, 00000000111021221, 00000011202102211, 00000010110121122,
00000010102121111;

$0^{1}74^{170}75^{442}76^{748}77^{1802}78^{2992}79^{5066}80^{10200}81^{18258}82^{31858}83^{52836}84^{85544}85^{143992}86^{225964}87^{349962}$
$88^{519350}89^{768570}90^{1092284}91^{1495014}92^{2038436}93^{2689774}94^{3414688}95^{4223786}96^{5108296}97^{6015110}98^{6891868}$
$99^{7603012}100^{8222254}101^{8634980}102^{8831602}103^{8755238}104^{8399088}105^{7839482}106^{7066356}107^{6244304}$
$108^{5317022}109^{4399838}110^{3495812}111^{2716736}112^{2044556}113^{1481550}114^{1033056}115^{711008}116^{460870}117^{289068}$
$118^{179282}119^{104516}120^{59330}121^{31348}122^{16456}123^{9010}124^{3910}125^{1904}126^{714}127^{510}128^{170}129^{102}130^{34}132^{34}$

A [54,18,19;3]-code:

000000000000000001, 000000000102201021, 000112210221022222;

$0^{1}19^{972}20^{2178}21^{7200}22^{22140}23^{59148}24^{160518}25^{372564}26^{840870}27^{1740456}28^{3351528}29^{6021648}30^{10063422}$
$31^{15531192}32^{22300902}33^{29760672}34^{36807336}35^{42065820}36^{44394630}37^{43148448}38^{38644668}39^{31663908}40^{23798214}$

$41^{16212672}42^{10093494}43^{5583348}44^{2808090}45^{1245348}46^{492984}47^{162252}48^{49374}49^{11700}50^{2232}51^{504}52^{54}54^{2}$

[72,18,28;3]-code:

000000000000000001, 000000001011121202, 000000000102201021, 000112210221022222;

$0^{1}28^{486}29^{864}30^{2952}31^{8532}32^{21114}33^{51384}34^{116928}35^{253008}36^{522078}37^{1016712}38^{1886040}39^{3260616}40^{5396040}$
$41^{8425260}42^{12430398}43^{17300016}44^{22855014}45^{28489068}46^{33394464}47^{36882036}48^{38539686}49^{37702224}50^{34661862}$
$51^{29949600}52^{24155910}53^{18228672}54^{12820160}55^{8390628}56^{5120316}57^{2877564}58^{1476378}59^{702720}60^{301788}$
$61^{118656}62^{42804}63^{12888}64^{4104}65^{1404}66^{78}67^{36}$

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

$$[100, 10, 55], [150, 10, 87], [170, 10, 99].$$

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

A [100,10,55;3]-code:

0112021122, 0010221101, 0011200212, 1121221121, 0010121021,
0001002002, 0101201021, 0122212211, 0010122111, 0101222012;

$0^{1}55^{460}56^{600}57^{240}58^{1320}59^{1900}60^{740}61^{3140}62^{4100}63^{1280}64^{5380}65^{6440}66^{1280}67^{6680}68^{5760}69^{1460}70^{5204}71^{4640}$
$72^{1200}73^{3020}74^{2160}75^{340}76^{880}77^{500}78^{20}79^{140}80^{104}82^{20}83^{40}$

A [150,10,87;3]-code:

0012020101, 0000101121, 0111021021, 0112221012, 0111022112, 0010220202, 00111102 02, 0122112221,
0102222012, 0102011021, 0111121211, 0012211212, 0121211212, 0111201121 0012211111
$0^{1}87^{1420}90^{2904}93^{5840}96^{9520}99^{11700}102^{11280}105^{8704}108^{4940}111^{2100}114^{480}117^{120}120^{40}$

A [150,10,87;3]-code:

0111012221, 0010222221, 0010112112, 0111220212, 0012112201, 0010210021, 00101221 22, 0010211222,
0122012211, 0112222112, 0001012112, 0001212012, 0000111102, 0102121021 0102120122, 0102112112,
0102112121;

$0^{1}99^{760}102^{2260}105^{5380}108^{8060}111^{9780}114^{10840}117^{9880}120^{6928}123^{3260}126^{1360}129^{400}132^{140}$

Table 1: Minimum Distances of the new linear codes over GF(3).

code	d	d_{br}	code	d	d_{br}
[104,9]	60	59	[60,14]	25	24
[130,9]	76	75	[60,15]	24	22
[143,9]	84	83	[64,16]	26	24
[156,9]	93	91	[68,17]	27	25
[100,10]	55	54	[72,17]	29	27
[150,10]	87	85	[136,17]	64	63
[170,10]	99	97	[153,17]	74	73
[65,13]	30	28	[54,18]	19	18
[56,14]	24	22	[72,18]	28	27

References

[1] A.E. Brouwer, Minimum distance bounds for linear codes over GF(3), lincodbd server, aeb@cwi.nl, Eindhoven University of Technology, Eindhoven, the Netherlands.

[2] 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.

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

[4] T.A. Gulliver and P.R.J. Östergård, "Improved bounds for ternary linear codes of dimension 7," *IEEE Trans. Inf. Theory*, vol. 43, pp.1377–1381, 1997.

[5] T.A. Gulliver and P.R.J. Östergård, "Improved bounds for ternary linear codes of dimension 8," (submitted).

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

[7] 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.

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

[9] 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.