New Optimal Ternary Linear Codes of Dimension 6[1]

T. Aaron Gulliver[2]

Abstract In this paper, new optimal (pm, m) and $(pm, m-1)$ ternary linear codes of dimension 6 are presented. These codes belong to the class of quasi-twisted codes, and have been constructed using a greedy local search algorithm. Other codes are also given which provide a lower bound on the maximum possible minimum distance. The minimum distances of known quasi-twisted codes of dimension 6 are given.

Keywords: quasi-twisted codes, heuristic search, optimal ternary linear codes

I. Introduction

A fundamental and challenging problem in coding theory is to find a linear (n, k) code over GF(q) achieving the maximum possible minimum Hamming distance, d_{min}. This value is denoted as $d_q(n, k)$, and linear codes which have a minimum distance equal to $d_q(n, k)$ are called *optimal.* A related problem is to find the smallest value of n for which there exists an (n, k) code with minimum distance d. This is denoted as $n_q(d, k)$. For

[1]This research was supported in part by the Natural Sciences and Engineering Research Council of Canada.

[2]T. Aaron Gulliver is with the Department of Systems and Computer Engineering, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, Canada K1S 5B6, gulliver@sce.carleton.ca.

a given value of q, solving one of these problems is equivalent to solving the other. For $q = 3$, $n_q(d,k)$ has been determined for $k \leq 4$ [1], and all but 11 values of $n_3(d,5)$ have been established [2]. Conversely, there remain many unknown values of $n_3(d,6)$ and $d_3(n,6)$. Lower bounds for linear codes over GF(3) with $k \leq n \leq 50$, have been tabulated by Kschischang and Pasupathy [3]. Sloane [4] is presently tabulating bounds and Brouwer [5] maintains an up to date table of upper and lower bounds for $k \leq n \leq 132$. In this paper several values of $d_3(n,6)$ are determined through code constructions.

The Gilbert-Varshamov bound [6] gives a lower bound on $d_q(n,k)$, but few classes of codes are known which attain this bound. One exception is the class of rate $1/p$ quasi-twisted (QT) codes, which has been shown to meet this bound [7]. Therefore it is not surprising that QT codes exists for many values of $d_q(n,k)$. QT codes were first characterized by Hill and Greenough [8]. They are a generalization of the class of quasi-cyclic (QC) codes in the same way that constacyclic codes are a generalization of cyclic codes [9, 3].

A *best* code is defined as one which achieves the maximum possible minimum distance for a given class of linear codes. A *good* code is defined as one which has the maximum known minimum distance for a given n and k, i.e., it attains (or improves) the known lower bound on the minimum distance. In general, to find a best (n,k) linear code requires an almost exhaustive search, which is intractable for all but the smallest code dimensions. In fact, this problem falls into the class of NP-hard combinatorial optimization problems [10]. While the restriction to QT codes considerably reduces the search, this approach also becomes computationally intensive as k increases because the number of potential codes increases very rapidly [11]. Therefore some means must be found to prune the search, while maintaining the possibility of achieving $d_q(n,k)$.

The approach taken here is to begin with an arbitrary QT code of the required blocklength and dimension, and use a greedy

local search to find a better code. By restricting the search to QT codes, and using a heuristic algorithm rather than one which guarantees a best code, good codes can be found with a reasonable amount of computational effort. The next section describes the class of QT codes considered. Section 3 gives the construction results, and lists the codes which have improved the lower bounds on $d_3(n,6)$, as well as all new optimal codes. These codes extend previous results on rate $1/p$ [12] and rate $(m-1)/pm$ [13] QC codes.

II. Quasi-Twisted Codes

The class of quasi-twisted codes is a generalization of the class of quasi-cyclic codes over GF(q), $q > 2$ [8]. A code is called quasi-twisted if a negacyclic[1] shift of a codeword by p positions results in another codeword. Thus if $p = 1$ the code is constacyclic. The blocklength, n, of a QT code is a multiple of p, so that $n = mp$. Many 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)$\backslash\{0\}$. The algebra of $m \times m$ twistulant matrices over GF(q) is isomorphic to the algebra of polynomials in the

[1] A negacyclic 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)$\backslash\{0\}$.

ring $\mathrm{GF}(q)[x]/(x^m - \alpha)$ if B_i is mapped onto the polynomial,

$$b_i(x) = b_{0,i} + b_{1,i}x + b_{2,i}x^2 + \cdots + b_{m-1,i}x^{m-1}$$

formed from the entries in the first row of B_i. The $b_i(x)$ are called *defining polynomials.* If $\alpha = 1$, we obtain the algebra of $m \times m$ circulant matrices [6], and a subclass of quasi-cyclic codes.

The 1-generator QC codes [14] can be generalized to 1-generator QT codes. The *order* of a 1-generator QT code, V, is defined as

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

where $\alpha \in \mathrm{GF}(q)\backslash\{0\}$, and k, the dimension of V, is equal to the degree of $h(x)$. If $h(x)$ has degree m, the dimension of V is m, and (1) is a generator matrix for V. If $\deg(h(x)) = k < m$, a generator matrix for V can be constructed by deleting $m-k$ rows of (1). Only codes with $k = 6$ and $m = 6$ or 7 are considered in this paper.

A search for good QT codes requires a representative set of defining polynomials. Consider the set, A, of polynomials of degree $m - 1$ or less, with $|A| = q^m$ elements. Let two polynomials, $b_j(x)$ and $b_i(x)$ belong to the same equivalence class if

$$b_j(x) = ax^l b_i(x) \bmod (x^m - \alpha),$$

for some integer l and scalar $a \in \mathrm{GF}(q)\backslash\{0\}$. This means that two polynomials are in the same class if one can be obtained from the other by a constacyclic shift, by multiplying by a nonzero scalar, or both. Only one polynomial from each class need be considered when constructing QT codes since polynomials from the same class produce equivalent codes [11]. This equivalence relation is induced by the action of a finite group on the set of ternary n-tuples. Distinct equivalence classes correspond to distinct orbits under the action of this group and so can be enumerated using Burnside's Lemma [11]. It has been shown

that if m is odd, the ternary QT codes are equivalent to QC codes [8]. For $q = 3$ and $m = 6$, there are 67 equivalence classes for $\alpha = 1$ and 62 classes for $\alpha = 2$. For 1-degenerate QC codes with $m = 7$, there are 48 classes, and the corresponding 1-degenerate QT codes are all QC since m is odd.

The exponential growth in the number of codes which must be examined to find a best rate $1/p$ QT code quickly renders an exhaustive search impractical. As an alternative, heuristic techniques can be used. Although the resulting code is not guaranteed to be the best possible, it can still attain or improve the known bounds. Techniques for heuristic combinatorial optimization include greedy algorithms, genetic algorithms and simulated annealing [10]. To limit the number of potential codes to be examined, the search can be restricted to a subset of the defining polynomials. A greedy search algorithm is used in this paper, similar to that employed in [12].

The Griesmer bound [15] provides a lower bound on the length, n, of a linear code for a given k, d and q,

$$n(k,d) \geq G(k,d) = \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil, \tag{4}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. For the problem considered in this paper, if d is the maximum minimum distance found for an (n,k) code, the code is optimal if $G(k,d+1) > n$.

III. Construction Results

The maximum minimum distances for the ternary QT codes constructed are compiled in Tables I and II. d_{br} denotes the present bounds given in [5]. For $m = 7$, $x^7 - \alpha$ has a degree 1 factor for $\alpha = 1$ and $\alpha = 2$, but the resulting $(7p, 6)$ codes are all QC since m is odd. It is interesting that for $m = 6$, the codes with $\alpha = 1$ (QC codes) establish the larger minimum distance in some cases, while in other cases the best code is achieved with

$\alpha = 2$. For example, with $\alpha = 1$ and $m = 6$, the best QC code found had $d_{min} = 20$, while for $\alpha = 2, d_{min} = 21$ was achieved. This code has generator matrix

$$G = \left[\begin{array}{c|c|c|c|c|c} 100000 & 211000 & 101210 & 221210 & 110210 & 222100 \\ 010000 & 021100 & 010121 & 022121 & 011021 & 022210 \\ 001000 & 002110 & 201012 & 202212 & 201102 & 002221 \\ 000100 & 000211 & 120101 & 120221 & 120110 & 200222 \\ 000010 & 200021 & 212010 & 212022 & 012011 & 120022 \\ 000001 & 220002 & 021201 & 121202 & 201201 & 112002 \end{array}\right]$$

and weight distribution

Weight	0	21	24	27	30
Count	1	240	288	152	48

This code establishes that $d_3(36, 6) = 21$ based on the upper bound given in [5].

The defining polynomials for the QT codes which have established the maximum possible minimum distance are given in Table III. The polynomials are listed with the lowest degree coefficient on the left, i.e., 2021 corresponds to the polynomial $x^3 + 2x^2 + 2$, or $x^3 - x^2 - 1$. Several of the codes with $n \leq 132$ appear in the tables of bounds on maximum minimum distance [5]. The weight distributions of those that have not appeared in [12] or [13] are listed below, along with those for which optimality can be proven by the Griesmer bound. It is expected that many of the other codes will be proven to be optimal once the table of bounds [5] is extended.

The (90,6) QT code with $d_{min} = 57$ establishes that $d_3(90, 6) = 57$ since this attains the upper bound on d_{min} given in [5]. This code has weight distribution

Weight	0	57	60	63	66	72
Count	1	384	144	4	192	4

The (114,6) QT code with $d_{min} = 73$ establishes that $d_3(114, 6) = 73$ since the upper bound given in [5] is 73. This code has weight distribution

Weight	0	73	74	75	76	78	81	82	83	91	92
Count	1	156	264	36	108	36	8	48	48	12	12

The (120,6) QT code with $d_{min} = 78$ establishes that $d_3(120, 6) = 78$ since this attains the upper bound on d_{min} given in [5]. This code has weight distribution

Weight	0	78	81	87	96
Count	1	528	80	96	24

The (174,6) QC code with $d_{min} = 114$ establishes that $d_3(174, 6) = 114$ since

$$G(6, 115) = 175 > 174$$

This code has weight distribution

Weight	0	114	117	120	123	126	132
Count	1	516	100	36	24	16	36

The (246,6) QT code with $d_{min} = 162$ establishes that $d_3(246, 6) = 162$ since

$$G(6, 163) = 248 > 246$$

This code has weight distribution

Weight	0	162	171	180
Count	1	572	132	24

Note that this is a 3 weight code. The (259,6) QC code with $d_{min} = 171$ establishes that $d_3(259, 6) = 171$ since

$$G(6, 172) = 261 > 259$$

This code has weight distribution

Weight	0	171	180	189
Count	1	588	126	14

Note that this is also a 3 weight code.

IV. Summary

The construction of quasi-twisted (QT) codes of dimension 6 over GF(3) has been presented. The new codes include several optimal codes which determine $d_3(n, 6)$ for $n = 36, 90, 114, 120, 174, 246$ and 259. In addition, lower bounds have been established for ternary linear codes of length $130 < n < 260$.

References

[1] R. Hill, "Optimal linear codes," *Cryptography and Coding II*, (C. Michell, Ed.), Oxford University Press, pp. 75-104, 1992.

[2] G.T. Bogdanova and I.G. Boukliev, "New linear codes of dimension 5 over GF(3)," Proc. *Int. Workshop Algebraic and Comb. Coding Theory*, Novgorod, Russia, pp. 41-43, Sept. 1994.

[3] F.R. Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inf. Theory*, vol. 38, pp. 227-246, Mar. 1992.

[4] N.J.A. Sloane, "Tables of lower bounds on dmax(n,k) for linear codes over fields of order 3," to appear in V. Pless, et. al., *Handbook of Coding Theory.*

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

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

[7] V. Chepyzhov, "A Gilbert-Varshamov bound for quasi-twisted codes of rate $1/n$," Proc. *Joint Swedish-Russian*

Int. Workshop Inf. Theory, Mölle, Sweden, pp. 214-218, Aug. 1993.

[8] 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.

[9] E.R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw Hill, 1968.

[10] E.H.L. Aarts and P.J.M. van Laarhoven, "Local search in coding theory," *Discrete Math.* vol. 106/107 pp. 11-18, 1992

[11] T.A. Gulliver, "New optimal ternary linear codes," to appear in *IEEE Trans. Inf. Theory.*

[12] T.A. Gulliver and V.K. Bhargava, "Some best rate $1/p$ and $(p-1)/p$ quasi-cyclic codes over GF(3) and GF(4)," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1369-1374, July 1992.

[13] T.A. Gulliver and V.K. Bhargava, "New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes," to appear in *Designs, Codes and Cryptography.*

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

[15] G. Solomon and J.J. Stiffler, "Algebraically punctured cyclic codes," *Inf. & Contr.*, no. 8, pp. 170-179, 1965.

Table I. Maximum Minimum Distances for $(6p, 6)$ Ternary QT Codes

p	$\alpha=1$ d_{min}	$\alpha=2$ d_{min}	d_{br}	p	$\alpha=1$ d_{min}	$\alpha=2$ d_{min}	d_{br}	p	$\alpha=1$ d_{min}	$\alpha=2$ d_{min}
2	6	6	6	16	60	61	$61-62$	30	117	117
3	9	9	9	17	64	64	$64-66$	31	121	120
4	13	13	13	18	69	69	$69-70$	32	124	124
5	17	16	17	19	72	73	73	33	128	129
6	20	21	21	20	76	78	78	34	132	133
7	24	24	25	21	81	81	81	35	136	136
8	28	28	$29-30$	22	84	84	$84-86$	36	139	141
9	33	34	34	23	89	89	–	37	144	144
10	36	36	$36-37$	24	93	92	–	38	149	148
11	40	40	$41-42$	25	96	97	–	39	153	154
12	45	45	45	26	101	100	–	40	156	157
13	48	48	$49-50$	27	105	106	–	41	161	162
14	52	52	54	28	109	108	–	42	165	164
15	56	57	57	29	114	112	–	43	169	169

Table II. Maximum Minimum Distances for $(7p, 6)$ Ternary QC Codes

p	d_{min}	d_{br}	p	d_{min}	d_{br}	p	d_{min}
2	6	6	14	63	63	26	118
3	11	11	15	66	$66-68$	27	123
4	15	$15-16$	16	72	72	28	127
5	20	$20-21$	17	76	77	29	132
6	24	25	18	80	81	30	136
7	30	30	19	85	–	31	141
8	34	36	20	90	–	32	146
9	39	39	21	94	–	33	150
10	43	$43-44$	22	99	–	34	156
11	48	$48-49$	23	103	–	35	160
12	54	54	24	108	–	36	165
13	57	$57-58$	25	114	–	37	171

Table III. Defining Polynomials for Quasi-Twisted Codes over GF(3)

code	α	$b_i(x)$
(36,6)	2	1, 211, 10121, 22121, 11021, 2221
(90,6)	2	12111, 2211, 1101, 1121, 1001, 1211, 2221, 2111, 22221, 1201, 112121, 2011, 10111, 11021, 11
(114,6)	2	112121, 121, 20111, 10121, 10211, 1001, 2101, 21021, 21, 20221, 20121, 2021, 12121, 2201, 12211, 22121, 20211, 11211, 10221
(120,6)	2	10211, 11, 221, 111211, 111111, 20211, 11121, 11011, 1121, 22211, 121 , 11211, 2201, 21, 1101, 12211, 2121, 21021, 2101, 1201
(174,6)	1	102, 1111, 11111, 112122, 112, 1021, 11021, 10122, 10211, 1, 11212, 11, 11221, 11211, 121, 12221, 11122, 10102, 1212, 1121 10212, 10111, 122, 1101, 1201, 111112, 1222, 12112, 12111
(246,6)	2	10101, 11121, 20111, 22111, 2221, 1111, 1221, 11, 10201, 12121, 2211, 2111, 1201, 2201, 20121, 22121, 1001, 101, 1, 11211 21121, 21111, 211, 21, 221, 11221, 111111, 11011, 1011, 10211, 2101, 1101, 1211, 111221, 21211, 12111, 2021, 22021, 12211 111121, 112121
(259,6)	1	2211, 2001, 202101, 2021022, 21012, 21, 21102, 22221, 212121, 222111, 2202, 221112, 211122, 2212122, 222, 212112, 2022 22011, 21021, 20211, 22212, 221022, 20121, 222102, 2201202, 212022, 21222, 2121, 21111, 212202, 20112, 202212, 222222 22122, 211101, 21201, 221211