Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 62-68*

Computer construction of quasi-twisted two-weight codes

Eric Z. Chen eric.chen@hkr.se
Dept. of Computer Science, Kristianstad University College,
291 88 Kristianstad, SWEDEN

Abstract. A code is said to be two-weight if the non-zero codewords have only two different weights w_1 and w_2. In this paper, it is generalized that a consta-cyclic code of composite length can be put in the quasi-twisted(QT) form. Based on this result, a new computer construction method of QT two-weight codes is presented. A large amount of QT two-weight codes are found, and several new codes are also constructed.

1 Introduction

A linear $[n, k, d]_q$ code is a k-dimensional subspace of an n-dimensional vector space over a finite field GF(q), with minimum distance d between any two codewords. As a generalization to cyclic codes, quasi-twisted (QT) codes have been shown to contain many good linear codes. Many researchers have been using modern computers to search for good QT codes, and many record-breaking codes are found.

A code is said to be two-weight if any non-zero codeword has a weight of w_1 or w_2. Two-weight codes are closely related to strongly regular graphs [5]. This paper is about the construction of two-weight codes.

The rest of the paper is organized as follows. Section 2 presents the introduction to consta-cyclic and quasi-twisted codes. In Section 3, it is shown that a consta-cyclic code of composite length can be put into a quasi-twisted form. In Section 4, a new construction method of QT two-weight codes from consta-cyclic simplex codes is presented, and a large amount of QT two-weight codes are obtained. Several new codes are also constructed.

2 Consta-cyclic codes and quasi-twisted codes

A code is said to be cyclic if every cyclic shift of a codeword is also a codeword. A cyclic code can be described by the polynomial algebra. A cyclic $[n, k, d]_q$ code has a unique generator polynomial $g(x)$ with a degree of $n - k$. All codewords of a cyclic code are multiples of $g(x)$ modulo $x^n - 1$. A linear $[n, k, d]_q$ code is said to be λ-consta-cyclic if there is a non-zero elementλ of GF(q) such that for any codeword $(a_0, a_1, ..., a_{n-1})$, a consta-cyclic shift by one position or

$(\lambda a_{n-1}, a_0, \ldots, a_{n-2})$ is also a codeword [1]. Therefore, the consta-cyclic code is a generalization of the cyclic code, or a cyclic code is a λ-consta-cyclic code with $\lambda = 1$. Similarly, a consta-cyclic code can be defined by a generator polynomial.

A code is said to be quasi-twisted (QT) if a consta-cyclic shift of any codeword by p positions is still a codeword. Thus a consta-cyclic code is a QT code with $p = 1$, and a quasi-cyclic (QC) code is a QT code with $\lambda = 1$. The length n of a QT code is a multiple of p, i.e., $n = mp$. The consta-cyclic matrices are also called twistulant matrices. They are basic components in the generator matrix for a QT code. An $m \times m$ consta-cyclic matrix is defined as

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ \lambda c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\ \lambda c_{m-2} & \lambda c_{m-1} & c_0 & \cdots & c_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda c_1 & \lambda c_2 & \lambda c_3 & \cdots & c_0 \end{bmatrix}, \tag{1}$$

and the algebra of $m \times m$ consta-cyclic matrices over GF(q) is isomorphic to the algebra in the ring $f[x]/(x^m - \lambda$ if C is mapped onto the polynomial formed by the elements of its first row, $c(x) = c_0 + c_1 x + \ldots + c_{m-1}x^{m-1}$, with the least significant coefficient on the left. The polynomial c(x) is also called the defining polynomial of the matrix C. A twistulant matrix is called a circulant matrix if $\lambda = 1$.

The generator matrix of a QT code can be transformed into rows of twistulant matrices by suitable permutation of columns [2]. For example, a 1-generator QT $[mp, k]_q$ code has the following form of the generator matrix [3]:

$$[G_0, G_1, G_2, \ldots, G_{p-1}], \tag{2}$$

where G_i, $i = 0, 1, 2, \ldots, p-1$, are twistulant matrices of order m.

3 Quasi-twisted structure of a consta-cyclic code of composite length

In [4], it was shown that a circulant matrix can be put into a quasi-cyclic (QC) form. A direct generalization can be made to transform a consta-cyclic matrix into a quasi-twisted (QT) form.

Consider an $n \times n$ consta-cyclic matrix C with $n = mr$. Let $c(x)$ be its defining polynomial. We number the rows and columns with $0, 1, 2, \ldots, mr-1$. To obtain a quasi-twisted form of such a consta-cyclic matrix, we do the row and column permutations. If we re-order the rows and columns in the following order:

$0, r, \ldots, (m-1)r, 1, r+1, (m-1)r+1, \ldots, (r-1), r+(r-1), \ldots, (m-1)r+(r-1)$. Then we obtain a matrix that consists of r rows of r twistulant matrices of order m. If we use the defining polynomials to represent the first row of the twistulant matrices, the QT form of the consta-cyclic matrix can be represented by these defining polynomials.

It is well known that for any positive integer $t > 1$ and prime power q, we have a Hamming $[n, n-t, 3]_q$ code, where $n = (q^t - 1)/(q-1)$. Further, if t and $q-1$ are relatively prime, then the Hamming code is equivalent to a cyclic code. The dual code of a Hamming code is called the simplex code. So for any integer $t > 1$ and prime power q, there is a simplex $[(q^t - 1)/(q-1), t, q^{t-1}]_q$ code.

A simplex code can be constructed as a consta-cyclic code [1]. Let $h(x)$ be a primitive polynomial of degree t over GF(q). A λ-consta-cyclic simplex $[(q^t-1)/(q-1), t, q^{t-1}]_q$ code can be defined by the generator polynomial $g(x) = (x^n - \lambda/h(x)$, where $n = (q^t-1)/(q-1)$, and λ is a non-zero element of GF(q) of order $q-1$. It should be noted that a simplex code is an equidistant code, where $q^t - 1$ non-zero codewords have a weight of q^{t-1}. The $q^t - 1$ non-zero codewords are rows given by the consta-cyclic matrix defined by the generator polynomial, and their multiples by non-zero elements of GF(q). If $n = (q^t - 1)/(q-1)$ is not prime, we write $n = mr$. Let $g(x)$ be a generator polynomial of such a λ-consta-cyclic simplex $[(q^t - 1)/(q-1), t, q^{t-1}]_q$ code, and G be the consta-cyclic matrix defined by $g(x)$. Then using the method given, G can be put into quasi-twisted form. It consists of $r \times r$ matrix of consta-cyclic matrices of order m. Therefore, the λ-consta-cyclic simplex $[q^t - 1)/(q-1), t, q^{t-1}]_q$ code is equivalent to a QT $[mr, t, q^{t-1}]_q$ code.

Example: Let $n = 21 = mr = 3 \times 7$, $m = 3$, $r = 7$, and $q = 4$. Let $0, 1, \alpha$, and $\beta = 1+\alpha$ be the elements of GF(4) and $\lambda = \beta$. Then a λ-consta-cyclic matrix defined by $c(x) = 1 + \beta x + \beta x^3 + \beta x^4 + \beta x^5 + \alpha x^6 + x^7 + x^8 + \alpha x^9 + x^{10} + \alpha x^{11} + x^{13} + \alpha x^{15} + \beta x^{16} + x^{17} + x^{18}$ can be constructed. In fact, this polynomial is also a generator polynomial for the consta-cyclic simplex $[21, 3, 16]_4$ code. With the transformation as given in the last section, we obtain a matrix of 7 twistulants of order 3. If we use $a_i(x)$ to denote the defining polynomials for the first row of twistulant matrices, we have $a_1(x) = 1+x$, $a_2(x) = \beta+\alpha x+x^2$, $a_3(x) = \alpha x+\beta x^2$, $a_4(x) = \beta + x + x^2$, $a_5(x) = \beta + \alpha x + x^2$, $a_6(x) = \beta$, and $a_7(x) = \alpha + x$. The matrix A can be specified by the matrix of defining polynomials,

$$A(x) = \begin{bmatrix} a_1(x) & a_2(x) & a_3(x) & \cdots & a_r(x) \\ xa_r(x) & a_1(x) & a_2(x) & \cdots & a_{r-1}(x) \\ xa_{r-1}(x) & xa_r(x) & a_1(x) & \cdots & a_{r-2}(x) \\ \vdots & \vdots & \vdots & \vdots & \\ xa_2(x) & xa_3(x) & xa_4(x) & \cdots & a_1(x) \end{bmatrix}, \qquad (3)$$

where the computation is done with modulo $x^m - \lambda$ and $a_1(x) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ \beta & 0 & 1 \end{bmatrix}$,

$a_2(x) = \begin{bmatrix} \beta & 1 & \alpha \\ 1 & \beta & 1 \\ \beta & 1 & \beta \end{bmatrix}$, $a_3(x) = \begin{bmatrix} 0 & \alpha & \beta \\ \alpha & 0 & \alpha \\ 1 & \alpha & 0 \end{bmatrix}$, $a_4(x) = \begin{bmatrix} \beta & 1 & 1 \\ \beta & \beta & 1 \\ \beta & \beta & \beta \end{bmatrix}$,

$a_5(x) = \begin{bmatrix} \beta & \alpha & 1 \\ \beta & \beta & \alpha \\ 1 & \beta & \beta \end{bmatrix}$, $a_6(x) = \begin{bmatrix} \beta & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \beta \end{bmatrix}$, $a_7(x) = \begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ \beta & 0 & \alpha \end{bmatrix}$.

So after the column permutation, we obtain the equivalent QT simplex $[3 \times 7, 3, 16]_4$ code.

4 Computer construction of quasi-twisted two-weight codes

A linear code is called projective if any two of its coordinates are linearly independent, or in other words, if the minimum distance of its dual code is at least three. A code is said to be two-weight if any non-zero codeword has a weight of w_1 or w_2, where $w_1 \neq w_2$. We denote a two weight code by $[n, k; w_1, w_2]_q$ code.

In [5], Calderbank and Kantor presented many known families of two-weight codes. An online database of two-weight codes is also available [6].In [7], a special family of two-weight codes, named SU2, was studied and an explicit construction of the codes was given. They are 2-generator quasi-twisted codes. Quasi-cyclic two-weight codes can also be constructed from irreducible cyclic codes [8]. Gulliver [9, 10] presented 3 new quasi-cyclic two-weight codes when he made computer searches for good QT codes. Recently, Kohnert [11] has presented a construction of new two-weight codes with prescribed groups of automorphisms. Next, we present a construction based on QT structure of a simplex code.

Let $g(x)$ be the generator polynomial of a consta-cyclic simplex $[(q^k - 1/(q - 1), k, q^{k-1}]_q$ code of composite length, and G be the consta-cyclic matrix defined by its generator polynomial $g(x)$. Let $n = (q^k - 1)/(q - 1) = mr$. Using the method given above, we can put G into r rows of r twistulant matrices of order m. Let $a_i(x)$ be r defining polynomials for the first row of the twistulant matrices, $i = 1, 2, \ldots, r$. Then we get a matrix of defining polynomials as given in (4). Let d_i be the weights of the defining polynomials $a_i(x)$, $i = 1, 2, \ldots, r$. We denote W the weight matrix corresponding to the weights of the defining polynomials of A(x). Based on the structure of A(x), the i-th row of W is the cyclic shift by one position of the (i-1)-th row, $i = 2, 3, ..., r$.

Example(continued) By computing the weights of defining polynomials in the first row of A(x), we obtain the weight matrix W for A(x). It is a cyclic

matrix.

$$W = \begin{bmatrix} 2 & 3 & 2 & 3 & 3 & 1 & 2 \\ 2 & 2 & 3 & 2 & 3 & 3 & 1 \\ 1 & 2 & 2 & 3 & 2 & 3 & 3 \\ 3 & 1 & 2 & 2 & 3 & 2 & 3 \\ 3 & 3 & 1 & 2 & 2 & 3 & 2 \\ 2 & 3 & 3 & 1 & 2 & 2 & 3 \\ 3 & 2 & 3 & 3 & 1 & 2 & 2 \end{bmatrix},$$

It is obvious that the weight matrix has the following properties: (1) The weight matrix is cyclic. Therefore only r elements of the matrix are needed in memory. Other elements of the matrix can be obtained from these r elements. So space is not a computer problem. (2) The sum of weights in any row is $d = q^{t-1}$, the weight of the non-zero codewords of the simplex code.

Computer construction: For the given weight matrix W, to search for a QT two-weight $[mp, k, d]_q$ code, we need to find p columns of W, such that the row sums of the selected columns can only be of two non-zero values w_1 or w_2. If columns $c_1, c_2, \ldots, c_p$ produce the row sums of two values, then the complement columns (all other columns than columns $c_1, c_2, \ldots, c_p$) produce also the row sums of two values, since the sum of any row of W has the same value. Therefore, among r columns, it is sufficient to search for QT two-weight $[mp, k, d]_q$ codes with $p \leq \lfloor r/2 \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. When the columns are found, the corresponding columns in the defining polynomial matrix give the defining polynomials of the QT two-weight code. The procedure given in [4] can be used to decide if the code is a 1-generator, or 2-generator, or g-generator QT code.

Comparison with computer construction for QT codes: The computer construction presented above is similar to the ones used by many researchers for searching good QT codes [9, 10]. But with the method given in this paper, a weight matrix can be computed directly from a generator polynomial for a consta-cyclic simplex code of composite length, and only one row of the matrix is required to be in memory. Also, it is sufficient to search for two-weight codes with $p \leq \lfloor r/2 \rfloor$ due to the complement relationship. So our method is better both in space and time requirement.

Results: For small and reasonable value of r, an exhaustive search can be used. For large r, the exhaustive search is not possible, so a limited search is used. We set an iteration limit or presume some initial columns in the limited search. Extensive computer search has been made and a large amount of QT two-weight codes have been found. Although many codes found have the same parameters as known ones, they are constructed in the quasi-twisted form, and

we do not know if they are equivalent to the known codes or not. Due to space limit, only selected results are given in Table I. More results can be obtained from the author. It should be noted that all SU2 family of two-weight codes are found, and they are not listed in the tables. The original sources of known codes can be found by looking them up in the online database [6].

Example: (continued) The weight matrix from the cosnta-cyclic simplex $[21, 3, 16]_4$code is given above. The columns 1, 2, 4 of W produce the row sums of 8, 6, 6, 6, 8, 6, 8, respectively. So these row sums are of values 6 and 8. Therefore, columns 1, 2, and 4 define a QT two-weight $[9, 3; 6, 8]_4$ code. The complement columns are columns 3, 5, 6 and 7. The row sums are 8, 10, 10, 10, 8, 10, 8. That is, the row sums are of values 8 and 10. They define a QT two-weight $[12, 3; 8, 10]_4$code. Their generator matrices are given by the corresponding columns in A, and can be found to be as follows (by using the method given in [4]):

$$G = (a_1(x); a_2(x); a_4(x)) = \left[\begin{array}{ccc|ccc|cc} 1 & 1 & 0 & \beta & 1 & \alpha & \beta & 1 & 1 \\ 0 & 1 & 1 & 1 & \beta & 1 & \beta & \beta & 1 \\ \beta & 0 & 1 & \beta & 1 & \beta & \beta & \beta & \beta \end{array}\right],$$

$$G = (a_3(x); a_5(x); a_6(x); a_7(x)) = \left[\begin{array}{ccc|ccc|ccc|ccc} 0 & \alpha & \beta & \beta & \alpha & 1 & \beta & 0 & 0 & \alpha & 1 & 0 \\ \alpha & 0 & \beta & \beta & \alpha & 1 & 0 & \beta & 0 & 0 & \alpha & 1 \\ 1 & \alpha & 0 & 1 & \beta & \beta & 0 & 0 & \beta & \beta & 0 & \alpha \end{array}\right].$$

Table I: q-ary QT two-weight $[mp, k]$ codes

q	k	m	p	w_1, w_2	Note
2	12	3796	2	5022, 5103	new
4	6	39	10	288, 304	new
			15	432, 448	new
			20	576,59	new
			25	720,74	new
8	4	13	3	32, 36	new
			42	476, 480	new
9	4	41	7	215, 225	new
			13	504, 513	new
13	4	119	5	546, 559	new
			15	1638, 1651	new

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*, Revised 1984 Edition, Aegean Park Press, 1984.

[2] C. L. Chen, W. W. Peterson, Some results on quasi-cyclic codes, *Info. Contr.* 15, 1969, 407-423.

[3] N. Aydin, I. Siap, D. Ray-Chaudhury, The structure of 1-generator quasi-twisted codes and new linear codes, *Des., Codes, Crypt.* 24, 2001, 313-326.

[4] E. Z. Chen, Quasi-cyclic codes derived from cyclic codes, *Int. Symp. Inform. Theory Appl. (ISITA2004)*, Parma, Italy, Oct. 10-13, 2004, 162-165.

[5] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* 18, 1986, 97-122.

[6] E. Z. Chen, Web database of two-weight codes, [online], http://moodle.tec.hkr.se/ chen/research/2-weight-codes/search.php

[7] E. Z. Chen, An explicit construction of 2-generator quasi-twisted codes", *IEEE Trans. Inform. Theory* 54, 2008, 5770-5773.

[8] E. Z. Chen, Constructions of quasi-cyclic two-weigh codes, *Proc. Tenth Intern. Workshop ACCT*, Zvenigorod, Russia, Sept. 2006, 56-59.

[9] T. A. Gulliver, Two new optimal ternary two-weight codes and strongly regular graphs, *Discr. Math.* 149, 1996, 83-92.

[10] T. A. Gulliver, A new two-weight code and strongly regular graph, *Appl. Math. Lett.* 9, 1996, 17-20.

[11] A. Kohnert, Constructing two-weight codes with prescribed groups of automorphisms, to appear in *Discr. Appl. Math.*