New Construction of 2-Generator Quasi-Twisted Codes

Eric Z. Chen

Abstract— Quasi-twisted (QT) codes are a generalization of quasi-cyclic (QC) codes. Based on consta-cyclic simplex codes, a new explicit construction of a family of 2-generator quasi-twisted (QT) two-weight codes is presented. It is also shown that many codes in the family meet the Griesmer bound and therefore are length-optimal. New distance-optimal binary QC [195, 8, 96], [210, 8, 104] and [240, 8, 120] codes, and good ternary QC [208, 6, 135] and [221, 6, 144] codes are also obtained by the construction.

Index Terms—linear codes, optimal codes, quasi-cyclic codes, quasi-twisted codes, simplex codes

I. INTRODUCTION

As a generalization to cyclic codes, quasi-cyclic (QC) codes and quasi-twisted (QT) codes have been shown to contain many good linear codes. Many researchers have been using modern computers to search for good QC or QT codes, and many record-breaking codes are found [1]–[12]. The problem with this method is that it becomes intractable when the dimension and the length of the code become large. Unfortunately, very little is known on explicit constructions of good QC or QT codes. For 2-generator QC or QT codes, even fewer results are known [13], [14].

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 it has only two non-zero weights. Projective two-weight codes are closely related to strongly regular graphs [15].

In this paper, a new explicit construction of a family of 2-generator QT two-weight codes is presented. It is the first time that a family of 2-generator QT codes is constructed systematically. It is also shown that many codes of this family are good and optimal. Examples are given to show the construction and the modular structure of the codes.

II. QUASI-TWISTED CODES AND TWO-WEIGHT CODES

A. Consta-Cyclic Codes

The code discussed in the following sections is linear. A q-ary linear code is a k-dimensional subspace of an n-dimensional vector space over the finite field Fq, with minimum distance d between any two codewords. We denote a q-ary code as an [n, k, d]q code, or a binary [n, k, d] code if q = 2. A linear [n, k, d]q code is said to be λ-consta-cyclic if there is a non-zero element λ of Fq such that for any
codeword \((a_0, a_1, \ldots, a_{n-1})\), a consta-cyclic shift by one position or \((\lambda a_{n-1}, a_0, \ldots, a_{n-2})\) is also a codeword [16]. Therefore, the consta-cyclic code is a generalization of the cyclic code, and a cyclic code is a λ-consta-cyclic code with \(\lambda = 1\). A consta-cyclic code can be defined by a generator polynomial.

B. Hamming Codes and Simplex Codes

Hamming codes are a family of linear single error correcting codes. 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 \([t(q^t-1)/(q-1), t, q^t-1]q\) code. It should be noted that a simplex code is an equidistance code, where \(q^t-1\) non-zero codewords have a weight of \(q^t-1\). Let h(x) be a primitive polynomial of degree t over Fq. A \(\lambda\)-consta-cyclic simplex \([t(q^t-1)/(q-1), t, q^t-1]q\) code can be defined by the generator polynomial \(g(x) = (x^t-\lambda^t)h(x)\), where \(n = (q^t-1)/(q-1)\) and \(\lambda\) has order of \(q-1\) [16]. Further, a simplex code is equivalent to a cyclic code if t and \(q-1\) are relatively prime.

C. Quasi-Twisted Codes

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 \(p\), or \(n = pm\). 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

\[
C = \begin{bmatrix}
  c_0 & c_1 & c_2 & \cdots & c_m-1 \\
  \lambda c_{m-1} & c_0 & c_1 & \cdots & c_{m-2} \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  \vdots & \vdots & \vdots & \ddots & c_0 \\
  \lambda c_1 & \lambda c_2 & \lambda c_3 & \cdots & c_0
\end{bmatrix},
\]

and the algebra of \(m \times m\) consta-cyclic matrices over Fq is isomorphic to the algebra in the ring \(\mathbb{F}_q[x]/(x^m-\lambda)\) 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

Eric Z. Chen is with Dept. of Computer Science, Kristianstad University, 291 88 Kristianstad, Sweden (eric.chen@hkr.se).
columns. So a 1-generator QT code has the following form of the generator matrix [17]:

\[ G = \begin{bmatrix} G_0 & G_1 & \cdots & G_{p-1} \end{bmatrix}, \]

where \( G_i \), for \( i = 0, 1, \ldots, p-1 \), are twistulant matrices of order \( m \).

A 2-generator QT code has generator matrix of the following form:

\[ G = \begin{bmatrix} G_{00} & G_{01} & \cdots & G_{0,p-1} \\ G_{10} & G_{11} & \cdots & G_{1,p-1} \end{bmatrix}, \]

where \( G_{ij} \) are twistulant matrices, for \( i = 0, 1, \) and \( j = 0, 1, \ldots, p-1 \).

Very little on 2-generator QT codes is known in the literature. Two 2-generator QC codes were given in [13], while a construction method for 2-generator QC codes was presented in [14]. In both cases, the codes were constructed by the help of modern computers. In the following section, we will present an explicit construction of a family of 2-generator QT codes, that also are two-weight codes, and we will prove that for many parameters they are good or optimal.

D. Two-Weight Codes

Let \( w_1 \) and \( w_2 \) be the two non-zero weights of a two-weight code, where \( w_1 \neq w_2 \). We denote a projective \( q \)-ary linear two weight code as an \([n, k; w_1, w_2]_q \) code. There is an online database of two-weight codes [20]. In the survey paper [15], Calderbank and Kantor listed many known families of projective two-weight codes. Among those families, there is a family of two-weight \([n, k; w_1, w_2]_q \) codes, noted by SU2. For any prime power \( q \), positive integers \( t > 1 \) and \( i \), it has the following parameters:

- Block length: \( n = \left(\frac{qt-1}{q-1}\right) \cdot t \cdot q^{t-1} \)
- Dimension: \( k = 2t \)
- Weights: \( w_1 = (i-1)q^{t-1}, w_2 = iq^{t-1} \), where \( 2 \leq i \leq q \).

No explicit construction of the code is known and studied in the literature, and very little is known about its structure and performance.

III. 2-GENERATOR QUASI-TWISTED TWO-WEIGHT CODES

A. Explicit Construction

For any integer \( t > 1 \) and prime power \( q \), a \( \lambda \)-consta-cyclic simplex \([\lambda, q^{t-1}]_q \) can be constructed. Let \( g(x) \) be the generator polynomial for the \( \lambda \)-consta-cyclic simplex code. Let \( a_0, a_1, \ldots, a_{q-1} \) be \( q-1 \) non-zero elements of \( F_q \) and \( m = (q-1)/\lambda \). Any codeword of the \( \lambda \)-consta-cyclic simplex \([\lambda, q^{t-1}]_q \) can be expressed by a polynomial \( g_i(x) = a_i x^j g(x) \), with the computation modulo \( x^{m-\lambda} \), where \( i = 1, 2, \ldots, q-1 \), and \( j = 0, 1, \ldots, m-1 \). Let \( G_i \) be the twistulant matrix defined by the generator polynomial \( g(x) \), and \( G_{ij} \) be the twistulant matrix defined by \( g_j(x) \). So totally, we obtain \( q^{t-1} \) twistulant matrices. We construct a generator matrix of a 2-generator QT code as follows:

\[ G = \begin{bmatrix} G_0 & G_1 & \cdots & G_{p-1} \\ 0 & G_{1,0} & \cdots & G_{1,p-1} \end{bmatrix} = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}, \]

where \( G_{ij} \) are \( p-1 \) different twistulant matrices from \( q^{t-1} \) twistulant matrices defined above, \( G_1 \) and \( G_2 \) are the first and second row of the twistulant matrices of \( G \). Then we have following result.

Theorem 1: For any positive integer \( t > 1 \), and prime power \( q \), the generator matrix given in (4) defines a 2-generator QT two-weight \([pm, 2t; (p-1)q^{t-1}, pq^{t-1}]_q \) code, where \( m = \left(\frac{(q-1)}{(q-1)}(q-t)\right) p = 2, 3, \ldots, q \).

Proof: Let \( C_1 \) be the sub-code defined by \( G_1 \), and \( C_2 \) be the sub-code defined by \( G_2 \). So \( C_1 \) consists of codewords that just repeat the codewords of the consta-cyclic simplex \([m, t, q^{t-1}]_q \) code by \( p \) times. Therefore, \( C_1 \) is also a consta-cyclic code with a distance of \( pq^{t-1} \). Similarly, \( C_2 \) is also such a consta-cyclic code with a distance of \( p(q-1)q^{t-1} \), since its codeword consists of first \( m \) zeros, followed by \( (p-1) \) different codewords of the consta-cyclic simplex \([m, t, q^{t-1}]_q \) code. Based on the consta-cyclic property of the simplex code and the generator matrix structure of (4), the sum of non-zero codewords from \( C_1 \) and \( C_2 \) has the same codeword from the consta-cyclic simplex \([m, t, q^{t-1}]_q \) code or not. Therefore, any non-zero codeword of the 2-generator QC code defined by (4) has a weight \( w_1 = (p-1)q^{t-1} \) or \( w_2 = pq^{t-1} \). This proves Theorem 1.

Q.E.D.

Theorem 1 provides the complete solution to this family of two-weight codes. The results presented in [21] are two special cases. We state them as corollaries. When \( q = 2 \), the binary simplex \([2t-1, t, 2t-1]_q \) code is cyclic. So the constructed two-weight code is quasi-cyclic.

Corollary 2: Let \( q = 2 \). For any positive integer \( t > 1 \), the generator matrix (4) defines a 2-generator QC two-weight \([p(2t-1), 2t; (p-1)^{-1}2^{t-1}, p^22^{t-1}]_q \) code, where \( p = 2, 3, \ldots, 2 \).

If \( t \) and \( q-1 \) are relatively prime, the simplex \([q^{t-1}]_q \) code is also a cyclic code, and thus we have the following result:

Corollary 3: For any positive integer \( t > 1 \), and prime power \( q \). If \( t \) and \( q-1 \) are relatively prime, the generator matrix (4) defines a 2-generator QC two-weight \([pm, 2t; (p-1)q^{t-1}, pq^{t-1}]_q \) code, where \( m = (q-1)(q-1) \) and \( p = 2, 3, \ldots, q \).

B. Examples

Example 1: Let \( q = 2 \) and \( t = 3 \). So we have \( x^7 - 1 = (x^3 + x + 1)(x^2 + x + 1) \). So a binary cyclic simplex \([7, 3, 4] \) code can be defined by \( g(x) = x^4 + x^2 + x + 1 \). Let \( G_1 \) be the circulant matrix defined by the generator polynomial \( g(x) \), and \( G_{1,j} \) be the circulant matrices defined by \( g_j(x) \), where \( j = 0, 1, \ldots, 6 \). Then the following generator matrix defines a binary 2-generator QC two-weight code [56, 6; 28, 32] code:

\[ G = \begin{bmatrix} G_3 & G_3 & G_3 & G_3 & G_3 & G_3 & G_3 \\ 0 & G_{1,0} & G_{1,1} & G_{1,2} & G_{1,3} & G_{1,4} & G_{1,5} \end{bmatrix}, \]

where \( G_{ij} \) are \( p-1 \) different twistulant matrices from \( q^{t-1} \) twistulant matrices defined above, \( G_1 \) and \( G_2 \) are the first and second row of the twistulant matrices of \( G \). Then we have following result.

Theorem 1: For any positive integer \( t > 1 \), and prime power \( q \), the generator matrix given in (4) defines a 2-generator QT two-weight \([pm, 2t; (p-1)q^{t-1}, pq^{t-1}]_q \) code, where \( m = \left(\frac{(q-1)}{(q-1)}(q-t)\right) p = 2, 3, \ldots, q \).

Proof: Let \( C_1 \) be the sub-code defined by \( G_1 \), and \( C_2 \) be the sub-code defined by \( G_2 \). So \( C_1 \) consists of codewords that just repeat the codewords of the consta-cyclic simplex \([m, t, q^{t-1}]_q \) code by \( p \) times. Therefore, \( C_1 \) is also a consta-cyclic code with a distance of \( pq^{t-1} \). Similarly, \( C_2 \) is also such a consta-cyclic code with a distance of \( p(q-1)q^{t-1} \), since its codeword consists of first \( m \) zeros, followed by \( (p-1) \) different codewords of the consta-cyclic simplex \([m, t, q^{t-1}]_q \) code. Based on the consta-cyclic property of the simplex code and the generator matrix structure of (4), the sum of non-zero codewords from \( C_1 \) and \( C_2 \) has the same codeword from the consta-cyclic simplex \([m, t, q^{t-1}]_q \) code or not. Therefore, any non-zero codeword of the 2-generator QC code defined by (4) has a weight \( w_1 = (p-1)q^{t-1} \) or \( w_2 = pq^{t-1} \). This proves Theorem 1.

Q.E.D.
\(x^5 + x^4 + x^3 + x^2 + 1\) defines a cyclic simplex \([13, 3, 9]\) code. So a series of 2-generator QC two-weight \([15p, 6; 9(p-1), 3p]\) codes can be constructed, with \(p = 2, 3, \ldots, 27\).

Example 3: Let \(q = 3\), and \(t = 2\). So \(m = 4, q - 1 = 2,\) and \(\lambda = 2\). Since \(t\) and \(q - 1\) are not relatively prime, we have a 2-consta-cyclic \([4, 2, 3]\) code. One primitive polynomial of degree 2 over \(F_3\) is \(h(x) = x^2 - x - 1\). So the corresponding generator polynomial for this 2-consta-cyclic code is \(g(x) = (x^3 - 2)/h(x) = x^2 + x - 1\). Let \(a_1 = 1, a_2 = 2\). Let \(G_2\) be the twistulant matrix defined by \(g(x)\), and \(G_4\) be the twistulant matrices defined by \(a_i x^j g(x)\), for \(i = 1, 2,\) and \(j = 0, 1, 2,\) and 3. With Theorem 1, a series of 2-generator QT two-weight \([4p, 4; 3(p-1), 3p]\) codes can be constructed for \(p = 2, 3, \ldots, 9\).

Let \(p = q^i\). Then a simplex code with dimension \(2t\) can be constructed in a 2-generator QT form:

Theorem 4: For any prime power \(q\), integer \(t > 1\). Let \(p = q^i\) and \(m = (q^i - 1)/(q - 1)\). The following generator matrix defines a 2-generator QT simplex \([(q^i - 1)/(q - 1) - (p + 1)m, 2t, q^{i-1}\)] codes:

\[
G = \begin{bmatrix}
G_t & G_{t-1} & \cdots & G_1 & 0 \\
0 & G_{t+1} & \cdots & G_{t+p-1} & G_j \\
\end{bmatrix}
\]

Similar to the proof of Theorem 1, this theorem can be proved. So it is not omitted.

As the given examples show that many SU2 codes are good or distance-optimal. The following theorem tells how good the codes are in general. For integers \(t > 1, j = 1, 2, \ldots, t,\) and \(i = 1, 2, \ldots, q^{i-1}\), we define a function called gap as follows:

\[
gap(i,t,q) = \sum_{j=1}^{i} \left( \frac{1}{q^j} - 1 \right).
\]

**IV. GOOD AND OPTIMAL CODES**

**A. Distance-Optimal Codes**

A linear \([n, k, d]\) code is distance-optimal or d-optimal if its minimum distance cannot be improved, i.e., if there does not exist an \([n, k, d + 1]\) code. For given \(n, k\) and \(q\), there is an online database on best-known binary QC codes [19]. Among these codes, \([221, 6; 144, 153]\) codes can be obtained and they reach the Griesmer bound with a gap given by \(\gap(i, t, q)\).

**Theorem 5:** For prime power \(q\), integer \(t > 1\). Let \(i, r, \) and \(p\) be integers such that \(i = 1, 2, \ldots, t, r = 1, 2, \ldots, q,\) and \(p = q^i - iq + r + 1\). The 2-generator QT \([p(q^i - 1)/(q - 1), 2t, (p-1)q^{i-1}\)] code generated by the generator matrix given in (4) and (6) meets the Griesmer bound with a gap given by \(\gap(i, t, q)\).

**B. Length-Optimal Codes**

A linear \([n, k, d]\) code is length-optimal or n-optimal if its block length \(n\) cannot be improved, i.e., if there does not exist an \([n-1, k, d]\) code. For an \([n, k, d]\) code, the block length \(n\) is ruled by Griesmer bound [16]:

\[
n \geq \sum_{j=0}^{k-1} \frac{d}{q^j},
\]

where \([x]\) denotes the smallest integer greater than or equal to \(x\).
calculated results on the codes obtained for $p = 17, 18, \ldots, 28$. It shows that the code becomes better when $p$ increases. In the table, $gb$ denotes the Griesmer bound on the length. But maximum $p$ for a 2-generator QT two-weight code in the family is $q^t$, and when $p = q^t+1$, a 2-generator QT simplex code is obtained.

### Table I

**EXAMPLE OF CODES**

| $p$ | $d$ | $n$ | $gb$ | gap | $i$ | $R$ | $q$ |
|-----|-----|-----|------|-----|-----|-----|-----|
| 17  | 144 | 221 | 217  | 4   | 4   | 1   | 3   |
| 18  | 153 | 234 | 230  | 4   | 4   | 2   | 3   |
| 19  | 162 | 247 | 243  | 4   | 4   | 3   | 3   |
| 20  | 171 | 260 | 258  | 2   | 3   | 1   | 3   |
| 21  | 180 | 273 | 271  | 2   | 3   | 2   | 3   |
| 22  | 189 | 286 | 284  | 2   | 3   | 3   | 3   |
| 23  | 198 | 299 | 298  | 1   | 2   | 1   | 3   |
| 24  | 207 | 312 | 311  | 1   | 2   | 2   | 3   |
| 25  | 216 | 325 | 324  | 1   | 2   | 3   | 3   |
| 26  | 225 | 338 | 338  | 0   | 1   | 1   | 3   |
| 27  | 234 | 351 | 351  | 0   | 1   | 2   | 3   |
| 28  | 243 | 364 | 364  | 0   | 1   | 3   | 3   |

### REFERENCES

[1] C. L. Chen and W.W. Peterson, “Some results on quasi-cyclic codes”, Inform. Contr., vol. 15, pp.407–423, 1969.

[2] E. J. Weldon, Jr., “Long quasi-cyclic codes are good”, IEEE Trans. Inform. Theory, vol.13, p.130, Jan. 1970.

[3] T. Kasami, “A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2”, IEEE Trans. Inform. Theory, vol. IT-20, p.679, 1974.

[4] San Ling and Patrick Solé, “Good self-dual quasi-cyclic codes exist”, IEEE Trans. Inform. Theory, vol.39, pp.1052–1053, 2003.

[5] H.C.A. van Tilborg, "On quasi-cyclic codes with rate 1/m", IEEE Trans. Inform. Theory, vol. IT-24, pp.628–629, Sept. 1978.

[6] T.A. Gulliver and V.K. Bhargava, "Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes", IEEE Trans. Inform. Theory, vol. IT-37, pp.552–555, May 1991.

[7] E. Z. Chen, "Six new binary quasi-cyclic codes", IEEE Trans. Inform. Theory, vol. IT-40, pp.1666–1667, Sept. 1994.

[8] R. N. Daskalov, T. A. Gulliver and E. Metodieva, “New good quasi-cyclic ternary and quaternary linear codes”, IEEE Trans. Inform. Theory, vol. 43, pp.1647–1650, 1997.

[9] P. Heijnen, H. C. A. van Tilborg, T. Verhoeff, and S. Weijs, "Some new binary quasi-cyclic codes", IEEE Trans. Inform. Theory, vol. 44, pp.1994–1996, Sept. 1998.

[10] N. Aydin, I. Siap, and D. Ray-Chaudhury, “The structure of 1-generator quasi-twisted codes and new linear codes”, Design, Codes, and Cryptography, 24, pp.313–326, 2001.

[11] R. Daskalov and P. Hristov, “New quasi-twisted degenerate ternary linear codes”, IEEE Trans. Inform. Theory, vol. 49, pp. 2259–2263, 2003.

[12] R. Daskalov, P. Hristov and E. Metodieva, "New minimum distance bounds for linear codes over GF(5)", Discrete Math., vol. 275, pp. 97–110, 2004.

[13] T. A. Gulliver and V. K. Bhargava, “Two new rate 2/p binary quasi-cyclic codes”, IEEE Trans. Inform. Theory, Vol. 40, pp. 1667–1668, Sept. 1994.

[14] E. Z. Chen, “New quasi-cyclic codes from simplex codes”, IEEE Trans. Inform. Theory, vol. 53, pp. 1193–1196, March 2007.

[15] R. Calderbank and W. M. Kantor, “The geometry of two-weight codes”, Bull. London Math. Soc., vol. 18, pp. 97–122, 1986.

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