On normalized generating sets for generalized quasi-twisted codes over finite fields

Jingjie Lv\textsuperscript{1,a}, Ruihu Li\textsuperscript{1,b}, Youliang Zheng\textsuperscript{1,c}, Yu Yao\textsuperscript{1,d}

\textsuperscript{1}Department of Basic Sciences Air Force Engineering University Xi’an, Shaanxi, 710051, P. R. China
\textsuperscript{a}E-mail: juxianljj@163.com, \textsuperscript{b}Corresponding author’s e-mail: llzsy2015@163.com, 
\textsuperscript{c}E-mail: zxy951783247@163.com, \textsuperscript{d}E-mail: njjbxqyy@163.com

Abstract—In this short correspondence, we firstly determine the normalized generating set for generalized quasi-twisted codes over finite fields. Then we present an algorithm to construct it. As an application, some optimal or the best-known linear codes are derived from generalized quasi-twisted codes by applying our method.

1. INTRODUCTION
In 1948, a seminal paper “a mathematical theory of communication” has been presented by Claude Shannon. This paper shown that, even in a noisy channel, reliable communication can be achieved at any rate below the channel capacity, which marked the birth of error-correcting codes. Nowadays, error-correcting codes have found wide applications in areas of communication systems, storage technology, compact disc players and so on.

The design of good codes, from both the theoretical and practical aspect, is a very vital problem in coding theory. Generalized quasi-twisted (GQT) codes are generalizations of quasi-twisted (QT) codes, which have been investigated by [1-3]. QT codes form an important class of linear codes, which can be viewed as the generalization of quasi-cyclic codes (QC) codes. The motivation of researching QC and QT codes includes that they have good algebra structures and they can produce many breakers in short lengths [1,4]. Moreover, they are closely related to convolutional codes [5,6]. Compared to QT codes, an advantage of GQT code is that one can construct GQT codes of any length. Further, we can construct GQT codes having dimensions larger than those for the QT codes of the same length.

Recently, there were many papers on the relevant questions. In [7], Esmaeili and Yari studied the structural properties and codes construction of GQC code over finite fields. They utilized the Chinese reminder theorem to characterize multi-generator GQC codes in details. However, they haven’t given the concrete generators’ form of GQC codes. In [8], Borges et al. determined the structure of $Z_2$-double cyclic codes and gave the generator polynomials of these codes, which were the specific cases of GQT codes over $Z_2$. Then, Bae et al. [9] gave the structure of GQC codes over $Z_2$ and constructed the normalized generating sets, which were generalizations of $Z_2$-double cyclic codes. At the last of the paper, they have presented an open question about constructing some binary good GQC codes by the normalized generating sets. It is well known that GQT codes are generalizations of GQC codes.
We prove that GQT codes over finite fields also have the normalized generating sets, and we construct some good GQT codes by the normalized generating sets.

This paper is organized as follows. In Section II, we introduce some preliminaries notations and definitions. Section III determines the normalized generating set for GQT and presents an algorithm to construct it. In Section IV, we construct some optimal or the best-known GQT codes. Section V concludes the paper.

2. Preliminaries

Let \( q \) be a finite field and \( \mathbb{F}_q \) be the unit group of \( q \), where \( q \) is a power of a prime. Let \( * \) be positive integers for \( 1 \leq i \leq \lambda \). Let \( \mathbb{C} \) be a linear code of length \( n = \eta + \rho_1 + \cdots + \rho_l \). If \( 1,0,1,1,0,1,2,1,1,0,2,1 \in \mathbb{C} \), then \( \mathbb{C} \) is called a \( \lambda \)-generalized quasi-twisted (GQT) code of length \( n \) over \( q \). Note that, if \( \rho_1 = \cdots = \rho_l \), then \( \mathbb{C} \) is a \( \lambda \)-quasi-twisted (QT) code. And if \( \lambda = 1 \), then \( \mathbb{C} \) is a generalized quasi-cyclic (GQC) code.

Let \( \pi_i \) be the \( i \)-th canonical projection of \( \mathbb{C} \), i.e., \( \pi_i(c) = (c_1, c_1, \ldots, c_{\rho_i}, \ldots, c_{\rho_i}) \). Obviously, \( \pi_i(\mathbb{C}) \) is a \( q \)-ary \( \lambda \)-constacyclic code of length \( \rho_i \).

Let \( R = \mathbb{F}_q[x] / (x^\lambda - \lambda) \) and \( R = R_1 \times \cdots \times R_\ell \). Then \( R \) has an \( \mathbb{F}_q[x] \)-module structure given by the multiplication \(*\)** as follows:

\[
\lambda(x) * (c_1(x) \cdots (c_j(x)) \mapsto (\lambda(x)c_1(x) \cdots (\lambda(x)c_j(x)),
\]

where \( \lambda(x) \in \mathbb{F}_q[x] \) and \( c(x) = (c_1(x) \cdots (c_j(x)) \in R \).

Let \( \mathbb{C} \) be a GQT code and we have an isomorphism of \( \mathbb{F}_q \)-modules from \( \mathbb{C} \) to \( R \) by mapping

\[
e = (c_1, c_1, \ldots, c_{\rho_1}, \ldots, c_{\rho_{\ell-1}}, c_{\rho_{\ell}-1}) \in \mathbb{C}
\]

\[
e(x) = (c_1 + \cdots + c_{\rho_i}x^{\rho_i-1} \cdots | c_{\rho_i} + \cdots + c_{\rho_{\ell-1}}x^{\rho_{\ell-1}}).
\]

Therefore, each codeword of GQT code \( \mathbb{C} \) can be related to a polynomial vector in \( R \).

Observe that the shift from (1) to (2) on \( \mathbb{F}_q^\lambda \times \cdots \times \mathbb{F}_q^\lambda \) corresponds to componentwise multiplication by \( x \) in \( R \). Hence, a GQT code \( \mathbb{C} \subset \mathbb{F}_q^\lambda \times \cdots \times \mathbb{F}_q^\lambda \) is an \( \mathbb{F}_q[x] \)-submodule of \( R \). If a GQT code \( \mathbb{C} \) of length \( n = \eta + \rho_1 + \cdots + \rho_l \) over \( \mathbb{F}_q \) has \( \mathbb{C} \) with \( \rho_1 = \cdots = \rho_l \) and \( \mathbb{C} \) has the following form of generator matrix over \( \mathbb{F}_q \) wherein \( B/_{ij} \) is a \( \rho_i \times \rho_j \) circulant matrix for some integer \( t_i \).

\[
G = \begin{pmatrix}
B_{11} & B_{12} & \cdots & B_{1\ell} \\
B_{21} & B_{22} & \cdots & B_{2\ell} \\
\vdots & \vdots & \ddots & \vdots \\
B_{\rho_1,1} & B_{\rho_1,2} & \cdots & B_{\rho_1,\ell}
\end{pmatrix}
\]

3. On Normalized Generating Sets for GQT Codes over Finite Fields

A GQT code \( \mathbb{C} \subset \mathbb{F}_q^\lambda \times \cdots \times \mathbb{F}_q^\lambda \) is an \( \mathbb{F}_q[x] \)-submodule of \( R \) and there exists a generating set \( \{b_1, b_2, \ldots, b_\rho\} \) of \( \mathbb{C} \). In this section, we will show that any generating set of GQT codes can be normalized. Further, by the normalized generating sets, we can construct some GQT codes with good parameters to solve the open question in [9].

**Theorem 1** Let \( \mathbb{C} \) be a GQT code of length \( n = \eta + \rho_1 + \cdots + \rho_l \) over \( \mathbb{F}_q \). Then there is a generating set \( \{a_1, a_2, \ldots, a_\ell\} \) of the form
\[ a_1 = (F_1 | 0 | \cdots | 0), \]
\[ a_2 = (F_2 | F_22 | 0 | \cdots | 0), \]
\[ \vdots \]
\[ a_\ell = (F_\ell | F_\ell_2 | \cdots | F_\ell_\ell) \]
such that \( C = \langle a_1, a_2, \ldots, a_\ell \rangle \), where \( F_\ell \in R_1 \), \( F_\ell_2 \mid x^\ell - \lambda \), \( \langle a_1, a_2, \ldots, a_\ell \rangle = \{ c \in C | \pi(c) = 0 \quad \text{for all} \quad j > k \} \) and \( a_i = 0 \) if \( (x^\ell - \lambda)|F_\ell_\ell \). Such a generating set is called normalized here.

**Proof:** When \( \ell = 1 \), then \( C \) is a \( \lambda \)-constacyclic code. Obviously, the results hold for \( \ell = 1 \). When \( \ell > 1 \), we suppose that \( \ker(\pi|_c) \) is generated by \( a_1, a_2, \ldots, a_\ell \), which satisfy above conditions by mathematical induction. Since \( \pi|_c \) is a \( \lambda \)-constacyclic code in \( R_1 \), let \( F_\ell \) be a generator with codeword minimum degree of \( \pi|_c \). Then \( F_\ell \mid x^\ell - \lambda \) and \( x^\ell - \lambda = \lambda * F_\ell \), where \( \lambda \in R_1 \). Select polynomials \( F_\ell \), \( i = 1, 2, \ldots, \ell - 1 \) and \( a_i = (F_\ell_i | F_\ell_2 | \cdots | F_\ell_\ell) \) is a codeword in \( C \). For any \( c = (c_1(x), c_2(x), \ldots, c_\ell(x)) \in C \), we can find a polynomial \( \lambda(x) \) such that \( c(x) = \lambda(x) F_\ell \). Then we can gain that \( c - \lambda(x) * a_i \in \ker(\pi|_c) \). By mathematical induction, we get the desired results.

**Corollary 2** If a GQT code \( C \) has a normalized generating set as in Theorem 1, then the dimension of \( C \) is

\[ \sum_{i=1}^\ell r_i - \sum_{i=1}^\ell \deg F_\ell_i. \]

Proof: for \( i = 1, 2, \ldots, \ell \), let
\[ S_i = \{ a_i, x^\ast a_i, \ldots, x^\ast \deg F_\ell_i - a_i \}, \]
\[ S = \bigcup_{i=1}^\ell S_i. \]

Then it is easy to see that the set \( S \) generates \( C \) ant the elements in \( S \) are \( F_q \)-linear independent.

By Theorem 1, we give an algorithm to construct a normalized generating set from any generating set of the GQT code \( C \). Suppose that
\[ b_1 = (B_1 | B_2 | \cdots | B_\ell_1), \]
\[ b_2 = (B_2 | B_22 | \cdots | B_\ell_2), \]
\[ \vdots \]
\[ b_m = (B_1 | B_{m2} | \cdots | B_{m\ell}) \]
is a generating set of \( C \).

*step(a):* By Euclidean algorithm, find
\[ F_\ell = \gcd(B_1, B_2, \ldots, B_\ell), \]
we write
\[ F_\ell = A_1 B_1 + A_2 B_2 + \cdots + A_\ell B_\ell + C(x^\ell - \lambda), \]
for \( A_i \in F_q[x] \). If \( x^\ell - \lambda | F_\ell \), then we put \( F_\ell = x^\ell - \lambda \) and
\[ a_i = (0 | \cdots | 0 | x^\ell - \lambda). \]

Otherwise, for \( i < \ell \), let
\[ F_\ell = A_1 B_1 + A_2 B_2 + \cdots + A_\ell B_\ell (\text{mod} \ x^\ell - \lambda). \]

Therefore, we have
\[ a_i = (F_1 | F_2 | \cdots | F_\ell). \]

*step(b):* Let \( A_\ell = \frac{B_\ell}{F_\ell} \). Then
\[ b_{i0} = b_i - \lambda a_i = (B_{i1} | B_{i2} | \cdots | B_{i,\ell-1} | 0). \]

Use the same method in step (a) to get \( a_{i-1} \) from \( b_{i0}, \ldots, b_{m0} \). By this way, we can gain a normalized generating set \( \{ a_1, a_2, \ldots, a_\ell \} \) of \( C \).
4. SOME GOOD GQT CODES

In the section, we will construct some good GQT codes over $\mathbb{F}_q$ by Theorem 1.

**Example 4:** Suppose $\eta=3$, $r_2=9$, $q=3$ and $\lambda=2$. Then we decompose the following polynomials over $\mathbb{F}_3$

\[
x^3 - 2 = (1 + x)^3, \\
x^9 - 2 = (1 + x)^9.
\]

Let $F_{11} = (1 + x)^2 = 1 + 2x + x^2$, $F_{12} = 2 + x + x^2$ and $F_{22} = (1 + x)^2$

$= 1 + 2x + x^2$. Let $C$ be a GQT code with normalized generating sets $a_1 = (1 + 2x + x^2 | 0)$ and $a_2 = (2 + x + x^2 | 1 + 2x + x^2)$.

By the Corollary 3, we have the minimal generating set

\[
S = \{(1 + 2x + x^2 | 0), (2 + x + x^2 | 1 + 2x + x^2), (2 + x + x^2 | x + 2x^2 + x^3)\},
\]

set $(2 + 2x + x^2 | x^2 + 2x^3 + x^4), (1 + 2x + 2x^2 | x^3 + 4x^4 + x^5), (1 + x + 2x^2 | x^4 + x^5)$. Then $C$ has the following generator

\[
x^4 + 2x^5 + x^6), (1 + x + x^2 | x^3 + 2x^4 + x^5), (2 + x + x^2 | x^6 + 2x^7 + x^8)\}.
\]

Let $C$ be a GQT code with normalized generating sets $a_1 = (1 + 2x + x^2 | 0)$ and $a_2 = (2 + x + x^2 | 1 + 2x + x^2)$.

By calculation, we attain that $C$ is a $[12,8,3]$-code over $\mathbb{F}_3$ which is an optimal linear code.

**Example 5:** Suppose $\eta=11$, $r_2=3$, $q=3$ and $\lambda=2$. Decompose the following polynomials over $\mathbb{F}_3$

\[
x^{11} - 2 = (1 + x)(1 + 2x + 2x^2 + 2x^3 + x^5)(1 + 2x^2 + 2x^3 + 2x^4 + x^5), \\
x^3 - 2 = (1 + x)^3.
\]

Let $F_{11} = (1 + x)(1 + 2x^2 + 2x^3 + 2x^4 + x^5) = 1 + x + 2x^2 + x^3 + x^4 + x^6$, $F_{12} = 1 + x^3 + 2x^4 + 2x^5 + 2x^7 + 2x^8 + 2x^9 + 2x^{10}$

and $F_{22} = (1 + x)^2 = 1 + 2x + x^2$. Let $C$ be a GQT code with normalized generating sets $a_1 = (1 + x + 2x^2 + x^3 + x^4 + x^5 | 0)$ and $a_2 = (1 + x + 2x^4 + 2x^5 + 2x^6 + 2x^7 + 2x^8 + 2x^9 + 2x^{10} | 1 + 2x + x^2)$.

By calculation, we attain that $C$ is a $[14,6,6]$-code over $\mathbb{F}_3$ which is an optimal linear code.

**Example 6:** Suppose $\eta=5$, $r_2=25$, $q=7$ and $\lambda=6$. Then we decompose the following polynomials over $\mathbb{F}_7$

\[
x^{25} - 6 = (1 + x)(1 + 6x + x^2 + 6x^3 + x^5), \\
x^{25} - 6 = (1 + x)(1 + x + 5x^2 + x^3 + 3x^4)(1 + 5x + 4x^2 + 5x^3 + x^4)(1 + 6x + x^2 + 6x^3 + x^5).
\]

Let $F_{11} = 0$, $F_{12} = 3 + x$ and $F_{22} = (1 + 2x + 5x^2 + 2x^3 + x^4)(1 + 3x + 3x^2 + 5x^3 + x^4)(1 + 5x + 4x^2 + 5x^3 + x^4)(1 + 6x + x^2 + 6x^3 + x^5) + 3x^3 + x^4).

Let $C$ be a GQT code with normalized generating sets $a_1 = 0$ and $a_2 = (3 + x | 1 + 3x + 5x^2 + 4x^3 + 3x^4 + 4x^5 + 5x^6 + 3x^7 + x^8)$. By calculation, $C$ is a $[30,17,9]$-code over $\mathbb{F}_7$ that is the best-known.
**Example 7:** Suppose $\eta = 5$, $r_2 = 29$, $q = 5$ and $\lambda = 2$. Then we decompose the following polynomials over $\mathbb{F}_7$
\[
x^5 - 2 = (3 + x)^5,
\]
\[
x^{29} - 2 = (1 + x)(4 + 3x + 4x^2 + x^3 + 3x^4 + 3x^5 + 4x^7 + 3x^9 + 2x^{10} + x^{11})\]
Let $F_{11} = 0$, $F_{12} = 3 + 4x + 2x^2 + x^3 + 3x^4$ and
\[
+ x^{12} + 3x^{13} + x^{14}).(4 + 4x + 4x^2 + x^4 + 3x^5 + 3x^6 + 3x^7 + 2x^8 + 3x^9 +
4x^{10} + x^{11} + 4x^{13} + x^{14}).
\]
\[
F_{22} = 4 + 3x + 4x^2 + 3x^4 + 4x^7 + 3x^9 + 2x^{10} + x^{11} + x^{12} + 3x^{13} + x^{14}.\]
Let $C$ be a GQT code with normalized generating sets $a_1 = 0$ and $a_2 = (3 + 4x + 2x^2 + x^3 + 3x^4 | 4 + 3x + 4x^2 + x^4 + 3x^5 + 3x^6 + 3x^7 + 2x^8 + 3x^9 +
2x^{10} + x^{11} + x^{12} + 3x^{13} + x^{14}).$

By calculation, $C$ is a good code over $\mathbb{F}_5$ with parameters $[34,15,12]$.

**5. CONCLUSIONS**
In this paper, we determined the normalized generating sets for GQT codes. Moreover, an algorithm of producing normalized generating sets also has been presented. As an application, some good GQT codes are derived by our construction.

**REFERENCES**
[1] N. Aydin, I. Siap, D. Ray-Chaudhuri, “The Structure of 1-generator quasi-twisted codes and new linear Codes,” Des. Codes Cryptogr, vol. 24, pp. 313-326, 2001.
[2] S. Bae, P. L. Kang, C. J. Li, “On normalized generating sets for GQC codes over $\mathbb{Z}_2$, ” Finite Fields Appl, vol. 45, pp. 285-300, 2017.
[3] J. Borges, C. F. Córdoba, R. T. Valls, $\mathbb{Z}_2$-double cyclic codes, Computer Science, 2014.
[4] W. Bosma, J. Cannon, C. Playoust, “The MAGMA algebra system I: the user language,” J. Symb. Comput. vol. 24, pp. 235-265, 1997.
[5] M. Esmaeili, S. Yari, “Generalized quasi-cyclic codes: structural properties and code construction,” Appl. Algebra Engrg. Comm. Compt, vol. 20, pp. 159-173, 2009.
[6] M. Esmaeili, T.A. Gulliver, N.P. Secord, S.A. Mahmoud, “A link between quasi-cyclic codes and convolutional codes,” IEEE Trans. Inf. Theory, vol. 44, pp. 431-435, 1998.
[7] J. Gao, F. Fu, “Note on quasi-twisted codes and an application,” J. Appl. Math. Comput, vol. 47, pp. 487-506, 2005.
[8] J. Gao, Q. Kong, “One generator $(1+u^r)$-quasistatic code over $\mathbb{F}_2+u\mathbb{F}_2$,” Math. comput, vol. 2, pp. 1-5, 2013.
[9] M. Grassl, Bounds on the minimum distance of linear codes. http://www.codetables.de, 2015.
[10] Y. Jia, “On quasi-twisted codes over finite fields, Finite Fields Appl,” vol. 18, pp. 237-257, 2012.
[11] G. Solomon, H.C.A.V. Tilborg, “A connection between block and convolutional codes,” SIAM J. Appl. Math. vol. 37, pp. 358-369, 1979.