Finite Fields and Their Applications 18 (2012) 237–257

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On quasi-twisted codes over finite fields

Yan Jia

Nanyang Technological University, Division of Mathematical Sciences, SPMS-MAS-03-01, 21 Nanyang Link, Singapore 637371, Singapore

ARTICLE INFO

Article history:
Received 22 February 2011
Revised 29 July 2011
Accepted 1 August 2011
Available online 15 September 2011
Communicated by Simeon Ball

MSC:
94B05
94B15

Keywords:
Quasi-twisted code
Finite field
Generalized discrete Fourier transform
Repeated-root case
Nonrepeated-root case
Construction

ABSTRACT

In coding theory, quasi-twisted (QT) codes form an important class of codes which has been extensively studied. We decompose a QT code to a direct sum of component codes – linear codes over rings. Furthermore, given the decomposition of a QT code, we can describe the decomposition of its dual code. We also use the generalized discrete Fourier transform to give the inverse formula for both the nonrepeated-root and repeated-root cases. Then we produce a formula which can be used to construct a QT code given the component codes.

1. Introduction

Quasi-twisted (QT) codes over finite fields form an important class of block codes that includes cyclic codes, quasi-cyclic codes and constacyclic codes as special cases. In this paper, we investigate issues related to the decomposition and construction of a QT code. The important tool used is the generalized discrete Fourier transform.

Let $\mathbb{F}_q$ denote the finite field of $q = p^m$ elements, where p is a prime and m is a positive integer. Let $\mathscr{C}$ be a linear code of length n over $\mathbb{F}_q$. Let $\lambda \in \mathbb{F}_q^*$ and let l be a positive integer. For each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, if the vector

$$(\lambda c_{n-l}, \lambda c_{n-l+1}, \ldots, \lambda c_{n-1}, c_0, \ldots, c_{n-l-1}) \in \mathscr{C},$$

E-mail address: jiayanmiss@hotmail.com.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.08.001

where the subscripts are taken modulo n, then the code $\mathscr{C}$ is called a (λ, l)-quasi-twisted (QT) code. It is well known that a (λ, l)-QT code of length $n = l\theta$ over $\mathbb{F}_q$ is identified with a $\frac{\mathbb{F}_q[x]}{(x^\theta-\lambda)}$-submodule of $(\frac{\mathbb{F}_q[x]}{(x^\theta-\lambda)})^l$.

First, by decomposing the ring $\mathbb{R}_{\theta,\lambda} := \frac{\mathbb{F}_q[x]}{(x^\theta-\lambda)}$ into a direct sum of coprime component rings, it is shown that a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$ can be decomposed into a direct sum of linear codes $\mathscr{C}_i$ over these component rings.

The decomposition of the ring involves the factorization of the polynomial $x^\theta - \lambda$ over $\mathbb{F}_q$. If $\gcd(\theta, q) = 1$ (nonrepeated-root case), then the polynomial $x^\theta - \lambda$ is factorized into a product of distinct irreducible polynomials. It is shown that if $\gcd(\theta, q) = p^a$ with $a \geqslant 1$ (repeated-root case), then all the irreducible factors of the polynomial $x^\theta - \lambda$ are with multiplicity p^a. In this paper, we allow $a \geqslant 0$ and then both cases are included. When $x^\theta - \lambda = (f_1(x))^{p^a}(f_2(x))^{p^a}\cdots(f_k(x))^{p^a}$, where $f_i(x)$'s are irreducible polynomials over $\mathbb{F}_q$, the ring $\mathbb{R}_{\theta,\lambda}$ is decomposed into a direct sum of the coprime component rings $\mathbb{R}_i := \frac{\mathbb{F}_q[x]}{((f_i(x))^{p^a})}$, $1 \leqslant i \leqslant k$.

Since the dual code $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ of a (λ, l)-QT code $\mathscr{C}$ is a (λ^{-1}, l)-QT code, a natural question that then arises is: given the decomposition of $\mathscr{C}$, what is the decomposition of $\mathscr{C}^{\perp_{\mathbb{F}_q}}$? When $\lambda = \pm 1$, $\mathscr{C}$ and $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ are modules over the same ring $\frac{\mathbb{F}_q[x]}{(x^\theta-\lambda)}$ and hence, only in this case, self-dual QT codes make sense. When $\lambda \neq \pm 1$, $\mathscr{C}$ and $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ are modules over different rings: $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$ respectively. Since the two rings are isomorphic by identifying $x \in \mathbb{R}_{\theta,\lambda}$ with $x^{-1} \in \mathbb{R}_{\theta,\lambda^{-1}}$, we map $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ into the module $\mathbb{R}^l_{\theta,\lambda}$ and get an isomorphic copy of $\mathscr{C}^{\perp_{\mathbb{F}_q}}$. Based on the dual defined over two modules over the same ring, the decomposition of the dual code over $\mathbb{R}_{\theta,\lambda^{-1}}$ is explicitly described. In particular, the decomposition of self-dual QT codes is given.

An important tool to study algebraic codes is the discrete Fourier transform (DFT). When $\gcd(\theta, p) = 1$, i.e., in the nonrepeated-root case, the classical DFT of $c(x) \in \frac{\mathbb{F}_q[x]}{(x^\theta-\lambda)}$ is defined to be a matrix

$$\hat{c} = [\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{\theta-1}],$$

where

$$\hat{c}_i = c\big(\beta\xi^i\big), \quad \text{for } 0 \leqslant i \leqslant \theta - 1,$$

β is a θ-th root of λ,

and ξ is a primitive θ-th root of unity.

It is well known that the DFT is invertible. However, in the repeated-root case, the classical DFT is not applicable. Therefore, we adopt the Hasse derivatives to develop the generalized discrete Fourier transform (GDFT). We also give the inverse formula of the GDFT.

The GDFT also gives an explicit connection between a QT code and its component codes. Therefore, by the inverse formula of the GDFT, we produce a formula to construct a QT code from linear codes over component rings. It is further shown that the computation can be done in the field $\mathbb{F}_q$ instead of the extension fields.

This paper is organized as follows. After a brief introduction of the key notions and notations in Section 2, the decomposition of a (λ, l)-QT code is given in Section 3. Section 4 deals with the decomposition of the dual code of a QT code in two cases: $\lambda = \pm 1$ and $\lambda \neq \pm 1$. In Section 5, the GDFT and the inverse formula are given. After the construction formula is given in Section 6, some examples are shown in Section 7. A summary concludes the paper in Section 8.

2. Preliminaries

Let $\mathbb{F}_q$ denote the finite field of $q = p^m$ elements and let $\mathbb{F}_q^*$ denote $\mathbb{F}_q \setminus \{0\}$, where p is a prime and m is a positive integer. Denote by $\mathbb{F}_q[x]$ the polynomial ring in indeterminate x with coefficients from $\mathbb{F}_q$.

A *linear code* $\mathscr{C}$ of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$. It is known as an $[n,k]_q$ code. The elements of the subspace are the *codewords* of $\mathscr{C}$ and written as row vectors: $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$.

Definition 1. An $[n,k]_q$ code $\mathscr{C}$ is called *cyclic* provided that, for each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also a codeword in $\mathscr{C}$.

Mapping a codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$ to a polynomial $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathbb{F}_q[x]$, a cyclic code $\mathscr{C}$ is an ideal in $\mathbb{F}_q[x]/(x^n - 1)$.

Generalized from cyclic codes, we have the following three classes of codes.

Definition 2. Let $\mathscr{C}$ be a linear code of length n over $\mathbb{F}_q$. Let $\lambda \in \mathbb{F}_q^*$. For each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, if the vector $(\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathscr{C}$, then the code $\mathscr{C}$ is called a λ-constacyclic code and λ is called the constant of $\mathscr{C}$.

By the correspondence between codewords and polynomials, a λ-constacyclic code can be identified with an ideal in $\mathbb{F}_q[x]/(x^n - \lambda)$.

Definition 3. Let $\mathscr{C}$ be a linear code of length n over $\mathbb{F}_q$. For each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, if the vector $(c_{n-l}, c_{n-l+1}, \ldots, c_{n-1}, c_0, \ldots, c_{n-l-1}) \in \mathscr{C}$ where the subscripts are taken modulo n and l is a positive integer, then the code $\mathscr{C}$ is called an l-quasi-cyclic (QC) code and l is called the index of $\mathscr{C}$.

It is easy to check that an l-QC code of length n is also a $\gcd(l,n)$-QC code. Without loss of generality, we therefore assume that the index l always divides the length n. Let $\theta = \frac{n}{l}$. Properly permuting the coordinates of a codeword $(c_0, c_1, \ldots, c_{n-1})$ in the l-QC code to the vector

$$\mathbf{c}' = (c_0, c_l, \ldots, c_{(\theta-1)l}, c_1, c_{l+1}, \ldots, c_{(\theta-1)l+1}, \ldots, c_{l-1}, \ldots, c_{\theta l-1}),$$

we divide $\mathbf{c}'$ to l parts and each part consists of θ consecutive coordinates.

It is observed that each part can be regarded as a codeword in a cyclic code of length θ over $\mathbb{F}_q$. Therefore, representing each part of $\mathbf{c}'$ by a polynomial in $\mathbb{F}_q[x]/(x^\theta - 1)$, the codeword $\mathbf{c}$ is equivalent to the vector in $(\mathbb{F}_q[x]/(x^\theta - 1))^l$:

$$\left(c_0 + c_l x + \cdots + c_{(\theta-1)l}x^{\theta-1}, c_1 + \cdots + c_{(\theta-1)l+1}x^{\theta-1}, \ldots, c_{l-1} + c_{2l-1}x + \cdots + c_{\theta l-1}x^{\theta-1}\right)$$

(see [4]). Then an l-QC code is equivalent to a submodule of $(\mathbb{F}_q[x]/(x^\theta - 1))^l$ over the ring $\mathbb{F}_q[x]/(x^\theta - 1)$.

Definition 4. Let $\mathscr{C}$ be a linear code of length n over $\mathbb{F}_q$. Let $\lambda \in \mathbb{F}_q^*$ and let l be a positive integer. For each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ in $\mathscr{C}$, if the vector

$$(\lambda c_{n-l}, \lambda c_{n-l+1}, \ldots, \lambda c_{n-1}, c_0, \ldots, c_{n-l-1}) \in \mathscr{C},$$

where the subscripts are taken modulo n, then the code $\mathscr{C}$ is called a (λ, l)-quasi-twisted (QT) code.

We define an action $T_{\lambda,l}$ on the codewords as

$$T_{\lambda,l}(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-l}, \lambda c_{n-l+1}, \ldots, \lambda c_{n-1}, c_0, \ldots, c_{n-l-1}).$$

A (λ, l)-QT code is invariant as a set under the action $T_{\lambda,l}$.

It is easy to check that a (λ, l)-QT code of length n is also a $(\lambda, \gcd(l, n))$-QT code (see [1]). Thus we always assume l divides n. Let $\theta = \frac{n}{l}$. When $\lambda = 1$, a (λ, l)-QT code is an l-QC code. When $l = 1$, a (λ, l)-QT code is a λ-constacyclic code. When $\lambda = l = 1$, a (λ, l)-QT code is a cyclic code. From the above discussion about constacyclic codes and QC codes, a (λ, l)-QT code of length n is a submodule of $(\mathbb{F}_q[x]/(x^\theta - \lambda))^l$ over the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$. For convenience, we use the same notation for both the code over $\mathbb{F}_q$ and its corresponding submodule of $(\mathbb{F}_q[x]/(x^\theta - \lambda))^l$ over the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$.

3. Decomposition of QT codes

Let $\mathscr{C}$ be a (λ, l)-QT code of length n over $\mathbb{F}_q$. Recall that $\mathscr{C}$ is a module over the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$. Denote the ring $\mathbb{F}_q[x]/(x^\theta - \lambda)$ by $\mathbb{R}_{\theta,\lambda}$.

In order to know more about the algebraic structure of QT codes, we next focus on the ring $\mathbb{R}_{\theta,\lambda}$.

Let $\theta = p^a\bar{\theta}$, where $\gcd(\bar{\theta}, p) = 1$. Since the map $x \mapsto x^{p^a}$ is a power of the Frobenius automorphism of $\mathbb{F}_q$ defined by $x \mapsto x^p$, it is an automorphism of $\mathbb{F}_q$. Therefore, for any $\lambda \in \mathbb{F}_q^*$, there exists a unique $\bar{\lambda} \in \mathbb{F}_q^*$ such that $\bar{\lambda}^{p^a} = \lambda$. Therefore, we may write

$$x^\theta - \lambda = \left(x^{\bar{\theta}} - \bar{\lambda}\right)^{p^a}.$$

Since $\gcd(\bar{\theta}, p) = 1$, the polynomial $x^{\bar{\theta}} - \bar{\lambda}$ is factorized into distinct irreducible polynomials over $\mathbb{F}_q$ as follows:

$$x^{\bar{\theta}} - \bar{\lambda} = f_1(x) f_2(x) \cdots f_k(x).$$

Therefore, we have

$$x^\theta - \lambda = \left(f_1(x)\right)^{p^a} \left(f_2(x)\right)^{p^a} \cdots \left(f_k(x)\right)^{p^a}. \tag{1}$$

By the Chinese Remainder Theorem, we have the following decomposition:

$$\frac{\mathbb{F}_q[x]}{(x^\theta - \lambda)} \simeq \frac{\mathbb{F}_q[x]}{((f_1(x))^{p^a})} \oplus \frac{\mathbb{F}_q[x]}{((f_2(x))^{p^a})} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{((f_k(x))^{p^a})},$$

$$r(x) \leftrightarrow \left(r(x) + \left(\left(f_1(x)\right)^{p^a}\right), \ldots, r(x) + \left(\left(f_k(x)\right)^{p^a}\right)\right).$$

For convenience, we denote the ring $\frac{\mathbb{F}_q[x]}{((f_i(x))^{p^a})}$ by $\mathbb{R}_i$ for $1 \leqslant i \leqslant k$. It follows that

$$\mathbb{R}_{\theta,\lambda}^l \simeq \bigoplus_{i=1}^{k} \mathbb{R}_i^l. \tag{2}$$

Then we have the following theorem immediately.

Theorem 1. *Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$. Then $\mathscr{C}$ is a linear code over $\mathbb{R}_{\theta,\lambda}$ of length l and it can be decomposed as the direct sum*

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i, \tag{3}$$

where $\mathscr{C}_i$ is a linear code over $\mathbb{R}_i$ of length l for each $1 \leqslant i \leqslant k$.

4. Dual codes of QT codes

In this section, we discuss the dual codes of QT codes. For our purpose, we give the following definition about dual codes.

Definition 5. Let $\mathbf{K}$ be a commutative ring or a finite field and let N be a positive integer. Let

$$\mathbf{u} = (u_0, \ldots, u_{N-1})$$

and

$$\mathbf{v} = (v_0, \ldots, v_{N-1})$$

be two vectors over $\mathbf{K}$. The *inner product* of $\mathbf{u}$ and $\mathbf{v}$ over $\mathbf{K}$ is denoted by

$$\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbf{K}} = \sum_{i=0}^{l-1} u_i v_i.$$

Let $\mathscr{C}$ be a linear code of length N over $\mathbf{K}$, then the dual code of $\mathscr{C}$ (with respect to the inner product over $\mathbf{K}$), denoted by $\mathscr{C}^{\perp_{\mathbf{K}}}$, is defined as

$$\mathscr{C}^{\perp_{\mathbf{K}}} = \left\{ \mathbf{v} \in \mathbf{K}^N \;\middle|\; \langle \mathbf{v}, \mathbf{u} \rangle_{\mathbf{K}} = 0, \text{ for any } \mathbf{u} \in \mathscr{C} \right\}.$$

In particular, if $\mathscr{C} = \mathscr{C}^{\perp_{\mathbf{K}}}$, then $\mathscr{C}$ is a self-dual code over $\mathbf{K}$.

Notice that when $\mathbf{K} = \mathbb{F}_q$, the inner product defined above is exactly the Euclidean inner product.

Recall that the index l always divides the length n for a QT code. The following proposition follows directly from the definition of QT codes.

Proposition 1. *Let $\mathscr{C}$ be a (λ, l)-QT code of length n over $\mathbb{F}_q$ and let $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ be the dual code of $\mathscr{C}$. Then $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ is a (λ^{-1}, l)-QT code of length n over $\mathbb{F}_q$.*

By the above proposition, we know that $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ is a submodule of $\mathbb{R}^l_{\theta,\lambda^{-1}}$ over $\mathbb{R}_{\theta,\lambda^{-1}}$, and hence a linear code over $\mathbb{R}_{\theta,\lambda^{-1}}$.

Notice that a (λ, l)-QT code is an $\mathbb{R}_{\theta,\lambda}$-module while its dual code is an $\mathbb{R}_{\theta,\lambda^{-1}}$-module. However, the two rings $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$ are isomorphic:

$$\mathbb{R}_{\theta,\lambda} \simeq \mathbb{R}_{\theta,\lambda^{-1}},$$
$$x \leftrightarrow x^{-1},$$

where $x^{-1} = \lambda^{-1} x^{\theta-1}$ in the ring $\mathbb{R}_{\theta,\lambda}$ and $x^{-1} = \lambda x^{\theta-1}$ in the ring $\mathbb{R}_{\theta,\lambda^{-1}}$.

By the above isomorphism, we define the map ϕ as follows.

Definition 6. For all $(r_0(x), r_1(x), \ldots, r_{l-1}(x)) \in \mathbb{R}^l_{\theta,\lambda^{-1}}$, we define the map $\phi : \mathbb{R}^l_{\theta,\lambda^{-1}} \to \mathbb{R}^l_{\theta,\lambda}$ with

$$\phi\big(\big(r_0(x), r_1(x), \ldots, r_{l-1}(x)\big)\big) = \big(r_0\big(x^{-1}\big), r_1\big(x^{-1}\big), \ldots, r_{l-1}\big(x^{-1}\big)\big).$$

Obviously, the map ϕ is bijective since it is induced from the isomorphism between $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$. Therefore, it immediately follows that:

Proposition 2. *The map ϕ gives a one-to-one correspondence between the $\mathbb{R}_{\theta,\lambda}$-submodules of $\mathbb{R}^l_{\theta,\lambda}$ and the $\mathbb{R}_{\theta,\lambda^{-1}}$-submodules of $\mathbb{R}^l_{\theta,\lambda^{-1}}$.*

Although the (λ, l)-QT code and its dual code are modules over different rings, by the above proposition, we can consider the image of the dual code of a (λ, l)-QT code under the map ϕ. Then $\phi(\mathscr{C}^{\perp_{\mathbb{F}_q}})$ and $\mathscr{C}$ are modules over the same ring $\mathbb{R}_{\theta,\lambda}$. Similarly, we can also consider the following two modules over $\mathbb{R}_{\theta,\lambda^{-1}}$: $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ and the preimage of $\mathscr{C}$ under the map ϕ.

The following lemma studies the dual with respect to the inner product over $\mathbb{R}_{\theta,\lambda}$.

Lemma 1. *Let $\mathbf{c}$ and $\mathbf{d}$ be any two vectors in $\mathbb{F}_q^n$, where $n = l\theta$. Let the vector $\mathbf{c}(x) \in \mathbb{R}^l_{\theta,\lambda}$ be the polynomial representation corresponding to the vector $\mathbf{c}$ and let the vector $\mathbf{d}(x) \in \mathbb{R}^l_{\theta,\lambda^{-1}}$ be the polynomial representation corresponding to the vector $\mathbf{d}$. Then $\langle \mathbf{c}(x), \phi(\mathbf{d}(x))\rangle_{\mathbb{R}_{\theta,\lambda}} = 0$ if and only if $\langle T^i_{\lambda,l}(\mathbf{c}), \mathbf{d}\rangle_{\mathbb{F}_q} = 0$ for each $0 \leqslant i \leqslant \theta - 1$.*

Proof. Assume that $\langle \mathbf{c}(x), \phi(\mathbf{d}(x))\rangle_{\mathbb{R}_{\theta,\lambda}} = 0$. Then we have

$$\sum_{i=0}^{l-1}\left(\left(\sum_{j=0}^{\theta-1} c_{i+jl}x^j\right)\left(\sum_{k=0}^{\theta-1} d_{i+kl}x^{-k}\right)\right) = 0. \tag{4}$$

Since the above equation is in the ring $\mathbb{R}_{\theta,\lambda}$, the left-hand side can be written as a unique polynomial over $\mathbb{F}_q$ of degree less than θ. Denote by $[x^i]$ the term in x^i in such a unique expression, where $0 \leqslant i \leqslant \theta - 1$.

Since $x^\theta = \lambda$ in the ring $\mathbb{R}_{\theta,\lambda}$, it immediately follows that

$$x^{-j} = \lambda^{-1}x^\theta x^{-j} = \lambda^{-1}x^{\theta-j}, \quad \text{for } 1 \leqslant j \leqslant \theta - 1.$$

Therefore, each term on the left-hand side of (4) is as follows:

$$\begin{aligned}
\big[x^0\big] &= \sum_{i=0}^{l-1}\sum_{j=0}^{\theta-1} c_{i+jl}d_{i+jl} = \sum_{i=0}^{\theta l-1} c_i d_i = \langle \mathbf{c}, \mathbf{d}\rangle_{\mathbb{F}_q},\\
\big[x^k\big] &= \sum_{i=0}^{l-1}\big((c_{i+kl}d_i + \cdots + c_{i+(\theta-1)l}d_{i+(\theta-1-k)l})x^k\\
&\qquad + (c_i d_{i+(\theta-k)l} + \cdots + c_{i+(k-1)l}d_{i+(\theta-1)l})x^{k-\theta}\big)\\
&= \lambda^{-1}\sum_{i=0}^{l-1}(\lambda c_{i+kl}d_i + \cdots + \lambda c_{i+(\theta-1)l}d_{i+(\theta-1-k)l}
\end{aligned}$$

$$+ c_i d_{i+(\theta-k)l} + \cdots + c_{i+(k-1)l} d_{i+(\theta-1)l})x^k$$
$$= \lambda^{-1}\big(\langle T_{\lambda,l}^{\theta-k}(\mathbf{c}), \mathbf{d}\rangle_{\mathbb{F}_q}\big)x^k, \quad \text{for each } 1 \leqslant k \leqslant \theta - 1.$$

Then the uniqueness of the expression of the left-hand side of (4) implies that each term is 0. Thus, the above equations imply that $\langle T_{\lambda,l}^{i}(\mathbf{c}), \mathbf{d}\rangle_{\mathbb{F}_q} = 0$ for $0 \leqslant i \leqslant \theta - 1$.

It is easy to observe that the converse is also true. □

Applying Lemma 1, we have the following theorem:

Theorem 2. *Let $\mathscr{C}$ be a (λ, l)-QT code of length n over $\mathbb{F}_q$ and $\mathscr{D}$ a (λ^{-1}, l)-QT code of length n over $\mathbb{F}_q$. Then $\mathscr{D}$ is the dual code of $\mathscr{C}$ with respect to the inner product on $\mathbb{F}_q^n$ if and only if $\phi(\mathscr{D})$ is the dual code of $\mathscr{C}$ with respect to the inner product on $\mathbb{R}_{\theta,\lambda}^l$, i.e.,*

$$\phi\big(\mathscr{C}^{\perp_{\mathbb{F}_q}}\big) = \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}, \tag{5}$$

where $\mathscr{C}$ on the left is the code over $\mathbb{F}_q$ while $\mathscr{C}$ on the right means its corresponding module over $\mathbb{R}_{\theta,\lambda}$.

Proof. Since $\mathscr{C}$ is a (λ, l)-QT code, for any codeword $\mathbf{c} \in \mathscr{C}$, we have $T_{\lambda,l}^{i}(\mathbf{c}) \in \mathscr{C}$. Then for any codeword $\mathbf{d} \in \mathscr{C}^{\perp_{\mathbb{F}_q}}$, we have $\langle T_{\lambda,l}^{i}(\mathbf{c}), \mathbf{d}\rangle_{\mathbb{F}_q} = 0$. By Lemma 1, it follows $\langle \mathbf{c}, \phi(\mathbf{d})\rangle_{\mathbb{R}_{\theta,\lambda}} = 0$. Therefore, we have $\phi(\mathbf{d}) \in \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$. Then by Definition 5, we have $\phi(\mathscr{C}^{\perp_{\mathbb{F}_q}}) \subseteq \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$.

Assume that $\mathbf{e} \in \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$. Then by Lemma 1, for any codeword $\mathbf{c} \in \mathscr{C}$, we have $\langle T_{\lambda,l}^{i}(\mathbf{c}), \phi^{-1}(\mathbf{e})\rangle_{\mathbb{F}_q} = 0$. It follows that $\phi^{-1}(\mathbf{e}) \in \mathscr{C}^{\perp_{\mathbb{F}_q}}$. Then $\mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}} \subseteq \phi(\mathscr{C}^{\perp_{\mathbb{F}_q}})$. Therefore, $\phi(\mathscr{C}^{\perp_{\mathbb{F}_q}}) = \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$. □

By the decomposition of the ring $\mathbb{R}_{\theta,\lambda}$ in (2), we have the following corollary.

Corollary 1. *Let $\mathscr{C}$ be a (λ, l)-QT code over $\mathbb{F}_q$ of length $n = l\theta$. Suppose that $\mathscr{C}$ is decomposed as in (2). Then $\mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}}$ is decomposed as follows*:

$$\mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}} \simeq \bigoplus_{i=1}^{k} \mathscr{D}_i, \tag{6}$$

where, for each $1 \leqslant i \leqslant k$, $\mathscr{D}_i$ is the dual code of $\mathscr{C}_i$ with respect to the inner product on $\mathbb{R}_i^l$. In particular, $\mathscr{C}$ is self-dual if and only if $\mathscr{C}_i = \mathscr{D}_i$ for all $1 \leqslant i \leqslant k$.

By Theorem 2, the above corollary gives the decomposition of $\phi(\mathscr{C}^{\perp_{\mathbb{F}_q}})$. Next we discuss the relationship between the decomposition of $\mathscr{C}^{\perp_{\mathbb{F}_q}} \subseteq \mathbb{R}_{\theta,\lambda^{-1}}^l$ and that of $\phi(\mathscr{C}^{\perp_{\mathbb{F}_q}}) = \mathscr{C}^{\perp_{\mathbb{R}_{\theta,\lambda}}} \subseteq \mathbb{R}_{\theta,\lambda}^l$.

Assume that $x^\theta - \lambda$ is factorized as in Eq. (1). Then

$$x^\theta - \lambda^{-1} = -\lambda^{-1}\big(f_1^*(x)\big)^{p^a} \cdots \big(f_k^*(x)\big)^{p^a}, \tag{7}$$

where $f_i^*(x) := x^{\deg f_i(x)} f_i(x^{-1})$ is the reciprocal polynomial of $f_i(x)$ over $\mathbb{F}_q$. It is easy to check that $f_i^*(x)$ is also irreducible over $\mathbb{F}_q$ if $f_i(x)$ is irreducible. Therefore, we have the following decomposition of the ring $\mathbb{R}_{\theta,\lambda^{-1}}$:

$$\frac{\mathbb{F}_q[x]}{(x^\theta - \lambda^{-1})} \simeq \frac{\mathbb{F}_q[x]}{((f_1^*(x))^{p^a})} \oplus \frac{\mathbb{F}_q[x]}{((f_2^*(x))^{p^a})} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{((f_k^*(x))^{p^a})},$$
$$r(x) \leftrightarrow \big(r(x) + \big(\big(f_1^*(x)\big)^{p^a}\big), \ldots, r(x) + \big(\big(f_k^*(x)\big)^{p^a}\big)\big). \tag{8}$$

For simplicity, we denote the ring $\frac{\mathbb{F}_q[x]}{((f_i^*(x))^{p^a})}$ by $\mathbb{R}_i^*$ for $1 \leqslant i \leqslant k$. It follows that

$$\mathbb{R}_{\theta,\lambda^{-1}}^l \simeq \bigoplus_{i=1}^{k} \big(\mathbb{R}_i^*\big)^l. \tag{9}$$

Note that a (λ, l)-QT code is self-dual only if $\lambda = \pm 1$. If $\lambda \neq \pm 1$, then the polynomials $x^\theta - \lambda$ and $x^\theta - \lambda^{-1}$ are coprime over $\mathbb{F}_q$. Therefore, the irreducible polynomials $f_i(x)$, $f_j^*(x)$, $1 \leqslant i, j \leqslant k$, are pairwise coprime where $f_i(x)$, $f_j^*(x)$, $1 \leqslant i, j \leqslant k$ are as in Eqs. (2) and (7). Thus, no irreducible polynomial is an associate of its reciprocal polynomial and no reciprocal pair exists in the factorization of $x^\theta - \lambda$, which is different from the case when $\lambda = \pm 1$.

4.1. Case when $\lambda = \pm 1$

In this subsection, we focus on the case when $\lambda = \pm 1$. If $\lambda = \pm 1$, then $x^\theta - \lambda = x^\theta - \lambda^{-1}$ and hence $\mathbb{R}_{\theta,\lambda} = \mathbb{R}_{\theta,\lambda^{-1}}$. With the proper permutation of the irreducible polynomial factors, $x^\theta - \lambda$ is written as

$$x^\theta - \lambda = \epsilon \big(g_1(x)\big)^{p^a} \cdots \big(g_s(x)\big)^{p^a} \big(h_1(x)\big)^{p^a} \big(h_1^*(x)\big)^{p^a} \cdots \big(h_t(x)\big)^{p^a} \big(h_t^*(x)\big)^{p^a},$$

where $s + 2t = k$, $\epsilon \in \mathbb{F}_q^*$ and, for each $1 \leqslant i \leqslant s$, $g_i(x)$ is an associate of its reciprocal polynomial, i.e., $g_i(x) = \epsilon_i g_i^*(x)$ over $\mathbb{F}_q$ for some unit ϵ_i. Throughout this subsection, we denote $\mathbb{F}_q[x]/((g_i(x))^{p^a})$ by $\mathbb{G}_i$ for $1 \leqslant i \leqslant s$, $\mathbb{F}_q[x]/((h_j(x))^{p^a})$ by $\mathbb{H}_j$ and $\mathbb{F}_q[x]/((h_j^*(x))^{p^a})$ by $\mathbb{H}_j^*$ for $1 \leqslant j \leqslant t$. Then the decomposition of $\mathbb{R}_{\theta,\lambda} = \mathbb{R}_{\theta,\lambda^{-1}}$ is

$$\mathbb{R}_{\theta,\lambda} \simeq \bigoplus_{i=1}^{s} \mathbb{G}_i \oplus \left(\bigoplus_{j=1}^{t} \big(\mathbb{H}_j \oplus \mathbb{H}_j^*\big) \right). \tag{10}$$

Therefore, when $\lambda = \pm 1$, the map ϕ is an automorphism of $\mathbb{R}_{\theta,\lambda}^l$. We define same isomorphisms between the component rings as follows.

Definition 7. For $1 \leqslant i \leqslant s$, define

$$\phi_i : (\mathbb{G}_i)^l \to (\mathbb{G}_i)^l$$

by

$$\begin{aligned} &\phi_i\big(\big(r_1(x) + \big(\big(g_i(x)\big)^{p^a}\big), \ldots, r_l(x) + \big(\big(g_i(x)\big)^{p^a}\big)\big)\big) \\ &\quad = \big(r_1\big(x^{-1}\big) + \big(\big(g_i(x)\big)^{p^a}\big), \ldots, r_l\big(x^{-1}\big) + \big(\big(g_i(x)\big)^{p^a}\big)\big). \end{aligned}$$

For $1 \leqslant j \leqslant t$, define

$$\phi_j' : (\mathbb{H}_j)^l \to \big(\mathbb{H}_j^*\big)^l$$

by

$$\begin{aligned} &\phi_j'\big(\big(r_1(x) + \big(\big(h_j(x)\big)^{p^a}\big), \ldots, r_l(x) + \big(\big(h_j(x)\big)^{p^a}\big)\big)\big) \\ &\quad = \big(r_1\big(x^{-1}\big) + \big(\big(h_j^*(x)\big)^{p^a}\big), \ldots, r_l\big(x^{-1}\big) + \big(\big(h_j^*(x)\big)^{p^a}\big)\big). \end{aligned}$$

Actually, when $\lambda = \pm 1$, the maps ϕ, ϕ_i and ϕ'_j are exactly the conjugate maps defined in [5].

Lemma 2. *Assume that $\lambda = \pm 1$ and the decomposition of the ring $\mathbb{R}_{\theta,\lambda} = \mathbb{R}_{\theta,\lambda^{-1}}$ is as in Eq.* (10)*. Let $r(x) \in \mathbb{R}_{\theta,\lambda}$ and let its decomposition in $\mathbb{R}_{\theta,\lambda}$ be*

$$\big(r_1(x), \ldots, r_s(x), r'_1(x), r''_1(x), \ldots, r'_t(x), r''_t(x)\big)$$

where for $1 \leqslant i \leqslant s$, $r_i(x) = r(x) + ((g_i(x))^{p^a}) \in \mathbb{G}_i$, and for $1 \leqslant j \leqslant t$, $r'_j(x) = r(x) + ((h_j(x))^{p^a}) \in \mathbb{H}_j$ and $r''_j(x) = r(x) + ((h^*_j(x))^{p^a}) \in \mathbb{H}^*_j$. Then the decomposition of $\phi^{-1}(r(x)) \in \mathbb{R}_{\theta,\lambda^{-1}}$ is

$$\big(r_1\big(x^{-1}\big), \ldots, r_s\big(x^{-1}\big), r''_1\big(x^{-1}\big), r'_1\big(x^{-1}\big), \ldots, r''_t\big(x^{-1}\big), r'_t\big(x^{-1}\big)\big).$$

Proof. For $1 \leqslant i \leqslant s$, since $r_i(x) = r(x) + ((g_i(x))^{p^a})$,

$$r_i\big(x^{-1}\big) = r\big(x^{-1}\big) + \big(\big(g_i\big(x^{-1}\big)\big)^{p^a}\big).$$

Since $g(x)$ is an associate of its reciprocal polynomial,

$$\big(\big(g_i(x)\big)^{p^a}\big) = \big(\big(g_i\big(x^{-1}\big)\big)^{p^a}\big).$$

Therefore, we have

$$r_i\big(x^{-1}\big) = r\big(x^{-1}\big) + \big(\big(g_i(x)\big)^{p^a}\big),$$

i.e., the component of $\phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{G}_i$ is $r_i(x^{-1})$.

For $1 \leqslant j \leqslant t$, we have

$$r'_j\big(x^{-1}\big) = r\big(x^{-1}\big) + \big(\big(h_j\big(x^{-1}\big)\big)^{p^a}\big).$$

Then

$$r'_j\big(x^{-1}\big) = r\big(x^{-1}\big) + \big(h^*_j(x)\big)^{p^a},$$

i.e., the component of $\phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{H}^*_j$ is $r'_j(x^{-1})$.

Similarly, the component of $\phi^{-1}(r(x)) = r(x^{-1})$ in $\mathbb{H}_j$ is $r''_j(x^{-1})$. □

The following theorem gives the algebraic structure of the dual code of a (λ, l)-QT code when $\lambda = \pm 1$.

Theorem 3. *Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$ with $\lambda = \pm 1$. Let the decomposition of the ring $\mathbb{R}_{\theta,\lambda}$ be as in Eq.* (10) *and let the corresponding decomposition of $\mathscr{C}$ be*

$$\mathscr{C} \simeq \bigoplus_{i=1}^{s} \mathscr{C}_i \oplus \left(\bigoplus_{j=1}^{t} \big(\mathscr{C}'_j \oplus \mathscr{C}''_j\big) \right).$$

Then the decomposition of its dual code $\mathscr{C}^{\perp_{\mathbb{F}_q}}$ is

$$\mathscr{C}^{\perp_{\mathbb{F}_q}} \simeq \bigoplus_{i=1}^{s} \phi_i\big(\mathscr{C}_i^{\perp_{\mathbb{G}_i}}\big) \oplus \left(\bigoplus_{j=1}^{t} \big(\big(\phi_j'\big)^{-1}\big(\big(\mathscr{C}_j''\big)^{\perp_{\mathbb{H}_j^*}}\big) \oplus \phi_j'\big(\big(\mathscr{C}_j'\big)^{\perp_{\mathbb{H}_j}}\big)\big)\right),$$

where the duality on the left is the duality with respect to the inner product over $\mathbb{F}_q$, while the dualities on the right are the dualities with respect to the inner products over the respective component rings.

In particular, $\mathscr{C}$ is self-dual if and only if

$$\begin{cases} \mathscr{C}_i = \phi_i\big(\mathscr{C}_i^{\perp_{\mathbb{G}_i}}\big), & 1 \leqslant i \leqslant s, \\ \mathscr{C}_j'' = \phi_j'\big(\big(\mathscr{C}_j'\big)^{\perp_{\mathbb{H}_j}}\big), & 1 \leqslant j \leqslant t. \end{cases} \tag{11}$$

Proof. This theorem follows from Corollary 1 and Lemma 2. □

When $\lambda = \pm 1$, the map ϕ_i's are actually the conjugates defined in [5]. We can check that the above theorem is consistent with Theorem 4.2 in [5] which describes the dual with respect to the Hermitian inner product.

4.2. Case when $\lambda \neq \pm 1$

In this subsection, we assume that $\lambda \neq \pm 1$. Recall that ϕ is the isomorphism between $\mathbb{R}_{\theta,\lambda}$ and $\mathbb{R}_{\theta,\lambda^{-1}}$. Let the decompositions of $\mathbb{R}_{\theta,\lambda}^l$ and $\mathbb{R}_{\theta,\lambda^{-1}}^l$ be as in Eqs. (2) and (9), respectively. Then the quotient rings $\mathbb{R}_i = \mathbb{F}_q[x]/((f_i(x))^{p^a})$ and $\mathbb{R}_i^* = \mathbb{F}_q[x]/((f_i^*(x))^{p^a})$ are isomorphic as rings. The corresponding isomorphism is defined as follows.

Definition 8. The isomorphism is

$$\phi_i' : (\mathbb{R}_i)^l \to \big(\mathbb{R}_i^*\big)^l$$

given by

$$\begin{aligned} &\phi_i'\big(\big(r_1(x) + \big(\big(f_i(x)\big)^{p^a}\big), \ldots, r_l(x) + \big(\big(f_i(x)\big)^{p^a}\big)\big)\big) \\ &\quad = \big(r_1\big(x^{-1}\big) + \big(\big(f_i^*(x)\big)^{p^a}\big), \ldots, r_l\big(x^{-1}\big) + \big(\big(f_i^*(x)\big)^{p^a}\big)\big). \end{aligned}$$

By Corollary 1, the following theorem immediately follows.

Theorem 4. *Let $\lambda \neq \pm 1$ and let the decompositions of $\mathbb{R}_{\theta,\lambda}^l$ and $\mathbb{R}_{\theta,\lambda^{-1}}^l$ be as in Eqs.* (2) *and* (9)*, respectively. Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$, i.e., an $\mathbb{R}_{\theta,\lambda}$-linear code. Suppose that the decomposition of $\mathscr{C}$ is as in* (3)*:*

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i.$$

Then the decomposition of its dual code $\mathscr{C}^{\perp_{\mathbb{F}_q}} \subseteq \mathbb{R}_{\theta,\lambda^{-1}}^l$ is

$$\mathscr{C}^{\perp_{\mathbb{F}_q}} \simeq \bigoplus_{i=1}^{k} \phi_i\big(\mathscr{C}_i^{\perp_{\mathbb{R}_i}}\big).$$

Given the decomposition of the code $\mathscr{C} \subseteq \mathbb{R}^l_{\theta,\lambda}$, Theorems 3 and 4 give the decomposition of the dual code $\mathscr{C}^{\perp_{\mathbb{F}_q}} \subseteq \mathbb{R}^l_{\theta,\lambda^{-1}}$, for cases $\lambda = \pm 1$ and $\lambda \neq \pm 1$ respectively.

5. Discrete Fourier transform

In order to deal with the repeated-root case, we introduce a generalized discrete Fourier transform (GDFT) as in [4]. For our purpose, we define the Hasse derivative as follows.

Definition 9. (See [3].) For a polynomial $g(x) = \sum_i g_i x^i \in \mathbb{F}_q[x]$, the j-th *Hasse derivative* is defined as

$$g^{[j]}(x) = \sum_i \binom{i}{j} g_i x^{i-j}.$$

Using the Hasse derivative, we define the generalized discrete Fourier transform (GDFT). Recall that $\theta = p^a\bar{\theta}$, where $\gcd(\bar{\theta}, p) = 1$.

Definition 10. If $c(x) = \sum_{i\in\mathbb{Z}/\theta\mathbb{Z}} c_i x^i \in \mathbb{R}_{\theta,\lambda}$, then the *generalized discrete Fourier transform (GDFT)* of $c(x)$ can be described in terms of a matrix

$$\hat{c} = \begin{bmatrix} \hat{c}_{0,0} & \hat{c}_{0,1} & \cdots & \hat{c}_{0,\bar{\theta}-1} \\ \hat{c}_{1,0} & \hat{c}_{1,1} & \cdots & \hat{c}_{1,\bar{\theta}-1} \\ \vdots & \vdots & \vdots & \vdots \\ \hat{c}_{p^a-1,0} & \hat{c}_{p^a-1,1} & \cdots & \hat{c}_{p^a-1,\bar{\theta}-1} \end{bmatrix}, \tag{12}$$

where

$$\hat{c}_{g,h} = \sum_{i\in\mathbb{Z}/\theta\mathbb{Z}} \binom{i}{g} c_i \left(\beta\xi^h\right)^{i-g}, \quad \text{for } 0 \leqslant g \leqslant p^a - 1,\ 0 \leqslant h \leqslant \bar{\theta} - 1,$$

β is a $\bar{\theta}$-th root of $\bar{\lambda}$,

and ξ is a primitive $\bar{\theta}$-th root of unity.

Notice that $\hat{c}_{g,h}$ is exactly the value of the g-th Hasse derivative at $\beta\xi^h$, a $\bar{\theta}$-th root of $\bar{\lambda}$. Let $x^\theta - \lambda$ be decomposed as in (1). Then for each $1 \leqslant h \leqslant \bar{\theta}$, there is an irreducible factor of $x^\theta - \lambda$, say $f_i(x)$, such that $\beta\xi^h$ is a root of $f_i(x)$. Then $\hat{c}_{g,h}$ is an element in $\mathbb{F}_q[x]/((f_i(x))^{p^a})$. Mimicking the method in [5] and replacing the root ξ^h in [5] by $\beta\xi^h$, then the explicit description of the inverse transform is given. We give the inverse transform in the following theorem and omit the proof.

Theorem 5. *The GDFT* (12) *is invertible. More precisely, the inverse formula of GDFT is*

$$c_{i+jp^a} = \frac{1}{\bar{\theta}} \sum_{h=0}^{\bar{\theta}-1} \left(\beta\xi^h\right)^{-jp^a} \left(\sum_{g=0}^{p^a-1} \binom{g}{i} \left(-\beta\xi^h\right)^{g-i} \hat{c}_{g,h} \right), \tag{13}$$

for $0 \leqslant i \leqslant p^a - 1$ *and* $0 \leqslant j \leqslant \bar{\theta} - 1$, *where* β *is a* $\bar{\theta}$*-th root of* $\bar{\lambda}$ *and* ξ *is a primitive* $\bar{\theta}$*-th root of unity.*

Since $(\beta^{q-1})^{\bar{\theta}} = \bar{\lambda}^{q-1} = 1$ for $\bar{\lambda} \in \mathbb{F}_q^*$, β^{q-1} is a $\bar{\theta}$-th root of unity. Then β^{q-1} can be expressed as a power of the primitive $\bar{\theta}$-th root of unity ξ, say

$$\beta^{q-1} = \xi^{\delta},$$

where $0 \leqslant \delta \leqslant \bar{\theta} - 1$.

By the definition of $\hat{c}_{g,h}$, it is easy to verify that, for $0 \leqslant g \leqslant p^a - 1$ and $0 \leqslant h \leqslant \bar{\theta} - 1$,

$$\begin{aligned}\hat{c}_{g,h}^{q} &= \sum_{i \in \mathbb{Z}/\theta\mathbb{Z}} \binom{i}{g}^{q} c_i^{q} \left[\left(\beta\xi^{h}\right)^{q}\right]^{i-g} \\ &= \sum_{i \in \mathbb{Z}/\theta\mathbb{Z}} \binom{i}{g} c_i \left(\beta\xi^{qh+\delta}\right)^{i-g} \\ &= \hat{c}_{g,qh+\delta}.\end{aligned}$$

Given an irreducible polynomial $f_i(x)$, if $\beta\xi^{z_i}$ is a root of $f_i(x)$, so is $\beta^q\xi^{qz_i} = \beta\xi^{qz_i+\delta}$. Define a map τ:

$$\begin{aligned}\tau : \mathbb{Z}/\bar{\theta}\mathbb{Z} &\to \mathbb{Z}/\bar{\theta}\mathbb{Z}, \\ z &\mapsto qz + \delta.\end{aligned}$$

As $\gcd(\bar{\theta}, q) = 1$, it follows that the map τ is one-to-one. Therefore, the map τ defines an equivalence relation $\sim$ on $\mathbb{Z}/\bar{\theta}\mathbb{Z}$ where $h_1 \sim h_2$ if and only if there exists an integer i such that $h_1 = \tau^i(h_2)$. Therefore, there is a one-to-one correspondence between the equivalence classes and the irreducible factors f_i's. For convenience, we call the equivalence classes *orbits of* τ. From each orbit $\mathbf{O}_i$, we can choose a representative, say z_i. Then there is a one-to-one correspondence between the irreducible factors $f_i(x)$'s and the representatives z_i's. We say the representative z_i is corresponding to the irreducible polynomial f_i. In particular, when $\delta = 0$, the equivalence classes are known as the q-cyclotomic cosets modulo $\bar{\theta}$.

Therefore, using the same notations above, the inverse formula of the GDFT can be further simplified as follows.

Theorem 6. *The GDFT* (12) *is invertible as follows*: *for* $0 \leqslant i \leqslant p^a - 1$ *and* $0 \leqslant j \leqslant \bar{\theta} - 1$,

$$c_{i+jp^a} = \frac{1}{\bar{\theta}} \sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \left(\sum_{\gamma=1}^{k} Tr_{\gamma}\left(\hat{c}_{g,z_\gamma}\left(\beta\xi^{z_\gamma}\right)^{g-i-jp^a}\right)\right), \tag{14}$$

where β *is a* $\bar{\theta}$*-th root of* $\bar{\lambda}$, ξ *is a primitive* $\bar{\theta}$*-th root of unity,* z_γ *is a representative in the orbit corresponding to* $f_\gamma(x)$ *and* Tr_γ *is the trace map on the field* $\mathbb{F}_q[x]/(f_\gamma(x))$ *down to* $\mathbb{F}_q$.

Although the choices of β and ξ in the formula (14) are not unique, the result of the formula (14) is unique when $\hat{c}_{g,h}$'s are given. The above theorem gives the trace description of QT codes.

6. Construction formula

Let $\mathscr{C}$ be a (λ, l)-QT code of length $l\theta$. By Theorem 1, we know that

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i,$$

where $\mathscr{C}_i$ is a linear code over $\mathbb{R}_i$ of length l for each $1 \leqslant i \leqslant k$.

The ring $\mathbb{R}_i = \frac{\mathbb{F}_q[x]}{((f_i(x))^{p^a})}$ is a finite chain ring. Each element in $\mathbb{R}_i$ can be written in the following canonical form:

$$a_0(x) + a_1(x) f_i(x) + \cdots + a_{p^a-1}(x)\big(f_i(x)\big)^{p^a-1},$$

where $a_j(x) \in \frac{\mathbb{F}_q[x]}{(f_i(x))}$ for $0 \leqslant j \leqslant p^a - 1$. Therefore,

$$\frac{\mathbb{F}_q[x]}{((f_i(x))^{p^a})} \simeq \frac{\mathbb{F}_q[x]}{(f_i(x))} + f_i(x)\frac{\mathbb{F}_q[x]}{(f_i(x))} + \cdots + \big(f_i(x)^{p^a-1}\big)\frac{\mathbb{F}_q[x]}{(f_i(x))}.$$

Let $d_i = \deg f_i(x)$ and let $\beta\xi^{z_i}$ be a root of $f_i(x)$. Then we have the following field isomorphism:

$$\frac{\mathbb{F}_q[x]}{(f_i(x))} \simeq \mathbb{F}_q + \big(\beta\xi^{z_i}\big)\mathbb{F}_q + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbb{F}_q,$$
$$r(x) \leftrightarrow r\big(\beta\xi^{z_i}\big).$$

Then we have the following proposition.

Proposition 3. *The following map is a ring isomorphism*:

$$\sigma : \mathbb{R}_i \to \big(\mathbb{F}_q + \big(\beta\xi^{z_i}\big)\mathbb{F}_q + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbb{F}_q\big) + u\big(\mathbb{F}_q + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbb{F}_q\big)$$
$$+ \cdots + u^{p^a-1}\big(\mathbb{F}_q + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbb{F}_q\big),$$
$$r(x) \mapsto r\big(\beta\xi^{z_i} + u\big),$$

where $u^{p^a} = 0$ *and* $\beta\xi^{z_i}$ *is a root of* $f_i(x)$.

Proof. For convenience, denote $f_i(x)$ by $f(x)$, $d = \deg(f(x))$ and $\beta\xi^{z_i}$ by η. Suppose that $f(x) = \sum_{i=0}^{d} a_i x^i$. Since η is a root of $f(x)$ and $u^{p^a} = 0$, we have

$$\begin{aligned}
\sigma\big(\big(f(x)\big)^{p^a}\big) &= \big(f(\eta + u)\big)^{p^a} \\
&= \sum_{i=0}^{d} a_i^{p^a}\big(\eta^{p^a} + u^{p^a}\big)^i \\
&= \sum_{i=0}^{d} a_i^{p^a}\eta^{p^a i} \\
&= \big(f(\eta)\big)^{p^a} \\
&= 0.
\end{aligned}$$

Therefore, this map is well defined.

Since η is a root of the irreducible polynomial $f(x)$, $\eta^{\bar{\theta}\bar{r}} = \bar{\lambda}^{\bar{r}} = 1$, where $\bar{r}$ is the order of $\bar{\lambda} \in \mathbb{F}_q^*$. Since $\bar{r}$ divides $q-1$, $\bar{r}$ is coprime to p^a. Since $\bar{\theta}$ is coprime to p^a too, p^a and $\bar{\theta}\bar{r}$ are coprime. Then there exist integers N_1 and N_2 such that

$$p^a N_1 + N_2\bar{\theta}\bar{r} = 1.$$

Then we have $\eta^{p^a N_1} = \eta$.

It follows that $x^{p^a N_1}$ is mapped to η and $x - x^{p^a N_1}$ is mapped to u. Hence, the map σ is a ring isomorphism. □

For simplicity, we denote by J_i the chain ring

$$\begin{aligned}&\big(\mathbb{F}_q + \big(\beta\xi^{z_i}\big)\mathbb{F}_q + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbb{F}_q\big) + u\big(\mathbb{F}_q + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbb{F}_q\big) + \cdots\\ &\quad + u^{p^a-1}\big(\mathbb{F}_q + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbb{F}_q\big).\end{aligned}$$

Then we have

$$\mathbb{R}_{\theta,\lambda} \simeq \bigoplus_{i=1}^{k} J_i,$$

and

$$\mathscr{C} \simeq \bigoplus_{i=1}^{k} \mathscr{C}_i,$$

where $\mathscr{C}_i$ is a code over J_i of length l.

Then a codeword $\mathbf{x}_i$ of $\mathscr{C}_i$ over J_i can be written as

$$\begin{aligned}\mathbf{x}_i &= \big(\mathbf{x}_{i,0,0} + \big(\beta\xi^{z_i}\big)\mathbf{x}_{i,0,1} + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbf{x}_{i,0,d_i-1}\big)\\ &\quad + u\big(\mathbf{x}_{i,1,0} + \big(\beta\xi^{z_i}\big)\mathbf{x}_{i,1,1} + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbf{x}_{i,1,d_i-1}\big) + \cdots\\ &\quad + u^{p^a-1}\big(\mathbf{x}_{i,p^a-1,0} + \big(\beta\xi^{z_i}\big)\mathbf{x}_{i,p^a-1,1} + \cdots + \big(\beta\xi^{z_i}\big)^{d_i-1}\mathbf{x}_{i,p^a-1,d_i-1}\big),\end{aligned}$$

where, for each $1 \leqslant i \leqslant k$, $0 \leqslant j \leqslant p^a - 1$ and $0 \leqslant w \leqslant d_i - 1$, $\mathbf{x}_{i,j,w}$ is a row vector over $\mathbb{F}_q$ of length l.

We vertically joint all the above row vectors $\mathbf{x}_{i,j,w}$ as

$$\tilde{\mathbf{x}}_i = (\mathbf{x}_{i,0,0}, \ldots, \mathbf{x}_{i,0,d_i-1}, \mathbf{x}_{i,1,0}, \ldots, \mathbf{x}_{i,1,d_i-1}, \ldots, \mathbf{x}_{i,p^a-1,0}, \ldots, \mathbf{x}_{i,p^a-1,d_i-1})^T.$$

Then $\tilde{\mathbf{x}}_i$ is a matrix of size $p^a d_i \times l$. We vertically joint all the above matrices as

$$\mathbf{x} = (\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2, \ldots, \tilde{\mathbf{x}}_k)^T. \tag{15}$$

Then $\mathbf{x}$ is in fact a matrix of size $\theta \times l$ because $\sum_{i=1}^{k} p^a d_i = \theta$.

By Theorem 5, a codeword in a QT code can be given if the component codewords are known. With the same notations as above, we have the following result about the construction of a QT code.

Theorem 7. *Let $\theta = p^a\bar{\theta}$ with $\gcd(p, \bar{\theta}) = 1$, where p is the characteristic of $\mathbb{F}_q$. Then, for any positive integer l and any $\lambda \in \mathbb{F}_q^*$, the (λ, l)-QT codes over $\mathbb{F}_q$ of length $l\theta$ are precisely given as follows*:

1. *Write $\lambda = \bar{\lambda}^{p^a}$ where $\bar{\lambda} \in \mathbb{F}_q^*$.*
2. *Write $x^{\bar{\theta}} - \bar{\lambda} = f_1(x) f_2(x) \cdots f_k(x)$, where for $1 \leqslant \gamma \leqslant k$, $f_\gamma(x)$ are monic irreducible polynomials over $\mathbb{F}_q$.*
3. *Write $\mathbb{F}_q[x]/((f_\gamma(x))^{p^a}) = \mathbb{R}_\gamma$ and $\deg f_\gamma(x) = d_\gamma$.*

4. *Let* $\mathbf{O}_\gamma$ *denote the orbit corresponding to* $f_\gamma(x)$ *and fix* $z_\gamma \in \mathbf{O}_\gamma$.
5. *For each* $1 \leqslant \gamma \leqslant k$, *let* $\mathscr{C}_\gamma$ *be a linear code of length* l *over* $\mathbb{R}_\gamma$. *For* $\mathbf{x}_\gamma \in \mathscr{C}_\gamma$, *write*

$$\begin{aligned}\mathbf{x}_\gamma = {} & \left(\mathbf{x}_{\gamma,0,0} + \left(\beta\xi^{z_\gamma}\right)\mathbf{x}_{\gamma,0,1} + \cdots + \left(\beta\xi^{z_\gamma}\right)^{d_\gamma-1}\mathbf{x}_{\gamma,0,d_\gamma-1}\right) \\ & + u\left(\mathbf{x}_{\gamma,1,0} + \left(\beta\xi^{z_\gamma}\right)\mathbf{x}_{\gamma,1,1} + \cdots + \left(\beta\xi^{z_\gamma}\right)^{d_\gamma-1}\mathbf{x}_{\gamma,1,d_\gamma-1}\right) + \cdots \\ & + u^{p^a-1}\left(\mathbf{x}_{\gamma,p^a-1,0} + \left(\beta\xi^{z_\gamma}\right)\mathbf{x}_{\gamma,p^a-1,1} + \cdots + \left(\beta\xi^{z_\gamma}\right)^{d_\gamma-1}\mathbf{x}_{\gamma,p^a-1,d_\gamma-1}\right),\end{aligned}$$

   where, for each $1 \leqslant \gamma \leqslant k$, $0 \leqslant g \leqslant p^a - 1$ *and* $0 \leqslant w \leqslant d_\gamma - 1$, $\mathbf{x}_{\gamma,g,w}$ *is a row vector over* $\mathbb{F}_q$ *of length* l.
6. *For each* $0 \leqslant i \leqslant p^a - 1$ *and* $0 \leqslant j \leqslant \bar{\theta} - 1$, *let*

$$\mathbf{c}_{i+jp^a} = \frac{1}{\bar{\theta}}\sum_{g=0}^{p^a-1}\binom{g}{i}(-1)^{g-i}\left(\sum_{\gamma=1}^{k}\left(\sum_{w=0}^{d_\gamma-1}\left(\mathbf{x}_{\gamma,g,w}Tr_\gamma\left(\left(\beta\xi^{z_\gamma}\right)^{g-i-jp^a+w}\right)\right)\right)\right), \tag{16}$$

   and hence the codewords $\mathbf{x}_\gamma \in \mathscr{C}_\gamma$, $1 \leqslant \gamma \leqslant k$ *give a vector* $(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\theta-1})$.

Then when the codeword $\mathbf{x}_\gamma$ *runs through all the codewords in* $\mathscr{C}_\gamma$ *for each* γ, *the collection of all the vectors* $(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\theta-1})$ *given by Eq.* (16)

$$\mathscr{C} = \left\{(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\theta-1})\right\}$$

is a (λ, l)*-QT code over* $\mathbb{F}_q$ *of length* $l\theta$. *Conversely, every QT code over* $\mathbb{F}_q$ *of length* $l\theta$ *is obtained through this construction. Moreover, the construction can be expressed as follows*:

$$(\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\theta-1})^T = A \cdot \mathbf{x},$$

where $\mathbf{x}$ *is defined as in* (15), A *is a* $\theta \times \theta$ *matrix over* $\mathbb{F}_q$ *such that, for* $0 \leqslant i \leqslant p^a - 1$, $0 \leqslant j \leqslant \bar{\theta} - 1$, $0 \leqslant g \leqslant p^a - 1$, $1 \leqslant \gamma \leqslant k$, $0 \leqslant w \leqslant d_\gamma - 1$, *the entry in the* $(i + jp^a + 1)$*-th row and* $(p^a\sum_{h=1}^{\gamma-1} d_h + gd_\gamma + w + 1)$*-th column, i.e., the coefficient in front of* $\mathbf{x}_{\gamma,g,w}$ *is*

$$A\left(i + jp^a + 1,\ p^a\sum_{h=1}^{\gamma-1} d_h + gd_\gamma + w + 1\right) = \frac{1}{\bar{\theta}}(-1)^{g-i}\binom{g}{i}Tr_\gamma\left(\left(\beta\xi^{z_\gamma}\right)^{g-i-jp^a+w}\right).$$

Proof. By the isomorphism in Proposition 3, $\hat{c}_{g,\gamma}$ in Eq. (14) can be written as $\sum_{w=0}^{d_\gamma-1}(\beta\xi^{z_\gamma})^w\mathbf{x}_{\gamma,g,w}$, and the γ-th component of $c(x)$ is $\hat{c}_{0,\gamma} + u\hat{c}_{1,\gamma} + \cdots + u^{p^a-1}\hat{c}_{p^a-1,\gamma}$. Then the theorem follows from Eq. (13). Obviously, the matrix A is over $\mathbb{F}_q$ because the entries are obtained by the respective trace maps down to $\mathbb{F}_q$. □

7. Examples

The examples in this section are computed by MAGMA [2].

The following example gives a self-dual $(2, 2)$-QT code of length 24 over $\mathbb{F}_3$. We can see that its decomposition satisfies Eq. (11) given in Theorem 3.

Example 1. Factorize $x^{12}-2$ over $\mathbb{F}_3$ as follows

$$\begin{aligned} x^{12}-2 &= \left(x^4+1\right)^3 \\ &= \left(x^2+x+2\right)^3\left(x^2+2x+2\right)^3 \\ &:= h(x)h^*(x). \end{aligned}$$

Denote by $\mathbb{H}$ the ring $\frac{\mathbb{F}_3[x]}{((x^2+x+2)^3)}$, and denote by $\mathbb{H}^*$ the ring $\frac{\mathbb{F}_3[x]}{((x^2+2x+2)^3)}$.

Let $\mathscr{C}$ be a self-dual $(2,2)$-QT code of length 24 over $\mathbb{F}_3$ with generator $(h(x), h^*(x))$. Then $\mathscr{C}$ can be decomposed as the direct sum of the following two component codes, $\mathscr{C}_1$ and $\mathscr{C}_2$, where:

1. $\mathscr{C}_1$ is generated by $(0, h^*(x) \bmod h(x))$ over $\mathbb{H}$ and
2. $\mathscr{C}_2$ is generated by $(h(x) \bmod h^*(x), 0)$ over $\mathbb{H}^*$.

Since $h(x)$ and $h^*(x)$ are coprime, the vector $(0,1)$ is also a generator of $\mathscr{C}_1$ over $\mathbb{H}$. For the same reason, $(1,0)$ is a generator of $\mathscr{C}_2$ over $\mathbb{H}^*$.

It is easy to observe that the dual code $\mathscr{C}_1^{\perp_{\mathbb{H}}}$ of $\mathscr{C}_1$ over $\mathbb{H}$ is with generator $(1,0)$ over $\mathbb{H}$. Since the isomorphism between $\mathbb{H}^2$ and $(\mathbb{H}^*)^2$ is

$$\begin{gathered} \phi' : \mathbb{H}^2 \to \left(\mathbb{H}^*\right)^2, \\ \left(r_1(x)+\left(h(x)\right), r_2(x)+\left(h^*(x)\right)\right) \mapsto \left(r_1\left(x^{-1}\right)+\left(h^*(x)\right), r_2\left(x^{-1}\right)+\left(h(x)\right)\right), \end{gathered}$$

the image of $(1,0)$ over $\mathbb{H}$ is $(1,0)$ over $\mathbb{H}^*$. Therefore, the image of $\mathscr{C}_1^{\perp_{\mathbb{H}}}$ under ϕ' is generated by $(1,0)$ over $\mathbb{H}^*$, which is exactly $\mathscr{C}_2$ over $\mathbb{H}^*$. Therefore, Eq. (11) given in Theorem 3 is satisfied.

The next example gives a QT code over $\mathbb{F}_5$ as well as that of its dual code where $\lambda \neq \pm 1$. We can see that they satisfy Eq. (5) in Theorem 2 and their decompositions satisfy Eq. (6) in Corollary 1.

Example 2. Factorize $x^{15}-2$ over $\mathbb{F}_5$ as follows

$$\begin{aligned} x^{15}-2 &= \left(x^3+3\right)^5 \\ &= (x+2)^5\left(x^2+3x+4\right)^5 \\ &:= \left(f_1(x)\right)^5\left(f_2(x)\right)^5. \end{aligned}$$

Then

$$\frac{\mathbb{F}_5[x]}{(x^{15}-2)} \simeq \frac{\mathbb{F}_5[x]}{((x+2)^5)} \oplus \frac{\mathbb{F}_5[x]}{((x^2+3x+4)^5)}.$$

Denote the ring $\frac{\mathbb{F}_5[x]}{(x^{15}-2)}$ by $\mathbb{R}_{15,2}$, denote the ring $\frac{\mathbb{F}_5[x]}{((x+2)^5)}$ by $\mathbb{R}_1$ and denote the ring $\frac{\mathbb{F}_5[x]}{((x^2+3x+4)^5)}$ by $\mathbb{R}_2$.

Since $2^{-1}=3$ in $\mathbb{F}_5$, by Eq. (8), we have

$$\mathbb{R}_{15,3} \simeq \mathbb{R}_1^* \oplus \mathbb{R}_2^*,$$

where

$$\mathbb{R}_{15,3} := \frac{\mathbb{F}_5[x]}{(x^{15}-3)},$$
$$\mathbb{R}_1^* := \frac{\mathbb{F}_5[x]}{((x+3)^5)},$$
$$\mathbb{R}_2^* := \frac{\mathbb{F}_5[x]}{((x^2+2x+4)^5)}.$$

Let

$$G_1(x) = x^2 + 4x + 4 = (x+2)^2,$$

and

$$G_2(x) = x^6 + 4x^5 + 4x^4 + 4x^3 + x^2 + 4x + 4 = \left(x^2 + 3x + 4\right)^3.$$

Let $\mathscr{C}$ be a $(2,2)$-QT code of length 30 over $\mathbb{F}_5$ with generator $(G_1(x), G_2(x))$. Then we can decompose $\mathscr{C}$ as the direct sum of the following two component codes, $\mathscr{C}_1$ and $\mathscr{C}_2$, where

1. $\mathscr{C}_1$ is generated by $(G_1(x) \bmod (f_1(x))^5, G_2(x) \bmod (f_1(x))^5)$ and
2. $\mathscr{C}_2$ is generated by $(G_1(x) \bmod (f_2(x))^5, G_2(x) \bmod (f_2(x))^5)$.

Then $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ is a $(3,2)$-QT code of length 30 over $\mathbb{F}_5$ with generator $(g_1(x), g_2(x))$ (over the ring $\mathbb{R}_{15,3}$) where

$$\begin{aligned} g_1(x) &= 3x^{12} + 3x^{11} + 2x^{10} + 4x^9 + 4x^8 + 2x^7 + 2x^6 + 2x^4 + 3x^3 + 4x^2 + 4x + 1 \\ &= \left(x^2 + 2x + 4\right)^3 \left(x^6 + 2x^3 + 3\right), \\ g_2(x) &= 4x^8 + 4x^7 + 2x^4 + 2x^2 + 4 \\ &= 4(x+3)^2 \left(x^3 + x^2 + 4x + 1\right)\left(x^3 + 4x^2 + 3x + 4\right). \end{aligned}$$

The generator $(g_1(x), g_2(x))$ of $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ over $\mathbb{R}_{15,3}$ is mapped to $(g_1'(x), g_2'(x))$ over $\mathbb{R}_{15,2}$ under the isomorphism defined as in Definition 6, where

$$\begin{aligned} g_1'(x) &= 2x^{14} + 2x^{13} + 4x^{12} + x^{11} + x^9 + x^8 + 2x^7 + 2x^6 + x^5 + 4x^4 + 4x^3 + 1, \\ g_2'(x) &= x^{13} + x^{11} + 2x^8 + 2x^7 + 4. \end{aligned}$$

Then the image of $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ can be decomposed as the direct sum of the following two component codes, $\mathscr{D}_1$ and $\mathscr{D}_2$, where

1. $\mathscr{D}_1$ is generated by $(g_1'(x) \bmod (f_1(x))^5, g_2'(x) \bmod (f_1(x))^5)$ and
2. $\mathscr{D}_2$ is generated by $(g_1'(x) \bmod (f_2(x))^5, g_2'(x) \bmod (f_2(x))^5)$.

Notice that

$$\begin{aligned} g_1'(x)G_1(x) + g_2'(x)G_2(x) &\equiv x^{19} + 4x^{18} + 3x^4 + 2x^3 \mod \left(x^{15} - 2\right) \\ &\equiv 0 \mod \left(x^{15} - 2\right). \end{aligned}$$

Therefore, Eq. (5) in Theorem 2 is satisfied.

Since both $(f_1(x))^5$ and $(f_2(x))^5$ are divisors of $(x^{15}-2)$ over $\mathbb{F}_5$, we have

$$\begin{aligned}
&\big\langle \big(g_1'(x), g_2'(x)\big), \big(G_1(x), G_2(x)\big)\big\rangle_{\mathbb{R}_{15,2}} \\
&\quad = \big(g_1'(x)G_1(x) + g_2'(x)G_2(x)\big) \mod \big(x^{15}-2\big) \\
&\quad = 0, \\
&\big\langle \big(g_1'(x) \bmod \big(f_1(x)\big)^5, g_2'(x) \bmod \big(f_1(x)\big)^5\big), \big(G_1(x) \bmod \big(f_1(x)\big)^5, G_2(x) \bmod \big(f_1(x)\big)^5\big)\big\rangle_{\mathbb{R}_1} \\
&\quad = \big(g_1'(x)G_1(x) + g_2'(x)G_2(x)\big) \mod \big(f_1(x)\big)^5 \\
&\quad = 0, \\
&\big\langle \big(g_1'(x) \bmod \big(f_2(x)\big)^5, g_2'(x) \bmod \big(f_2(x)\big)^5\big), \big(G_1(x) \bmod \big(f_2(x)\big)^5, G_2(x) \bmod \big(f_2(x)\big)^5\big)\big\rangle_{\mathbb{R}_2} \\
&\quad = \big(g_1'(x)G_1(x) + g_2'(x)G_2(x)\big) \mod \big(f_2(x)\big)^5 \\
&\quad = 0.
\end{aligned}$$

Therefore, the decomposition of the image of $\mathscr{C}^{\perp_{\mathbb{F}_5}}$ satisfies Eq. (6) in Corollary 1.

The following example shows the decomposition of a $(2,2)$-QT code of length 30 over $\mathbb{F}_3$ using GDFT.

Example 3. Factorize $x^{15}-2$ over $\mathbb{F}_3$ as follows

$$x^{15}-2 = \big(x^5+1\big)^3 = (x+1)^3\big(x^4+2x^3+x^2+2x+1\big)^3. \tag{17}$$

Let

$$G_1(x) = (x+1)^2\big(x^4+2x^3+x^2+2x+1\big),$$

and

$$G_2(x) = (x+1)\big(x^4+2x^3+x^2+2x+1\big)^2.$$

Therefore,

$$\begin{aligned}
\frac{\mathbb{F}_3[x]}{(x^{15}-2)} &\simeq \frac{\mathbb{F}_3[x]}{(x+1)^3} \oplus \frac{\mathbb{F}_3[x]}{(x^4+2x^3+x^2+2x+1)^3} \\
&\simeq \big(\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3\big) \oplus \big(\mathbb{F}_{3^4} + u\mathbb{F}_{3^4} + u^2\mathbb{F}_{3^4}\big).
\end{aligned}$$

For simplicity, denote $\frac{\mathbb{F}_3[x]}{(x^{15}-2)}$ by $\mathbb{R}$, $(\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3)$ by J_1 and $(\mathbb{F}_{3^4} + u\mathbb{F}_{3^4} + u^2\mathbb{F}_{3^4})$ by J_2.

Set a root of x^5+1: $\beta = 2$. Let ξ be a 5-th primitive root of unity.

Since $\beta^{3-1} = 1 = \xi^5$, the map

$$\begin{aligned}
\tau : \mathbb{Z}/5\mathbb{Z} &\to \mathbb{Z}/5\mathbb{Z}, \\
z &\mapsto 3z+5,
\end{aligned}$$

defines two orbits: $\mathbf{O}_1 = \{0\}$ and $\mathbf{O}_2 = \{1, 3, 4, 2\}$. It is easily checked that β is the root of $x+1$ while $\beta\xi$, $\beta\xi^2$, $\beta\xi^3$, $\beta\xi^4$ are the roots of $x^4 + 2x^3 + x^2 + 2x + 1$. Therefore, the orbit $\mathbf{O}_1$ corresponds to the polynomial $x+1$ while the orbit $\mathbf{O}_2$ corresponds to the polynomial $x^4 + 2x^3 + x^2 + 2x + 1$ in (17).

Let $\mathscr{C}$ be the $(2,2)$-QT code of length 30 over $\mathbb{F}_3$ and let the generator of its corresponding $\mathbb{R}$-submodule of $\mathbb{R}^2$ be $(G_1(x), G_2(x))$. Then $\mathscr{C}$ can be decomposed as direct sum of a code over J_1 and another code over J_2.

For the codeword $(G_1(x), G_2(x)) \in \mathscr{C}$, $\hat{G}_1, \hat{G}_2$ are two matrices of size 3×5 as defined in Eq. (12), where

$$\hat{G}_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3 & 1 + (2\xi)^3 & 1 + 2(2\xi)^2 & 1 + (2\xi) \\ 2 & (2\xi)^3 & 2\xi & 1 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3 & 2(2\xi)^2 \end{bmatrix},$$

and

$$\hat{G}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 2 & 1 + (2\xi) + (2\xi)^3 & 1 + (2\xi) + 2(2\xi)^2 & 2 + 2(2\xi) + (2\xi)^2 & 2 + 2(2\xi) + 2(2\xi)^3 \end{bmatrix}.$$

Let $\mathscr{C}_1$ be the J_1-linear code of length 2 with the generator

$$\left(2u^2, u + 2u^2\right)$$

over J_1 and let $\mathscr{C}_2$ be the J_2-linear code of length 2 with the generator

$$\left(\left(2 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3\right)u + \left((2\xi)^3\right)u^2, \left(1 + (2\xi) + (2\xi)^3\right)u^2\right)$$

over J_2. Then $\mathscr{C} \simeq \mathscr{C}_1 \oplus \mathscr{C}_2$.

The following example shows the construction of $\mathscr{C}$ from $\mathscr{C}_1$ and $\mathscr{C}_2$ where $\mathscr{C}$, $\mathscr{C}_1$ and $\mathscr{C}_2$ are as in Example 3.

Example 4. Given the generator $(2u^2, u + 2u^2) \in \mathscr{C}_1$, its associated matrix $\tilde{\mathbf{x}}_1$ defined as in (15) is

$$\tilde{\mathbf{x}}_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 2 & 2 \end{bmatrix}.$$

The matrix $\tilde{x}_2$ associated to the generator

$$\left(\left(2 + 2(2\xi) + (2\xi)^2 + 2(2\xi)^3\right)u + \left((2\xi)^3\right)u^2, \left(1 + (2\xi) + (2\xi)^3\right)u^2\right) \in \mathscr{C}_2$$

is

$$\tilde{\mathbf{x}}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}^T.$$

Then

$$\mathbf{x} = \begin{bmatrix} 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}^T.$$

By Theorem 7, the matrix A is given as follows

$$\begin{bmatrix}
2 & 2 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 1 \\
0 & 2 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 \\
1 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 \\
0 & 1 & 2 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 2 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 2 \\
2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\
0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\
1 & 1 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 \\
0 & 1 & 2 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 1 & 1 & 2 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 1 \\
2 & 2 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 \\
0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 1 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2
\end{bmatrix}.$$

Then

$$A\mathbf{x} = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}^T,$$

whose columns are exactly the coefficients of $G_1(x)$ and $G_2(x)$, respectively. $(G_1(x), G_2(x))$ is the generator of the quasi-twisted code $\mathscr{C}$ in the previous example.

8. Conclusion

In this paper, we study the quasi-twisted (QT) codes both in the nonrepeated-root and repeated-root cases. Based on the factorization of the polynomial $x^\theta - \lambda$ over $\mathbb{F}_q$, the decomposition of a (λ, l)-QT code of length $l\theta$ over $\mathbb{F}_q$ is given as a direct sum of linear codes over the component rings. Furthermore, the connection between the decomposition of a QT code and that of its dual code is explicitly described. In particular, the decomposition of a self-dual QT code is given. We also study the generalized discrete Fourier transform (GDFT) and its inverse formula, which are applied to both the nonrepeated-root and repeated-root cases. Finally, by the inverse formula of GDFT, we produce a formula to construct a QT code from linear codes over rings, as shown in Example 4.

Acknowledgments

The research is partially supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03.

The author thanks her supervisor, Professor San Ling, for his supervision and guidance. She also thanks the anonymous referee for the helpful comments which improved the paper.

References

[1] N. Aydin, I. Siap, D.K. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, Des. Codes Cryptogr. 24 (3) (2001) 313–326.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.
[3] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[4] S. Ling, H. Niederreiter, P. Solé, On the algebraic structure of quasi-cyclic codes IV: repeated roots, Des. Codes Cryptogr. 38 (2) (2006) 337–361.
[5] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, Des. Codes Cryptogr. 30 (2003) 113–130.