Quantum Synchronizable Codes on Sextic Cyclotomy

Tao Wang\textsuperscript{a}, Tongjiang Yan\textsuperscript{a}, Xueting Wang\textsuperscript{a}
\textsuperscript{a} College of Science, China University of Petroleum, Qingdao 266555, Shandong, China
Email: 1409010215@s.upc.edu.cn; yantoji@163.com; s20090013@s.upc.edu.cn
May 11, 2021

Abstract
Quantum synchronizable codes are kinds of quantum error-correcting codes that can not only correct the effects of quantum noise on qubits but also the misalignment in block synchronization. In this paper, the quantum synchronizable codes constructed are CSS quantum error-correcting codes whose synchronization capabilities reach the upper bound. And we use cyclic codes gained by sextic cyclotomic classes to construct two classes of quantum synchronizable codes. Moreover, the quantum synchronizable codes are possess good error-correcting capability towards bit error and phase error, since the cyclic codes we used are optimal or almost optimal.

Index Terms. Quantum synchronizable codes, Cyclic codes, Cyclotomic classes.

1 Introduction

In the last two decades, quantum information theory has made great progress in quantum information and quantum communication, especially in quantum error-correcting codes \[15, 16\]. Since the properties of quantum state, quantum error-correcting codes have some advantages that classical error-correcting codes do not have. The theory and construction of quantum error-correcting codes have extensively been studied \[4, 5, 9, 17, 18\]. However, quantum error-correcting codes tend to just focus the simplest Pauli errors $I, X, Y, Z$, which roughly corresponds to additive noise in classical encoding theory.

Moreover, as a type of error in block synchronization, misalignment can also cause catastrophic failure in quantum information transmission. This kind of error occurs because the information processing device misidentifies the boundaries of an information stream. For instance, suppose that the quantum information can be expressed by an ordered sequence of information block and each chunk of information is encoded into a block of consecutive three qubits in a stream of qubit $|q_i\rangle$. If three blocks of information are encoded, we have 9 ordered qubits $(|q_0\rangle|q_1\rangle|q_2\rangle|q_3\rangle|q_4\rangle|q_5\rangle|q_6\rangle|q_7\rangle|q_8\rangle)$ in which each of the three blocks $(|q_0\rangle|q_1\rangle|q_2\rangle), (|q_3\rangle|q_4\rangle|q_5\rangle)$ and $(|q_6\rangle|q_7\rangle|q_8\rangle)$ forms an information chunk. Suppose the synchronization system was established at the beginning of information transmission, but synchronization may be lost during the quantum communications or quantum computations. This type of error occurs when the receiver incorrectly locates the boundary of each block of data by a certain number of
positions towards the left or right. For example, the receiver wrongly read out \((|q_6\rangle|q_9\rangle|q_7\rangle)\) instead of the correct information chunk \((|q_6\rangle|q_7\rangle|q_8\rangle)\). \[1\] [6] give more details.

As the subclass of quantum error-correcting codes, quantum synchronizable codes mainly function is to correct the errors caused by quantum noise and block synchronization in the process of quantum information transmission. In order to ensure information security, it is of great significance to study the construction of quantum synchronizable codes \[7\] [8]. In 2013, Y. Fujiwara [6] proposed the framework of quantum block synchronization and gave the first example of quantum synchronizable codes with standard quantum error correction capability and a general construction framework. In 2014, Xie Yixuan [20] proposed to use quadratic residual codes and hypercodes to construct quantum synchronizable codes with Mersenne prime numbers. The simple construction of the quantum synchronizable codes given by them can make its synchronization ability reach the upper limit. It also have been proved that it has good error correction performance. After that, quantum synchronizable codes were further studied in \[3\] [12] [13] [14] [19].

In this work, we propose a new method to construct the quantum synchronizable codes from the cyclic codes obtained by using sextic cyclotomic classes over \(F_q\). This paper is arranged as follows. In section 2 we review some general conclusions of cyclic codes and give some knowledge of sextic cyclotomic classes. In section 3 we briefly review the construction of quantum synchronizable codes and the process of synchronization recovery for quantum information. Section 4 construct some dual-containing cyclic codes and their augmented codes. In section 5 we constructed two classes quantum synchronizable codes and discuss their error correction capabilities. Finally, Concluding remarks are given in section 6.

2 Preliminaries

2.1 Cyclic codes and dual codes

Let \(F_q\) be a finite field, where \(q\) is a prime power. A linear code \(C = [n, k, d]_q\) is a \(k\)-dimensional subspace of the \(n\)-dimensional vector space \(F_q^n\) such that \(\min\{\operatorname{wt}(v) : v \in C, v \neq 0\} = d\), where \(\operatorname{wt}(v)\) is number of nonzero elements in \(v\). A linear code \(C = [n, k, d]_q\) is optimal (almost optimal) means that the code reaches some bound in \[9\]. A linear code \(C = [n, k, d]_q\) over \(F_q\) is a cyclic code if any codeword \(c = (c_0, c_1, \ldots, c_{n-1}) \in C\) implies \((c_t, c_{t+1}, c_{t+2}, \ldots, c_{n-t-1}) \in C\), where \(t\) is a nonnegative integer. If each codeword in \(C\) can be identified with \(I(C) = \{c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} | (c_0, c_1, c_2, \ldots, c_{n-1}) \in C\}\), then \(I(C)\) can be regarded as an ideal of the principal ring \(F_q[x]/(x^n - 1)\). Hence the cyclic code \(C\) can be generated by the monic polynomial \(g(x)\) of degree \(n - k\), \(g(x)\) is called generator polynomial of \(C\). Moreover, \(g(x)\) is a monic divisor of \(x^n - 1\). Let \(C = \langle g(x) \rangle\). Then the set of codewords of cyclic code \(C\) can be written as \(C = \{m(x)g(x)|m(x) \in F_q[x],\ \deg (m(x)) < k\}\).

The Euclidean inner product between two codewords \(x = (x_0, x_1, \ldots, x_{n-1})\) and \(y = (y_0, y_1, \ldots, y_{n-1})\) is defined by \((x, y) = \sum_{i=0}^{n-1} x_i y_i\). For a linear code \(C\) with length \(n\), the code \(C^\perp = \{x \in F(q)^n | (x, c) = 0, \forall c \in C\}\) is called an Euclidean dual code of \(C\). The dimension of \(C^\perp\) is \(\operatorname{dim}(C^\perp) = n - \operatorname{dim}(C) = n - k\). And the dual of a cyclic code is also a cyclic code \[11\].

Let \(g(x)\) be the generator polynomial of a cyclic code \(C\). It follows that \(g(x)|(x^n - 1)\). Let \(h(x) = \]}
Then \( h(x) \) is the parity check polynomial of cyclic code \( C \). Since the degree of the generator polynomial \( g(x) \) is \( \deg(g(x)) = n - k \), the degree of parity check polynomial \( h(x) \) is \( \deg(h(x)) = k \).

Then the generator polynomial of \( C^\perp \) has the form:

\[ g^{-1}(x) = \tilde{h}(x) = h(0)^{-1}x^k h(\frac{1}{x}) \tag{1} \]

where \( \tilde{h}(x) \) is called the reciprocal polynomial of \( h(x) \). Let \( C^\perp = (g^{-1}(x)) \).

Let \( C_1 = (g_1(x)) \) be a cyclic code with parameters \([n, k_1]\), and \( C_2 = (g_2(x)) \) be a cyclic code with parameters \([n, k_2]\), where \( k_1 < k_2 \). Then, if \( C_1 \subseteq C_2 \), \( C_2 \) is said to be \( C_1 \)-containing, and \( C_1 \) is called the subcodes of \( C_2 \). If \( C_2^\perp \subseteq C_2 \), \( C_2 \) is called dual-containing.

Let \( C_1 \subseteq C_2 \), then the generator polynomial \( g_2(x) \) can divide any codeword of \( C_1 \), i.e., for any \( c(x) \in C_1 \), there must exist a polynomial \( f_c(x) \) in \( F_q[x] \) such that \( c(x) = f_c(x)g_2(x) \). If \( f(x) = \frac{g_1(x)}{g_2(x)} \), then \( f(x) \in F_q[x] \) has degree \( k_2 - k_1 \).

### 2.2 Cyclotomic classes

Let \( n = 6f + 1 \) be an odd prime and \( \gamma \) be a fixed primitive element of \( F_n \). Then the sextic cyclotomic classes \( C_0^{(6,n)}, C_1^{(6,n)}, \ldots, C_5^{(6,n)} \) of \( F_n \) by

\[ C_i^{(6,n)} = \{ \gamma^{6j+i} | 0 \leq j \leq \frac{n-1}{6}-1 \}, \]

where \( 0 \leq i \leq 5 \). Trivially \( C_i^{(6,n)} = \gamma^i C_0^{(6,n)} \). The number of elements in \( C_i^{(6,n)} \) denoted by \( |C_i^{(6,n)}| \).

So for arbitrary integers \( i, j \) satisfy \(|i| \leq j \leq 5 \), we have \( |C_i^{(6,n)}| = |C_j^{(6,n)}| \), and \( F_n^* = \bigcup_{i=0}^5 C_i^{(6,n)} \), \( C_i^{(6,n)} \cap C_j^{(6,n)} = \emptyset \), where \( F_n^* = F_n \setminus \{0\} \).

**Lemma 1** Let \( n = 12m + 7 \) be an odd prime, where \( m \) is a nonnegative integer. Then

\[ (a) \ C_0^{(6,n)} = -C_3^{(6,n)}, \quad (b) \ C_1^{(6,n)} = -C_4^{(6,n)}, \quad (c) \ C_2^{(6,n)} = -C_5^{(6,n)}. \tag{2} \]

**Proof.** Case (a) Let \( \gamma \) be a fixed primitive element of \( F_p \). It is readily apparent that \(-1 = \gamma^\frac{n-1}{2} = \gamma^{6m+3} \in C_3^{(6,n)} \). Thus for any \( a \in C_3^{(6,n)} \), it has a form of expression \( a = \gamma^{6j+3} \) where \( j = 0, 1, ..., 2m \).

Furthermore, \(-a = \gamma^{6m+3+6j+3} = \gamma^{6(m+j+1)} \in C_0^{(6,n)} \). So, \(-C_3^{(6,n)} \subseteq C_0^{(6,n)} \). Since \( |C_3^{(6,n)}| = |C_0^{(6,n)}| \), we get \(-C_3^{(6,n)} = C_0^{(6,n)} \).

Similarly, the other conclusions can be proved like Case (a). \( \blacksquare \)

From now on, we let \( q \in C_0^{(6,n)} \), and \( \eta \) be a \( n \)-th primitive root of unity over \( F_{q^{ord_n(q)}} \), where \( ord_n(q) \) is the multiplicative order of \( q \) modulo \( n \). It is known that the polynomials

\[ c_i^{(6,n)}(x) = \prod_{j \in C_i^{(6,n)}} (x - \eta^j), \tag{3} \]

for \( i = \{0, 1, 2, 3, 4, 5\} \) belong to \( F_q[x] \), due to \( q \in C_0^{(6,n)} \). Thus, we can get the factorization of \( x^n - 1 \) as

\[ x^n - 1 = (x - 1) \prod_{i=0}^5 c_i^{(6,n)}(x). \]
3 Quantum synchronizable codes

3.1 Coding scheme

An $[[n, k]]$ quantum error-correcting code is a coding theory that encodes $k$ logical qubits into $n$ physical qubits. As in classic linear code, $n$ and $k$ are the length and dimension of the code, respectively. Quantum error-correcting codes tend to just correct the effects of bit error and phase error caused by Pauli operators. Quantum synchronizable code $(c_1, c_r) - [[n, k]]$ is a encode scheme that corrects not only bit errors and phase errors but also misalignment up to the left by $c_1$ qubits and up to the right by $c_r$ qubits, where $c_1$ and $c_r$ are nonnegative integers.

We provide here construction of quantum synchronizable codes by applying the method discovered by Fujiwara [5 8]. Let $f(x) \in F_q[x]$ be a polynomial over $F_q$ and $f(0) = 1$. The order $\text{ord}(f(x))$ of the polynomial $f(x)$ is the smallest integer $a$ such that $f(x)(x^a - 1)$ over $F_q[x]$.

**Lemma 2** Let $C_1 = \langle g_1(x) \rangle$ and $C_2 = \langle g_2(x) \rangle$ be two cyclic code of parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, with $k_1 > k_2$ respectively such that $C_2 \subset C_1$ and $C_2^\perp \subseteq C_2$. Define $f(x)$ of degree $k_1 - k_2$ to be the quotient of $\frac{g_2(x)}{g_1(x)}$ over $F_q[x]/x^n - 1$. For any pair of nonnegative integers $c_1$, $c_r$ satisfying $c_1 + c_r < \text{ord}(f(x))$, then exist a quantum synchronizable code $(c_1, c_r) - [[n + c_1 + c_r, 2k_2 - n]]$ that corrects at least up to $\left\lfloor \frac{c_1 - 1}{2} \right\rfloor$ bit errors and $\left\lfloor \frac{c_r - 1}{2} \right\rfloor$ phase errors, and misalignment up to the left by $c_1$ qubits and up to the right by $c_r$ qubits.

The quantum synchronizable code described in Lemma 2 requires a pair of cyclic codes $C_1$, $C_2$ of the same length, and dimension $k_1 > k_2 > \left\lceil \frac{n}{2} \right\rceil$. A misalignment of $\delta$ qubits can be recovered of $-c_1 < \delta < c_r$, where minus means that a misalignment occurs towards the left, and the maximum capability of quantum synchronization error is given by $c_1 + c_r < \text{ord}(f(x))$. To get a good quantum synchronizable code, cyclic codes with good minimum distance are required, while ensuring $\text{ord}(f(x))$ to be as large as possible.

3.2 Encoding

Since $\dim(C_2) = k_2$, $\dim(C_2^\perp) = n - k_2$ and $C_2^\perp \subseteq C_2$. Assuming that $c$, $c' \in C_2$ are two codewords of $C_2$. Define an equivalence relation $\equiv$ on $C_2$, $c \equiv c' \iff c - c' \in C_2^\perp$. Moreover, it is not difficult to see that the equivalence class $\hat{c}$ determined by a codeword $c \in C_2$ is equal to $\hat{c} = c + C_2^\perp := \{c + x | x \in C_2^\perp\}$. Thus, the coset $\hat{c}$ form a partition of $C_2$, and the dimension of coset is $\dim(\hat{C_2}/C_2^\perp) = 2k_2 - n$. Hence, the number of cosets is $q^{2k_2-n}$. Therefore, the quantum synchronizable codes encodes $2k_2 - n$ logical qubits. Let the representative of cosets denote $\mathcal{B} = \{b_i(x) | 0 \leq i \leq q^{2k_2-n}\}$. Then the set

$$V = \{|C_2^\perp + b_i(x) + g_1(x)| b_i(x) \in \mathcal{B}\}$$

of $q^{2k_2-n}$ quantum states forms an orthogonal basis of a vector space of dimension $q^{2k_2-n}$, where

$$|C_2^\perp + b_i(x) + g_1(x)| = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{c_i^\perp(x) \in C_2^\perp} |c_i^\perp(x) + b_i(x) + g_1(x)|.$$
By using the standard encoder for Calderbank-Shor-Steane (CSS) codes, we encode an arbitrary $q^{2k-2-n}$-qubit state $|\psi\rangle$ into $n$-qubit state $|\psi\rangle_{\text{enc}} = \sum_i \alpha_i |v_i\rangle$, where $v_i \in V$. Moreover, let $c_l$, $c_r$ be nonnegative integers such that $c_l + c_r < \text{ord} (f(x))$, ancilla qubits used to attach to the left and right of the original state respectively and then applying CNOT gate, we finally obtain an $n + c_l + c_r$-qubit state $|\Psi\rangle_{\text{enc}} = |0\rangle^{\otimes c_l} |\psi\rangle_{\text{enc}} |0\rangle^{\otimes c_r} = \sum_i \alpha_i |l_i, v_i, r_i\rangle$, where $l_i$ and $r_i$ are the last $c_l$ and the first $c_r$ positions of the vector $v_i$, respectively. Hence, $|\Psi\rangle_{\text{enc}}$ is ready to transmit.

3.3 Synchronization recovery

Here we introduce the procedures for error correction and synchronization recovery. [4] gives more details.

Suppose that the receiver gathered qubits of one block length, that is, consecutive $n + c_l + c_r - 1$ qubits, and correct bit errors, phase errors and misalignment if necessary. Define block frame $T = (t_0, t_1, \ldots, t_{n+c_l+c_r-1})$ of the encoded state. If no misalignment occurred, $T$ forms a properly aligned block encoded as $|\Psi\rangle_{\text{enc}}$. Now, we assume that $T$ may be misaligned by $\delta$ qubits to the right, where $-c_l < \delta < c_r$. When $\delta$ is negative, it means the misalignment occurs to the left by $|\delta|$ qubits.

Define a window frame $W = (w_{c_l}, w_{c_l+1}, \ldots, w_{c_l+n-1})$. The device first focus on consecutive $n$ qubits in the middle of $T$, then $W = (t_{c_l}, t_{c_l+1}, \ldots, t_{c_l+n-1})$. Assume misaligned by $\delta$ occurs, this set of qubits is $W = (t_{\delta+c_l}, t_{\delta+c_l+1}, \ldots, t_{\delta+c_l+n-1})$.

Let operator $E$ be the $n+c_l+c_r$-fold tensor product of linear combinations of Pauli errors. Therefore the corrupted encoded state is:

$$E |\Psi\rangle_{\text{enc}} = \sum_i \alpha_i (-1)^{(l_i, v_i, r_i)} e_p |(l_i, v_i, r_i) + e_b\rangle,$$

where $e_b$ and $e_p$ represent bit and phase error respectively.

The receiver corrects errors in two steps, first corrects bit errors on $W$ and then detects misalignment. Let $H_{C_1}$ be the $(n - k_1) \times n$ parity-check matrix of $C_1$. As in the standard decoding of CSS code, $E |\Psi\rangle_{\text{enc}} |0\rangle^{\otimes n-k_1} \rightarrow E |\Psi\rangle_{\text{enc}} |H_{C_1} e_b\rangle$, where $H_{C_1} e_b$ is the error syndrome of the window $W$. If at most $\lfloor \frac{n}{k_1} \rfloor$ bit errors in $W$, applying $X$ Pauli operators to the qubits can eliminate all bit errors in $W$.

The next step is the procedure of synchronization recovery. Since $C_2^\perp \subseteq C_2 \subset C_1$, the generator polynomial $g_1(x)$ divides every elements in $V$ given in [4] which implies

$$|c_i b_i(x) + g_1(x))| = |v_1(x) f(x) g_1(x) + v_2(x) f(x) g_1(x) + g_1(x)|,$$

for some polynomial $v_1(x)$ and $v_2(x)$ of degree less than $k_2$. Because of the misalignment and window farm $W$ contains a cyclic shift coefficient vectors of the correct polynomials. Thus, if a misalignment of $\delta$ qubits occurs, the corrupted state has the form $|x^\delta (c_i + b_i(x) + g_1(x))\rangle$. So the quotient of $W$ divided by $g_1(x)$ is $x^\delta (v_1(x) f(x) + v_2(x) f(x) + 1)$. Dividing this quotient by $f(x)$ gives remainder of $x^\delta$:

$$\frac{x^\delta (c_i + b_i(x) + g_1(x))}{g_1(x) f(x)} \equiv x^\delta \mod f(x).$$

Thus, if $c_l + c_r < \text{ord} (f(x))$, the synchronization error $\delta$ is uniquely determined. From now on, we know how many qubits the original frame $T$ is misaligned. By cyclicly shifting $T$ to recover the correct block of qubits. And any bit and phase errors can be correct as the standard CSS code does.
4 Cyclic codes from the sextic cyclotomic classes

In this section, we gave some dual-containing cyclic codes obtained by the sextic cyclotomic classes. Then we discussed their minimum distances. And give some optimal cyclic code finally.

4.1 Dual-containing Codes

Let $C_i$ be the cyclic code by generated $g_i^{(6,n)}(x)$ and $\tilde{C}_i$ be the cyclic code by generated $(x - 1)g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x)g_{i+4}^{(6,n)}(x)g_{i+5}^{(6,n)}(x)$, for any $i \in \{0, 1, 2, 3, 4, 5\}$.

**Lemma 3** Let $n = 12m + 7$ be an odd prime, where $m$ is a nonnegative integer. Then we have the following conclusions of cyclic codes $C_i$ and $\tilde{C}_i$:

(a) $C_i^\perp = C_i,$  (b) $C_i^\perp \subset C_i$

**Proof.** By (1), the reciprocal polynomial of $g_i^{(6,n)}(x)$ is

$$g_i^{(6,n)}(x) = \left(\frac{g_i^{(6,n)}(0)}{x^{\deg(g_i^{(6,n)})}}\right)g_i^{(6,n)}(x^{-1}),$$

where $g_i^{(6,n)}(x)$ is defined in (3). It follows that

$$g_i^{(6,n)}(x) = (x - \eta^{e_1})(x - \eta^{e_2})\ldots(x - \eta^{e_{2m+1}}),$$

where $C_i^{(6,n)} = \{e_i | 1 \leq j \leq 2m + 1\}$. Then

$$g_i^{(6,n)}(x) = (-\eta^{e_1})^{-1}(-\eta^{e_2})^{-1}\ldots(-\eta^{e_{2m+1}})^{-1}x^{2m+1}(x^{-1} - \eta^{e_1})(x^{-1} - \eta^{e_2})\ldots(x^{-1} - \eta^{e_{2m+1}})

= (x - \eta^{-e_1})(x - \eta^{-e_2})\ldots(x - \eta^{-e_{2m+1}}).$$

According to Lemma [1] it is readily seen that

$$g_i^{(6,n)} = g_{i+3}^{(6,n)}(x),$$

for any $i \in \{0, 1, 2, 3, 4, 5\}$. The parity check polynomial of $C_i$ is

$$h(x) = \left(\frac{x^n - 1}{g_i^{(6,n)}(x)}\right) = (x - 1) \prod_{j \in F_{i}^{*} \setminus C_{i}^{(6,n)}} (x - \eta^j).$$

And by (1) and (3),

$$\tilde{h}(x) = (x - 1)g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x)g_{i+4}^{(6,n)}(x)g_{i+5}^{(6,n)}(x).$$

Then $C_i^\perp = \langle \tilde{h}(x) \rangle$. According to the definition of $\tilde{C}_i$, we get $C_i^\perp = \tilde{C}_i$. Moreover, due to $g_i^{(6,n)}(x)|\tilde{h}(x)$, we obtain $C_i^\perp \subset C_i$. ■

In addition, let $D_i$ be the cyclic code by generated $g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x)$, and $\tilde{D}_i$ be the cyclic code with generator polynomial $(x - 1)g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+4}^{(6,n)}(x)$ for any $i \in \{0, 1, 2, 3, 4, 5\}$. We have the following results, obviously.
Lemma 4 Let \( n = 12m + 7 \) be an odd prime, where \( m \) is a nonnegative integer. Then the conclusions of cyclic codes \( D_i \) and \( D_i \) are

\[
\text{(a) } D_i^\perp = \bar{D}_i, \quad \text{(b) } D_i^\perp \subset D_i.
\]

Proof. The proof is straightforward from the Lemma 3. \( \square \)

Example 1 Let \( n = 12m + 7 \) and \( q \in C_0^{(6,n)} \). Table 1 gives some examples about cyclic codes and their duals, and some them are optimal or almost optimal. All computations have been done by MAGMA [2].

| Codes \( C_i \) or \( D_i \) | Duals \( C_i^\perp \) or \( D_i^\perp \) | Optimal or almost optimal [10] |
|-----------------------------|--------------------------------|-------------------------------|
| \( C_i = [19, 16, 3]_7 \)  | \( C_i^\perp = [19, 3, 15]_7 \) | Both optimal [10]             |
| \( D_i = [19, 13, 5]_7 \)   | \( D_i^\perp = [19, 6, 12]_7 \) | \( D_i \) almost optimal, \( D_i^\perp \) optimal [10] |
| \( C_i = [31, 26, 3]_2 \)   | \( C_i^\perp = [31, 5, 16]_2 \) | Both optimal [10]             |
| \( D_i = [31, 21, 5]_2 \)   | \( D_i^\perp = [31, 10, 12]_2 \) | Both optimal [10]             |

Table 1: Dual-containing cyclic codes \( C_i \) and \( D_i \)

4.2 Augmented cyclic codes

A cyclic code \( C' = \langle g'(x) \rangle \) is called augmented cyclic code of \( C = \langle g(x) \rangle \) if \( C \subset C' \). It follows that \( g'(x) | g(x) \). To obtain the augmented cyclic codes of \( C_i \) and \( D_i \), we need the concept of cyclotomic cosets. For any nonnegative \( s \) and \( n \), the cyclotomic cosets \( C(s,n) \) of \( s \) modulo \( n \) over \( \mathbb{F}_q \) is the set

\[
C(s,n) = \{ sq^i \mod n \mid i \in \mathbb{N} \}.
\] (8)

Let \( \eta \) be a primitive \( n \)-th root of unity in some extension field of \( \mathbb{F}_q \), where \( q \in C_0^{(6,n)} \). Then the unique irreducible minimal polynomial of \( \eta^s \) over \( \mathbb{F}_q[x] \) is \( M_s(x) = \prod_{i \in C(s,n)} (x - \eta^i) \in \mathbb{F}_q[x] \).

Theorem 1 Let cyclic code \( C_i = \langle g_i^{(6,n)}(x) \rangle \) be defined above. If the size of \( C(s,n) \) is \( |C(s,n)| = \ell \), then the generator polynomial \( g_i^{(6,n)} \) can be expressed as the product of \( t = \frac{n-1}{6\ell} \) irreducible polynomials of degree \( \ell \) over \( \mathbb{F}_q[x] \) as follows:

\[
g_i^{(6,n)} = \prod_{j=1}^{t} M_{i_j}(x),
\]

where the degree of \( M_{i_j} \) is \( \deg(M_{i_j}(x)) = \ell \), for all \( i_j \).

Proof. As \( n = 12m + 7 \) is an odd prime and \( |C(s,n)| = \ell \), then \( |C(s,n)| = \ell \) for any integers \( s \in \{1, 2, ..., n-1\} \). Since \( q \in C_0^{(6,n)} \), it is known that \( C_i^{(6,n)} = \bigcup_{j=1}^{t} C(i_j,n) \), where \( i_1, i_2, ..., i_t \in \{1, 2, ..., n-1\} \) are some integers. Moreover, we have \( t = \frac{|C^{(6,n)}|}{|C(s,n)|} = \frac{n-1}{6\ell} \). \( \square \)

7
Example 2 Consider the sextic cyclotomic classes modulo \( n = 127 \)

\[
C_0^{(6,127)} = \{1, 47, 50, 64, 87, 25, 32, 107, 76, 16, 117, 38, 8, 122, 19, 4, 61, 73, 2, 94, 100\},
\]
\[
C_1^{(6,127)} = \{6, 28, 46, 3, 14, 23, 65, 7, 75, 96, 67, 101, 48, 97, 114, 24, 112, 57, 12, 56, 92\},
\]
\[
C_2^{(6,127)} = \{36, 41, 22, 18, 84, 11, 9, 42, 69, 68, 21, 98, 34, 74, 49, 17, 37, 88, 72, 82, 44\},
\]
\[
C_3^{(6,127)} = \{89, 119, 5, 108, 123, 66, 54, 125, 33, 27, 126, 80, 77, 63, 40, 102, 95, 20, 51, 111, 10\},
\]
\[
C_4^{(6,127)} = \{26, 79, 30, 13, 103, 15, 70, 115, 71, 35, 121, 99, 81, 124, 113, 104, 62, 120, 52, 31, 60\},
\]
\[
C_5^{(6,127)} = \{29, 93, 53, 78, 110, 90, 39, 55, 45, 83, 91, 86, 105, 109, 124, 116, 118, 85, 58, 59, 106\}.
\]

Let \( \gamma \) be the fixed primitive element of \( F_{127} \). Then \( q = \gamma^{6K} \in C_0^{(6,127)} \), where \( K = \{0, 1, \ldots, 20\} \). The order of \( q \) modulo \( n \) is \( |q| = |\gamma^{6K}| = \frac{|\gamma^{|K|}|}{\gcd(|K|, 127)} \). For \( K = 3 \), \( \gamma = 39 \), we have \( q = 39^{18} = 2 \) and \( |q| = \frac{126}{\gcd(126, 18)} = 7 \) over \( F_{127} \). By (6), we have

\[
C_{(1,127)} = \{1, 2, 4, 8, 16, 32, 64\}, \quad C_{(47,127)} = \{47, 94, 61, 122, 117, 107, 87\},
\]
\[
C_{(19,127)} = \{19, 38, 76, 25, 50, 100, 73\}.
\]

Thus \( C_0^{(6,127)} = C_{(1,127)} \cup C_{(19,127)} \cup C_{(47,127)} \), which is equivalent to \( g_0^{(6,127)} = M_1(x)M_{19}(x)M_{47}(x) \). And in this way, the following equations can be drawn easily.

\[
C_1^{(6,127)} = C_{(3,127)} \cup C_{(7,127)} \cup C_{(23,127)}, \quad C_2^{(6,127)} = C_{(9,127)} \cup C_{(11,127)} \cup C_{(21,127)},
\]
\[
C_3^{(6,127)} = C_{(5,127)} \cup C_{(17,127)} \cup C_{(31,127)}, \quad C_4^{(6,127)} = C_{(13,127)} \cup C_{(15,127)} \cup C_{(33,127)},
\]
\[
C_5^{(6,127)} = C_{(29,127)} \cup C_{(43,127)} \cup C_{(55,127)}.
\]

It is easy to deduce that the augmented cyclic code \( C_i \) (or \( D_i \)) can be obtained by removing one or more irreducible factors of \( g_i^{(6,n)} \) (or \( g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x) \)). It is also notable that any augmented code \( C \) obtained by this way is also dual-containing. Furthermore, we have the following results.

Lemma 5 Let \( n = 12m + 7 \) be an odd prime, where \( m \) is a natural number. And \( C_i, D_i \) be the cyclic codes defined above for any \( i \in \{0, 1, 2, 3, 4, 5\} \). Then, the following conclusions hold.

(a) If \( C = \left\langle \frac{g_i^{(6,n)}}{\prod_{j \neq i} A_j(x)} \right\rangle \), then \( C_i \subset C \), where \( A \) is some proper subset of \( \{i_1, i_2, ..., i_t\} \).

(b) If \( D = \left\langle \frac{g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x)}{\prod_{j \neq i} A_j(x)} \right\rangle \), then \( D_i \subset D \), where \( B \) is some proper subset of \( \{i_1, i_2, ..., i_t\} \cup \{(i+1), (i+1)_1, (i+1)_2, ..., (i+1)_t\} \cup \{(i+2), (i+2)_1, (i+2)_2, ..., (i+2)_t\} \).

Proof. The results come from the definition of dual-containing code. ■
5 Quantum synchronizable codes from the cyclic codes obtained

According to Lemma 2, our main goal is to find a pair of cyclic codes $C_1$ and $C_2$ of the same length and dimensions $k_1 > k_2 > \left\lceil \frac{n}{2} \right\rceil$, and satisfies the chain condition $C_2^2 \subseteq C_2 \subset C_1$. In this section, we give construct a class of quantum synchronizable codes by the cyclic codes obtained above. To get a good quantum synchronizable code, the cyclic codes $C_1$ and $C_2$ are optimal or almost optimal. And analyzing the error-correcting capability of these quantum synchronizable codes.

5.1 Maximum misalignment tolerance

In the context of quantum synchronizable codes, we would like to maximize $\text{ord}(f(x))$, where $f(x)$ is the quotient in Lemma 2. As $f(x)(x^n - 1)$, we know that the $\text{ord}(f(x))$ is some divisor of $n$. Since $n = 12m + 7$ is an odd prime, $\text{ord}(f(x))$ must be $n$. So, the tolerance capability of quantum synchronizable codes constructed is upper bounded by its length $n$. We now give our main theorem.

Based on the cyclic code $C_i$ we constructed in Lemma 3, we can obtain a class of quantum synchronizable codes as follows, whose synchronizability capabilities attain the upper bound.

Theorem 2 Let $n = 12m + 7$ be an odd prime, $t = \frac{n}{2l} \geq 2k + 1$ ($k$ is a positive integer) and $q \in C_0^{(6,n)}$, where $q^t \equiv 1 \mod n$. For any nonnegative integers $c_l$ and $c_r$ satisfying $c_l + c_r < n$, then there exist a quantum synchronizable code with parameters $(c_l, c_r) = \left\lceil \frac{n + c_l + c_r}{2z\ell + 2n + 1} \right\rceil q$, where $z$ is a nonnegative integer such that $0 \leq z \leq \ell - 2 = \frac{n-12\ell-1}{6}$. 

Proof. Since $n = 12m + 7$ is an odd prime, then $|C_i^{(6,n)}| = \frac{n-1}{6} = 2m + 1$. Due to $|C_{(s,n)}| = \ell$ for any $s \in \{1, 2, ..., n-1\}$, and $\ell|(2m+1)$, it is obvious that cyclic code $C_i = \langle g_i^{(6,n)}(x) \rangle$ has augmented codes if and only if $g_i^{(6,n)}(x)$ has at least $2k+1$ irreducible factors over $F_q$, where $k$ is a positive integer. So we let $t = \frac{n}{2l} \geq 2k + 1$. According to (a) in Lemma 3, cyclic code $C_M = \langle M_i(x) \rangle$ has a augmented code $C = [n, n - \text{ord}(M_i(x))] = \left[n, n - \left(\frac{n}{6} - |A|\ell\right)\right] = \left[n, \frac{5n+1}{6} + |A|\ell\right]$, where $|A|$ is the size of the set $A$. Taking a set $A'$ such that $A \subset A' \subset \{i_1, i_2, ..., i_s\}$, then we can get cyclic code $C' = \left[n, \frac{5n+1}{6} + |A'|\ell\right]$ and $C \subset C'$. Let $|A| = z$, then $0 \leq z \leq \ell - 2 = \frac{n-12\ell-1}{6}$. Furthermore, we can obtain quantum synchronizable code with parameters $(c_l, c_r) = \left\lceil \frac{n + c_l + c_r}{2z\ell + 2n + 1} \right\rceil q$, by Lemma 2 where $c_l + c_r < n$.

Moreover, we can also construct the other class of quantum synchronizable codes whose synchronizability capabilities reach the upper bound, by using cyclic codes $D_i$ and their augmented codes.

Theorem 3 Let $n = 12m + 7$ be an odd prime, $t = \frac{n}{2l} \geq 2k + 1$ ($k$ is a positive integer) and $q \in C_0^{(6,n)}$, where $q^t \equiv 1 \mod n$. For any nonnegative integers $c_l$ and $c_r$ satisfying $c_l + c_r < n$, then there exist a quantum synchronizable code with parameters $(c_l, c_r) = \left\lceil \frac{n + c_l + c_r}{2z\ell + 2n + 1} \right\rceil q$, where $z$ is a nonnegative integer such that $0 \leq z \leq \ell - 2 = \frac{n-12\ell-1}{6}$. 

Proof. Since $n = 12m + 7$ is an odd prime, then $|C_i^{(6,n)}| = \frac{n-1}{6} = 2m + 1$. Due to $|C_{(s,n)}| = \ell$ for any $s \in \{1, 2, ..., n-1\}$, and $\ell|(2m+1)$, it is obvious that cyclic code $D_i = \langle g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x) \rangle$ has
augmented codes if and only if \( g^{(6,n)}_{i+2}(x) \) \((j \in \{0, 1, 2\})\) has at least \(2k + 1\) irreducible factors over \( F_2 \), where \( k \) is a positive integer. So we let \( t = \frac{n - 1}{6} \geq 2k + 1 \). According to (b) in Lemma 3 cyclic code \( D_M = \langle M_i(x) \rangle \) has a augmented code \( D = [n, n - \text{ord}(M_i(x))] = [n, n - (\frac{2n}{6} - |B|)] = [n, \frac{2n}{6} + |B|] \), where \( |B| \) is the size of the set \( B \). Taking a set \( B' \) such that \( B \subset B' \subset \{ (i_1, i_2, ..., i_t) \} \cup \{(i + 1)_1, (i + 1)_2, ..., (i + 1)_t \} \), then we can get cyclic code \( D' = [n, \frac{2n}{6} + |B'|] \) and \( D \subset D' \). Let \( |B| = z \), then \( 0 \leq z \leq t - 2 = \frac{n - 127}{6} \). Furthermore, we can obtain quantum synchronizable code with parameters \((c_1, c_r) = \lfloor n + c_1 + c_r, 2z \ell + 1 \rfloor \) by Lemma 2 where \( c_1 + c_r < n \). \( \blacksquare \)

Example 3 Let \( n = 127 \) and \( q = 2 \in C_0^{(6,n)} \). For convenience, we only consider the construction of quantum synchronizable codes from the cyclic code \( C_1 = \langle g^{(6,127)}_1(x) \rangle \) and its augmented cyclic code. In this case, \( 0 \leq z \leq 1 \), by Theorem 3.

If \( z = 0 \), then \( C = C_1 \) with parameters \([127, 106, 2] \) and \( C \subset C \). Iff \( z = 1 \), we can obtain \( C' = \langle g^{(6,127)}_1(x) \rangle \) with parameters \([127, 113, 2] \) and \( C' \subset C' \), where \( i \in \{3, 7, 23\} \). Furthermore, let \( C'' = \langle g^{(6,127)}_{M_1(x), M_{(2,2)}(x)} \rangle \) with parameters \([127, 120, 2] \) and \( C'' \subset C'' \) where \( i \neq j \in \{3, 7, 23\} \). Then it is obvious that \( C \subset C' \subset C'' \). By taking \( C \subset C' \) and \( C \subset C \), we have quantum synchronizable code with parameters \((c_1, c_r) = \lfloor [127 + c_1 + c_r, 85] \rfloor \) and \( c_1 + c_r < 127 \), according to Lemma 3. And taking \( C' \subset C'' \) and \( C' \subset C' \), we obtain quantum synchronizable code with parameters \((c_1, c_r) = \lfloor [127 + c_1 + c_r, 99] \rfloor \) and \( c_1 + c_r < 127 \).

6 Conclusion

We studied two classes quantum synchronizable codes from dual-containing cyclic codes obtained by sextic cyclotomic classes. Since \( n = 12m + 7 \) is an odd prime, these quantum synchronizable codes possess the highest possible tolerance against misalignment errors. By choosing some optimal dual-containing cyclic codes, the quantum synchronizable codes we get possess good error-correcting capabilities towards bit errors and phase errors.

References

[1] R. C. Bose and J. G. Caldwell. Synchronizable error-correcting codes. Information and Control, 10(6):616–630, 1967.

[2] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system I: The user language. Journal of Symbolic Computation, 24(3-4):235–265, 1997.

[3] A. E. Brouwer. Bounds on the size of linear codes. In V. S. Pless and W. Huffman, editors, Handbook of Coding Theory, chapter 4, pages 295–461. Elsevier, Amsterdam, 1998.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. Sloane. Quantum error correction via codes over GF(4). In IEEE International Symposium on Information Theory, 2002.
[5] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2), 1998.

[6] Y. Fujiwara. Block synchronization for quantum information. *Physical Review A*, 87(2), 2013.

[7] Y. Fujiwara, V. D. Tonchev, and T. W. Wong. Algebraic techniques in designing quantum synchronizable codes. *Physical Review A*, 88(1):012318, 2013.

[8] Y. Fujiwara and P. Vandendriessche. Quantum synchronizable codes from finite geometries. *IEEE Transactions on Information Theory*, 60(11):7345–7354, 2014.

[9] G. Gadioli and L. Guardia. *Quantum Error Correction: Symmetric, Asymmetric, Synchronizable, and Convolutional Codes*. Springer International Publishing, Switzerland, 2020.

[10] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, 2007. Accessed on 2021-04-19.

[11] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Fundamentals of Error-Correcting Codes, 2003.

[12] L. Li, S. Zhu, and L. Liu. Quantum synchronizable codes from the cyclotomy of order four. *IEEE Communications Letters*, 23(1):12–15, 2019.

[13] X. Li and Q. Yue. A new family of quantum synchronizable codes. *IEEE Communications Letters*, 25(2):342–345, 2021.

[14] L. Luo and Z. Ma. Non-binary quantum synchronizable codes from repeated-root cyclic codes. *IEEE Transactions on Information Theory*, pages 1461–1470, 2018.

[15] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, 2011. 10th Anniversary Edition.

[16] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493, 1995.

[17] A. Steane. Error correcting codes in quantum theory. *Physical review letters*, 77(5):793–797, 1996.

[18] A. Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 452:2551–2577, 1996.

[19] Y. Xie, L. Yang, and J. Yuan. q-ary chain-containing quantum synchronizable codes. *IEEE Communications Letters*, 20(3):414–417, 2016.

[20] Y. Xie, J. Yuan, and Y. Fujiwara. Quantum synchronizable codes from quadratic residue codes and their supercodes. In *Information Theory Workshop*, 2014.