Quantum Synchronizable Codes From Sextic Cyclotomy

Tao Wang, Xueting Wang, Qian Liu, and Tongjiang Yan
(Corresponding author: Tongjiang Yan)

College of Science, China University of Petroleum
Qingdao 266555, Shangdong, China.
Email: yantoji@163.com

(Received Oct. 22, 2021; Revised and Accepted Apr. 15, 2022; First Online May 1, 2022)

Abstract

Quantum synchronizable codes can be used to correct the effects of both quantum noise on qubits and misalignments in block synchronization. This paper contributes to constructing quantum synchronizable codes from the dual-containing cyclic codes obtained by sextic cyclotomy. We show that these quantum synchronizable codes possess good synchronization capabilities, which can always attain the upper bound, and good error-correcting capability towards bit errors and phase errors when the corresponding cyclic codes are optimal or almost optimal.

Keywords: Cyclic Codes; Quantum Synchronizable Codes; Sextic Cyclotomy

1 Introduction

In decades, quantum information theory has made great progress in quantum information and quantum communication, especially in quantum error-correcting codes [16]. However, the studies on quantum error-correcting codes tend to just focus on the simplest Pauli errors on qubits, which roughly corresponds to additive noise in classical encoding theory [3,9,17]. Meanwhile, the misalignment in block synchronization can also cause catastrophic failure in quantum information transmission. This kind of error occurs due to the fact that the information processing devices misidentify the boundaries of an information qubit 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 $|q_i\rangle$, $i \in I$, where I is an indexed set. If three blocks of information are encoded, we have 9 ordered qubits $(|q_0\rangle|q_1\rangle|q_2\rangle|q_3\rangle|q_4\rangle|q_5\rangle|q_6\rangle|q_7\rangle|q_8\rangle)$, then 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. The misalignment 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 $(|q_5\rangle|q_6\rangle|q_7\rangle)$ instead of the correct information chunk $(|q_6\rangle|q_7\rangle|q_8\rangle)$. For more details, see [4].

As a subclass of quantum error-correcting codes, quantum synchronizable codes (QSCs) can be used to prevent both the interference of quantum noises on qubits and misalignments in block synchronization. In order to ensure information security, it is of great significance to study the construction of QSCs. In 2013, Fujiwara *et al.* [5,6] proposed the framework of quantum block synchronization and gave the first example of QSCs. In 2014, Xie *et al.* [18] used quadratic residue codes to produce binary QSCs which attain the upper bound on synchronization capabilities. Recently, Li and Yue [13] obtained two families of QSCs with good error-correcting performance. Some further studies about QSCs can be seen in [12,14].

Although we now have the theoretical framework of QSCs, there exists only a few families of QSCs in the literature. Cyclotomic classes can be used to constructed self-dual codes [7,11], which have important appliance in constructing QSCs. Hence, we use the cyclic codes obtained by sextic cyclotomy to construct QSCs in this work. This paper is arranged as follows. In Section 2, we review some general conclusions of cyclic codes and cyclotomic classes. In Section 3, we construct some dual-containing cyclic codes and discuss their minimum Hamming distance. In Section 4, we construct two classes of QSCs and discuss their synchronization capabilities and error-correcting performance. Finally, some concluding remarks are given in Section 5.

2 Preliminaries

2.1 Cyclic Codes and Dual Codes

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. An $[n,k,d]_q$ linear code C is a k-dimensional subspace of the n-dimensional vector space over $\mathbb{F}_q$ such that

$\min\{\mathrm{wt}(v)|v \in C,\ v \neq 0\} = d$, where $\mathrm{wt}(v)$ is the Hamming weight of v. A linear code with parameters $[n,k,d]_q$ is called optimal if and only if its minimum Hamming distance reaches the Hamming bound, see e.g. [2]. A linear code with parameters $[n,k,d]_q$ is called almost optimal means that the code with parameters $[n,k,d+1]_q$ is optimal. An $[n,k]_q$ cyclic code C is a linear code with the property that if a codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in C$, then $(c_{n-1}, c_0, \cdots, c_{n-2}) \in C$. It is known that C can be seen as an principal ideal $\langle g(x)\rangle$ in $\mathbb{F}_q[x]/(x^n-1)$. The polynomial $g(x)$ with degree $n-k$ is a monic divisor of x^n-1, and it is called the generator polynomial of C. The polynomial $h(x) = x^n - 1/g(x)$ is called the parity-check polynomial of C.

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 $(x,y) = \sum\limits_{i=0}^{n-1} x_i y_i$. The Euclidean dual code $C^{\perp} = \{x \in \mathbb{F}_q^n | (x,c) = 0, \forall c \in C\}$ of C is also a cyclic code [10], and the generator polynomial of $C^{\perp}$ has the form

$$\tilde{h}(x) = h(0)^{-1} x^k h\left(x^{-1}\right), \tag{1}$$

which is called the reciprocal polynomial of $h(x)$.

Let $C_1 = \langle g_1(x)\rangle$ and $C_2 = \langle g_2(x)\rangle$ be two cyclic codes with parameters $[n,k_1]_q$ and $[n,k_2]_q$ respectively. If $C_1 \subseteq C_2$, then C_2 is said to be C_1-containing, and C_2 is called the augmented code of C_1. If $C_2^{\perp} \subset C_2$, C_2 is called dual-containing.

2.2 Sextic Cyclotomic Classes

Let $n = 12m+7$ be an odd prime and γ be a fixed primitive element in $\mathbb{F}_n$. Then the sextic cyclotomic classes $C_0^{(6,n)}$, $C_1^{(6,n)}$, $\ldots$, $C_5^{(6,n)}$ in $\mathbb{F}_n$ are

$$C_i^{(6,n)} = \{\gamma^{6j+i} | 0 \leq j \leq \frac{n-1}{6} - 1\}, \text{ for } i = 0, 1, \cdots, 5.$$

Trivially $C_i^{(6,n)} = \gamma^i C_0^{(6,n)}$ and $\mathbb{F}_n^* = \bigcup_{i=0}^{5} C_i^{(6,n)}$, where $\mathbb{F}_n^* = \mathbb{F}_n \backslash \{0\}$.

Lemma 1. *Let the notations be defined as above. Then*

$$C_i^{(6,n)} = -C_{i+3}^{(6,n)},$$

where $i = 0, 1, \cdots, 5$, and $i+3$ means $i+3 \pmod 6$.

Proof. Since γ is a fixed primitive element in $\mathbb{F}_n$, $-1 = \gamma^{\frac{n-1}{2}} = \gamma^{6m+3} \in C_3^{(6,n)}$. Then the result can be obtained immediately. □

From now on, we let $q \in C_0^{(6,n)}$, and η be a n-th primitive root of unity in $\mathbb{F}_{q^{\mathrm{ord}_n(q)}}$, where $\mathrm{ord}_n(q)$ is the multiplicative order of q modulo n. Let

$$g_i^{(6,n)}(x) = \prod_{j \in C_i^{(6,n)}} (x - \eta^j), \tag{2}$$

where $i = 0, 1, \cdots, 5$. It is known that $g_i^{(6,n)}(x) \in \mathbb{F}_q[x]$, and the factorization of $x^n - 1$ is

$$x^n - 1 = (x-1)\prod_{i=0}^{5} g_i^{(6,n)}(x).$$

3 Cyclic Codes from Sextic Cyclotomy

3.1 Dual-containing Codes

Let C_i and $\bar{C}_i$ be the cyclic codes over $\mathbb{F}_q$ generated by $g_i^{(6,n)}(x)$ and $\frac{x^n-1}{g_{i+3}^{(6,n)}(x)}$ respectively, $i = 0, 1, \cdots, 5$.

Lemma 2. *Let $n = 12m+7$ be an odd prime, where m is a nonnegative integer. Then*

$$(a)\ C_i^{\perp} = \bar{C}_i, \qquad (b)\ C_i^{\perp} \subset C_i. \tag{3}$$

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

$$\tilde{g}_i^{(6,n)}(x) = \left(g_i^{(6,n)}(0)\right)^{-1} x^{\deg\left(g_i^{(6,n)}(x)\right)} g_i^{(6,n)}(x^{-1}).$$

Assume that

$$g_i^{(6,n)}(x) = (x - \eta^{e_{i_1}})(x - \eta^{e_{i_2}})\ldots(x - \eta^{e_{i_{2m+1}}}),$$

where e_{i_j} runs over $C_i^{(6,n)}$ and each element appears only once. Then

$$\begin{aligned}\tilde{g}_i^{(6,n)}(x) =&(-\eta^{e_{i_1}})^{-1}(-\eta^{e_{i_2}})^{-1}\ldots(-\eta^{e_{i_{2m+1}}})^{-1}x^{2m+1}\\ &(x^{-1} - \eta^{e_{i_1}})(x^{-1} - \eta^{e_{i_2}})\ldots(x^{-1} - \eta^{e_{i_{2m+1}}})\\ =&(x - \eta^{-e_{i_1}})(x - \eta^{-e_{i_2}})\ldots(x - \eta^{-e_{i_{2m+1}}}).\end{aligned}$$

According to Lemma 1 and Equation (2), we have

$$\tilde{g}_i^{(6,n)}(x) = g_{i+3}^{(6,n)}(x), \tag{4}$$

where $i = 0, 1, \cdots, 5$. Note that the parity-check polynomial of C_i is

$$h(x) = \frac{x^n - 1}{g_i^{(6,n)}(x)} = (x-1)\prod_{j \in F_n^* \backslash C_i^{(6,n)}} (x - \eta^j).$$

And by Equation (4),

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

is the generator polynomial of $C_i^{\perp}$. This means $C_i^{\perp} = \bar{C}_i$. Moreover, since $g_i^{(6,n)}(x)|\tilde{h}(x)$, we get $C_i^{\perp} \subset C_i$. □

In addition, let D_i and $\bar{D}_i$ be the cyclic codes over $\mathbb{F}_q$ generated by $g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x)$ and $(x-1)g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x)$ respectively, for any $i \in \{0,1,2,3,4,5\}$. By using the similar method in Lemma 2, we have the following Lemma.

Lemma 3. *Let $n = 12m + 7$ be an odd prime. Then*

$$(a)\ D_i^{\perp} = \bar{D}_i, \qquad (b)\ D_i^{\perp} \subset D_i. \tag{5}$$

Proof. The proof is straightforward from Lemma 2. □

Theorem 1. *Let d_i be the minimum Hamming distance of the cyclic code D_i. Then $d_i^2 - d_i + 1 \geq n$, where n is the length of D_i.*

Proof. Let $d(x)$ be a codeword in D_i with minimum Hamming weight d. From Equation (2),

$$d(x) = \prod_{i \in C_i^{(6,n)} \cup C_{i+1}^{(6,n)} \cup C_{i+2}^{(6,n)}} (x - \eta^i) s(x),$$

where $s(x) \in \mathbb{F}_q[x]$, $\deg(s(x)) < \frac{n+1}{2}$. Since η^i are the roots of $d(x) = 0$, $d(x^{-1}) = 0$ have roots η^{-i}, where $i \in C_i^{(6,n)} \cup C_{i+1}^{(6,n)} \cup C_{i+2}^{(6,n)}$. Then we have $-1 \in C_{i+3}^{(6,n)}$, we then have $d(x^{-1})$ is a codeword in D_{i+3} with minimum Hamming weight d. Therefore, $d(x)d(x^{-1})$ is a codeword in $D_i \cap D_{i+3}$, which means $d(x)d(x^{-1})$ a multiple of

$$\begin{aligned} & g_i^{(6,n)}(x) g_{i+1}^{(6,n)}(x) g_{i+2}^{(6,n)}(x) g_{i+3}^{(6,n)}(x) g_{i+4}^{(6,n)}(x) g_{i+5}^{(6,n)}(x) \\ &= \frac{x^n - 1}{x - 1} = \sum_{j=0}^{n-1} x^j. \end{aligned}$$

Then the weight of codewrod $d(x)d(x^{-1})$ is n. Since there are d terms equal to some nonzero elements of $\mathbb{F}_q$ in $d(x)$, we have $d^2 - d + 1 \geq n$. The desired result follows. □

Example 1. *Let $n = 12m + 7$ and $q \in C_0^{(6,n)}$. Table 1 gives some examples of cyclic codes and their duals, and some of them are optimal or almost optimal. All computations have been done by MAGMA [1]. Obviously, the minimum Hamming distance of D_i in Table 1 satisfy the bound in Theorem 1.*

Remark 1. *From Lemmas 2 and 3, we obtain two classes of dual-containing cyclic codes C_i and D_i. Furthermore, for any $i = \{0, 1, 2\}$, the cyclic codes with generator polynomial $g_i^{(6,n)}(x) g_{i+j}^{(6,n)}(x)$ are dual-containing codes, where $j \in \{0, 1, 2, 4, 5\}$ and $j \neq i$.*

3.2 Augmented Cyclic Codes

In order to obtain the augmented cyclic codes of C_i and D_i, we need the concept of cyclotomic cosets. The q-cyclotomy coset modulo n containing the integer s is defined as

$$C_{(s,n)} = \{sq^i \pmod{n} | i \in \mathbb{N}\}, \tag{6}$$

where $\mathbb{N}$ is the set of all nonnegative integers. It is notable that $s \in \{0, 1, 2, \ldots, n-1\}$. Then the unique irreducible minimal polynomial of η^s in $\mathbb{F}_q[x]$ is

$$M_s(x) = \prod_{i \in C_{(s,n)}} (x - \eta^i). \tag{7}$$

Lemma 4. *[15] Let n be an odd prime, and the size of $C_{(1,n)}$ be ℓ. Then the size of any cyclotomic coset $C_{(s,n)}$ is ℓ.*

Theorem 2. *Let $n = 12m + 7$ be an odd prime, $C_i = \langle g_i^{(6,n)}(x) \rangle$. If the size of $C_{(1,n)}$ is ℓ, the generator polynomial $g_i^{(6,n)}(x)$ can be expressed as*

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

where $t = \frac{n-1}{6\ell}$.

Proof. By Lemma 4, the size of $C_{(s,n)}$ is ℓ. Let $q = \gamma^{6k} \in C_0^{(6,n)}$ be a prime power, where $k \in \{1, 2, \ldots, \frac{n-7}{6}\}$. As γ is the fixed primitive element in $\mathbb{F}_n$, it is easy to deduce that $C_{(s,n)} \subseteq C_i^{(6,n)}$. Since $\bigcup_{i=0}^{5} C_i^{(6,n)} = \bigcup_{s=1}^{n-1} C_{(s,n)} = \mathbb{F}_n^*$, we have $C_i^{(6,n)} = \bigcup_{j=1}^{t} C_{(i_j,n)}$, where $i_1, i_2, \cdots, i_t \in \{1, 2, \cdots, n-1\}$ are some appropriate integers. Furthermore, we have $t = \frac{|C_i^{(6,n)}|}{|C_{(s,n)}|} = \frac{n-1}{6\ell}$, where $|C_{(s,n)}|$ means the size of $C_{(s,n)}$. By Equations (7) and (2), we have $g_i^{(6,n)}(x) = \prod_{j=1}^{t} M_{i_j}(x)$. □

Example 2. *Consider the sextic cyclotomic classes $C_i^{(6,n)}$ in $\mathbb{F}_{127}$.*

$$\begin{aligned} C_0^{(6,127)} &= \{1, 47, 50, 64, 87, 25, 32, 107, 76, 16, 117, 38, 8, \\ &\quad 122, 19, 4, 61, 73, 2, 94, 100\}, \\ C_1^{(6,127)} &= \{6, 28, 46, 3, 14, 23, 65, 7, 75, 96, 67, 101, 48, 97, \\ &\quad 114, 24, 112, 57, 12, 56, 92\}, \\ C_2^{(6,127)} &= \{36, 41, 22, 18, 84, 11, 9, 42, 69, 68, 21, 98, 34, 74, \\ &\quad 49, 17, 37, 88, 72, 82, 44\}, \\ C_3^{(6,127)} &= \{89, 119, 5, 108, 123, 66, 54, 125, 33, 27, 126, 80, \\ &\quad 77, 63, 40, 102, 95, 20, 51, 111, 10\}, \\ C_4^{(6,127)} &= \{26, 79, 30, 13, 103, 15, 70, 115, 71, 35, 121, 99, \\ &\quad 81, 124, 113, 104, 62, 120, 52, 31, 60\}, \\ C_5^{(6,127)} &= \{29, 93, 53, 78, 110, 90, 39, 55, 45, 83, 91, 86, 105, \\ &\quad 109, 43, 116, 118, 85, 58, 59, 106\}. \end{aligned}$$

Let $\gamma = 3$ be the fixed primitive element of $\mathbb{F}_{127}$. Since $q = \gamma^{6K} \in C_0^{(6,127)}$, where $K \in \{0, 1, \cdots, 20\}$, the order of q modulo n is $\frac{|\gamma|}{\gcd(6K, |\gamma|)}$. If $K = 14$, then $q = 19$ and the order of q modulo n is 3. By Equation (6), we have

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

Thus $C_0^{(6,127)} = C_{(1,127)} \cup C_{(2,127)} \cup C_{(4,127)} \cup C_{(8,127)} \cup C_{(16,127)} \cup C_{(32,127)} \cup C_{(64,127)}$, which is equivalent to

$$g_0^{(6,127)}(x) = M_1(x) M_2(x) M_4(x) M_8(x) M_{16}(x) M_{32}(x) M_{64}(x).$$

Table 1: Dual-containing cyclic codes C_i and D_i

Codes	Dual codes	Comments
$C_i = [19, 16, 3]_7$	$C_i^{\perp} = [19, 3, 15]_7$	Both optimal [8]
$D_i = [19, 10, 7]_7$	$D_i^{\perp} = [19, 9, 8]_7$	Both almost optimal [8]
$C_i = [31, 26, 3]_2$	$C_i^{\perp} = [31, 5, 16]_2$	Both optimal [8]
$D_i = [31, 16, 7]_2$	$D_i^{\perp} = [31, 15, 8]_2$	D_i almost optimal, $D_i^{\perp}$ optimal [8]
$C_i = [43, 36, 5]_4$	$C_i^{\perp} = [43, 7, 27]_4$	Both optimal [8]
$D_i = [43, 22, 12]_4$	$D_i^{\perp} = [43, 21, 12]_4$	D_i almost optimal [8]
$C_i = [67, 56, 6]_9$	$C_i^{\perp} = [67, 11, 44]_9$	C_i almost optimal, $C_i^{\perp}$ optimal [8]
$\cdots$	$\cdots$	$\cdots$

In this way, we have the following equations.

$$\begin{aligned} C_1^{(6,127)} =& C_{(3,127)} \cup C_{(6,127)} \cup C_{(12,127)} \cup C_{(24,127)} \\ & \cup C_{(48,127)} \cup C_{(96,127)} \cup C_{(65,127)}, \\ C_2^{(6,127)} =& C_{(9,127)} \cup C_{(18,127)} \cup C_{(36,127)} \cup C_{(72,127)} \\ & \cup C_{(17,127)} \cup C_{(34,127)} \cup C_{(68,127)}, \\ C_3^{(6,127)} =& C_{(5,127)} \cup C_{(10,127)} \cup C_{(20,127)} \cup C_{(40,127)} \\ & \cup C_{(80,127)} \cup C_{(33,127)} \cup C_{(66,127)}, \\ C_4^{(6,127)} =& C_{(13,127)} \cup C_{(26,127)} \cup C_{(52,127)} \cup C_{(104,127)} \\ & \cup C_{(81,127)} \cup C_{(35,127)} \cup C_{(70,127)}, \\ C_5^{(6,127)} =& C_{(29,127)} \cup C_{(58,127)} \cup C_{(116,127)} \cup C_{(105,127)} \\ & \cup C_{(83,127)} \cup C_{(39,127)} \cup C_{(78,127)}, \end{aligned}$$

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

Lemma 5. *Let $n = 12m+7$ be an odd prime, and C_i, D_i be the cyclic codes defined by above for $i \in \{0, 1, 2, 3, 4, 5\}$. If t in Theorem 2 is greater than 1, the following conclusions are established.*

1) *If $C = \langle \frac{g_i^{(6,n)}(x)}{\prod_{i\in A} M_i(x)} \rangle$, then $C_i \subset C$, where A is some nonempty subset of $\{i_1, i_2, \cdots, i_t\}$.*

2) *If $D = \langle \frac{g_i^{(6,n)}(x)g_{i+1}^{(6,n)}(x)g_{i+2}^{(6,n)}(x)}{\prod_{i\in B} M_i(x)} \rangle$, then $D_i \subset D$, where B is some nonempty subset of $\{i_1, i_2, \cdots, i_t\} \cup \{(i+1)_1, (i+1)_2, \cdots, (i+1)_t\} \cup \{(i+2)_1, (i+2)_2, \cdots, (i+2)_t\}$.*

Proof. The results come from the definition of dual-containing codes. □

4 Quantum Synchronizable Codes from the Obtained Cyclic Codes

First we review some basic concepts of QSCs. An $[[n, k]]$ quantum error-correcting code encodes k logical qubits into n physical qubits. A QSC with parameters (c_l, c_r)-$[[n, k]]$ is an encode scheme that corrects not only bit errors and phase errors but also a misalignment up to the left by c_l qubits and up to the right by c_r qubits, where c_l and c_r are nonnegative integers.

We provide the construction of QSCs by applying the method discovered by Fujiwara *et al.* [4, 6].

Lemma 6. *[4] Let $C_1 = \langle g_1(x)\rangle$ and $C_2 = \langle g_2(x)\rangle$ be two cyclic codes of parameters $[n, k_1, d_1]_r$ and $[n, k_2, d_2]_r$ respectively in $\mathbb{F}_r$ with $k_1 > k_2$ such that $C_2 \subset C_1$ and $C_2^{\perp} \subseteq C_2$. Define $f(x) = \frac{g_2(x)}{g_1(x)}$ in $\mathbb{F}_r[x]/(x^n-1)$. Then for any pair of nonnegative integers c_l, c_r satisfying $c_l + c_r <$ $\mathrm{ord}\,(f(x))$, we can construct a (c_l, c_r)-$[[n+c_l+c_r, 2k_2-n]]$ QSC from C_1 and C_2 that can correct up to $\lfloor \frac{d_1-1}{2} \rfloor$ bit errors and $\lfloor \frac{d_2-1}{2} \rfloor$ phase errors.*

4.1 Maximum Misalignment Tolerance

Lemma 7. *The tolerable magnitude of QSCs is upper bounded by its length n.*

Proof. From Lemma 6, the synchronization capability of QSCs is related to the order of $f(x)$. According to the definition of $f(x)$ and $f(x)|(x^n-1)$, it is clear that the tolerable magnitude of QSCs is upper bounded by its length n. □

Lemma 8. *Let $n = 12m + 7$ be an odd prime. Then the tolerable magnitude of QSCs with length n can reach the upper bound.*

Proof. As the order of η is n in $\mathbb{F}_{q^{\mathrm{ord}_n(q)}}$, where n is an odd prime. We know that the order of any root of $f(x)$ is n, then the order of $f(x)$ must be n. By Lemma 7, the tolerable magnitude of QSCs constructed by Lemma 6 can reach the upper bound n. □

Based on the cyclic code C_i constructed in Lemma 2, we can obtain a class of QSCs as follows, whose synchronization capabilities can always reach the upper bound.

Theorem 3. *Let $n = 12m + 7$ be an odd prime, $t = \frac{n-1}{6\ell}$ and $q \in C_0^{(6,n)}$, where $q^{\ell} \equiv 1 \bmod n$. For any nonnegative integers c_l and c_r satisfying $c_l+c_r < n$, we can construct a*

QSC with parameters (c_l, c_r)-$[[n+c_l+c_r, 2|A|\ell+\frac{2n+1}{3}]]_q$, *where* $|A|$ *is the size of* A *in Lemma 5, and* $0 \le |A| \le t-2 = \frac{n-12\ell-1}{6\ell}$.

Proof. From the definition of cyclotomic coset, we have that the size of $C_{(s,n)}$ is ℓ and $\ell|(2m+1)$, for any $s \in \{1, 2, \dots, n-1\}$. It is obvious that the 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 $t = \frac{n-1}{6\ell}$ irreducible factors in $\mathbb{F}_q[x]$. Since the size of $C_i^{(6,n)}$ is odd, we let $t \ge 3$. According to (a) in Lemma 5, the cyclic code $C_i^{(6,n)} = \langle g_i^{(6,n)}(x)\rangle$ has an augmented code C with parameters $\left[n, \frac{5n+1}{6} + |A|\ell\right]$. Taking a set A' such that $A \subset A' \subset \{i_1, i_2, \dots, i_t\}$, then we can get a cyclic code C' with parameters $\left[n, \frac{5n+1}{6} + |A'|\ell\right]$ such that $C \subset C'$. Then $0 \le |A| \le t-2 = \frac{n-12\ell-1}{6\ell}$. Furthermore, by Lemmas 7 and 8, we can obtain a QSC with parameters (c_l, c_r)-$[[n+c_l+c_r, 2|A|\ell+\frac{2n+1}{3}]]_q$, whose tolerable magnitude against misalignment errors can reach the upper bound n. □

Moreover, we can also construct another class of QSCs whose synchronization capabilities reach the upper bound by using the cyclic code D_i and its augmented codes.

Theorem 4. *Let* $n = 12m+7$ *be an odd prime,* $t = \frac{n-1}{6\ell}$ *and* $q \in C_0^{(6,n)}$, *where* $q^\ell \equiv 1 \bmod n$. *For any nonnegative integers* c_l *and* c_r *satisfying* $c_l + c_r < n$, *we can construct a QSC with parameters* (c_l, c_r)-$[[n+c_l+c_r, 2|B|\ell+1]]_q$, *where* $|B|$ *is the size of* B *in Lemma 5, and* $0 \le |B| \le 3t-2 = \frac{n-4\ell-1}{2\ell}$.

Proof. Since the size of $C_{(s,n)}$ is ℓ and $\ell|(2m+1)$, it is obvious that the 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 $g_{i+j}^{(6,n)}(x)$ $(j \in \{0, 1, 2\})$ has at least $t = \frac{n-1}{6\ell}$ irreducible factors over $\mathbb{F}_q$. So we let $t \ge 3$. According to (b) in Lemma 5, the cyclic code $D_i = \langle g_i^{(6,n)}(x) g_{i+1}^{(6,n)}(x) g_{i+2}^{(6,n)}(x)\rangle$ has an augmented code D with parameters $\left[n, \frac{n+1}{2} + |B|\ell\right]$. Taking a set B' such that $B \subset B' \subset (\{i_1, i_2, \dots, i_t\} \cup \{(i+1)_1, (i+1)_2, \dots, (i+1)_t\} \cup \{(i+2)_1, (i+2)_2, \dots, (i+2)_t\})$, then we can get a cyclic code $D' = \left[n, \frac{n+1}{2} + |B'|\ell\right]$ such that $D \subset D'$. Then $0 \le |B| \le 3t-2 = \frac{n-4\ell-1}{2\ell}$. Furthermore, by Lemmas 7 and 8, we can obtain a QSC with parameters (c_l, c_r)-$[[n+c_l+c_r, 2|B|\ell+1]]_q$ whose tolerable magnitude against misalignment errors can reach the upper bound n. □

The following are two examples about QSCs which are constructed by sextic cyclotomy. In particular, we can give a lower bound of the error-correcting capability towards bit errors and phase errors of QSCs constrtucted by D_i and its augmented codes.

Example 3. (a) *Let* $n = 127$ *and* $q = 19 \in C_0^{(6,n)}$. *In this case, we only consider the construction of QSCs from the cyclic code* $C_0 = \langle g_0^{(6,127)}(x)\rangle$ *and its augmented codes. Then* $0 \le |A| \le 5$, *by Theorem 3. From Example 2, let* $A = \{8, 16, 32, 64\}$, $|A| = 4$. *Then the cyclic code* $C = \langle \frac{g_0^{(6,127)}(x)}{\prod_{i \in A} M_i(x)}\rangle$ *with parameters* $[127, 118, 6]_{19}$ *is optimal and* $C^\perp \subset C$. *Furthermore, let* $A \subset A' = \{2, 4, 8, 16, 32, 64\}$. *Then the cyclic code* $C' = \langle \frac{g_0^{(6,127)}(x)}{\prod_{i \in A'} M_i(x)}\rangle$ *with parameters* $[127, 124, 3]_{19}$ *is optimal and* $C^\perp \subset C \subset C'$. *Then by Lemma 6, we can construct a* (c_l, c_r)-$[[127+c_l+c_r, 109]]_{19}$ *QSC with* $c_l+c_r < 127$, *whose tolerable magnitude against misalignment errors can reach the upper bound. Moreover, since the cyclic codes* C *and* C' *are optimal, the QSC we construct has the optimal error-correcting capability towards bit errors and phase errors.*

(b) *Let the notations be defned as above. In this case, we only consider the QSCs constructed from* $D_0 = \langle g_0^{(6,127)}(x) g_1^{(6,127)}(x) g_2^{(6,127)}(x)\rangle$ *and its augmented codes. By Theorem 4,* $0 \le |B| \le 19$. *From Example 2, let* $B = \{2\}$. *Hence the augmented code of* D_0 *is* $D = \langle \frac{g_0^{(6,127)}(x) g_1^{(6,127)}(x) g_2^{(6,127)}(x)}{\prod_{i \in B} M_i(x)}\rangle$. *By Lemma 3,* D_0 *is a dual-containing code, then we have* $D_0^\perp \subset D_0 \subset D$. *From Lemma 6, we can construct a* (c_l, c_r)-$[[127+c_l+c_r, 1]]_{19}$ *QSC with* $c_l+c_r < 127$, *whose tolerable magnitude against misalignment errors can reach the upper bound. From Theorem 1, the lower bound of* D_0 *satisfies* $d_0^2 - d_0 + 1 \ge 127$, *then the parameters of* D_0 *are* $[127, 64, \ge 12]_{19}$ *and the parameter of* D *are* $[127, 67, \ge 12]_{19}$. *According to Lemma 6, the QSCs we constructed can correct up to 5 bit errors and 5 phase errors.*

5 Conclusion

We study two classes of QSCs from dual-containing cyclic codes obtained by sextic cyclotomic classes. The constructed QSCs possess the highest tolerance against misalignment errors, besides some of them have optimal or almost optimal error-correcting capability towards bit errors and phase errors. Since the exact Hamming distances of the cyclic codes used to construct QSCs are quite difficult to compute, the error-correcting capability of QSCs is difficult to determine in theory. We hope that our future work can make a breakthrough in this respect.

Acknowledgments

This work was supported by Fundamental Research Funds for the Central Universities (20CX05012A), the Major Scientific and Technological Projects of CNPC under Grant(ZD2019-183-008), National Nature Science Foundation of China (11775306), and Shandong Provincial Natural Science Foundation of China (ZR2019MF070).

References

[1] W. Bosma, J. J. Cannon, and C. Fieker, "Handbook of magma functions," *Journal of Symbolic Computation*, vol. 24, no. 3-4, p. 5017, 2010.

[2] A. E. Brouwer, *Bounds on the size of linear codes*. Elsevier, 1998.

[3] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, pp. 1098–1105, 1996.

[4] Y. Fujiwara, "Block synchronization for quantum information," *Physical Review A*, vol. 87, no. 2, p. 022344, 2013.

[5] Y. Fujiwara, V. D. Tonchev, and T. Wong, "Algebraic techniques in designing quantum synchronizable codes," *Physical Review A*, vol. 88, no. 1, p. 012318, 2013.

[6] Y. Fujiwara and P. Vandendriessche, "Quantum synchronizable codes from finite geometries," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 7345–7354, 2014.

[7] W. Gao and T. Yan, "Double circulant self-dual codes from generalized cyclotomic classes of order two," *International Journal of Network Security*, vol. 23, no. 3, pp. 395–400, 2021.

[8] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Mar. 2, 2022. (`http://www.codetables.de`)

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

[10] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[11] C. Jiang, Y. Sun, and X. Liang, "Eight power residue double circulant self-dual codes," *International Journal of Network Security*, vol. 22, no. 5, pp. 736–742, 2020.

[12] L. Q. Li, S. X. Zhu, and L. Liu, "Quantum synchronizable codes from the cyclotomy of order four," *IEEE Communications Letters*, vol. 23, no. 1, pp. 12–15, 2019.

[13] X. Li and Q. Yue, "A new family of quantum synchronizable codes," *IEEE Communications Letters*, vol. 25, no. 2, pp. 342–345, 2021.

[14] L. Luo and Z. Ma, "Non-binary quantum synchronizable codes from repeated-root cyclic codes," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1461–1470, 2018.

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: Elsevier, 1977.

[16] M. A. Nielsen and I. Chuang, *Quantum Computaion and Quantum Information*. New York: Cambridge University Press, 2011.

[17] A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters*, vol. 77, no. 5, pp. 793–797, 1996.

[18] Y. X. Xie, Yuan J. H, and Y. Fujiwara, "Quantum synchronizable codes from quadratic residue codes and their supercodes," in *2014 IEEE Information Theory Workshop (ITW 2014)*, pp. 172–176, August 2014.

Biography

Tao Wang received the B.S. degree in China University of Petroleum, Qingdao China, in 2018. He is currently pursuing his M.S. in Mathematics from China University of Petroleum. His research interests include coding theory and Information security.

Xueting Wang received the B.S. degree in University of Jinan, Jinan China, in 2020. She is currently pursuing her M.S. in Mathematics from China University of Petroleum. His research interests include coding theory and Information security.

Qian Liu is a undergraduate student of China University of Petroleum. He is mainly engaged in the research of Applied mathematics.

Tongjiang Yan was born in 1973 in Shandong Province of China. He was graduated from the Department of Mathematics, Huaibei Coal-industry Teachers College, China, in 1996. In 1999, he received the M. S. degree in mathematics from the Northeast Normal University, Lanzhou. He received the Ph. D. degree in cryptography from the Xidian University, Xian. He is now a professor of China University of Petroleum. His research interests include cryptography and coding.