International Journal of Theoretical Physics (2020) 59:1058–1068
https://doi.org/10.1007/s10773-020-04388-2

New Quantum Codes Derived from Cyclic Codes

Binbin Pang[1] · Shixin Zhu[1] · Jin Li[1] · Lanqiang Li[1]

Received: 19 September 2019 / Accepted: 9 January 2020 / Published online: 21 January 2020

Abstract
In this paper, we construct optimal or almost optimal dual-containing cyclic codes from cyclotomic classes of order r. Based on these cyclic codes constructed, we obtain many new quantum codes comparing with the known literatures. Furthermore, we construct some quantum synchronizable codes with good error-correcting ability towards bit errors and phase errors by a pair of cyclic codes with special containing property.

Keywords Cyclotomic classes · Quantum codes · Quantum synchronizable codes

1 Introduction

Quantum error-correcting codes (QECCs) play an important role in protecting quantum data transmitted over noisy quantum communication channels. The construction of new QECCs is a hot topic in recent decades [1, 9, 12, 14, 15, 21]. The quantum BCH codes were studied in many literatures [1, 14, 21]. In 2013, Kai et al. constructed some new quantum MDS codes from negacyclic codes. Recently, La Guardia constructed some new quantum codes from cyclic codes. After that, Gao et al. construct some new quantum codes from a special class of negacyclic codes. And they only consider the Pauli errors. However, this error model is not the only one of importance.

This research was supported by the National Natural Science Foundation of China under Grant No 61772168, 61972126 and 11501156, the Anhui Provincial Natural Science Foundation under Grant No 1708085QA01.

✉ Shixin Zhu
zhushixinmath@hfut.edu.cn

Binbin Pang
pbbmath@126.com

Jin Li
lijin_0102@126.com

Lanqiang Li
lilanqiang716@126.com

[1] School of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, People's Republic of China

Scholars paid little attention to another type of significance error misalignment, which respect to the block structure of a qubit stream in quantum information processing. Where the information receiver or processing device misidentifies the boundary of an information block, the catastrophic failure can be brought. As the special QECCs, quantum synchronizable codes (QSCs) correct the effects of both quantum noise on qubits and misalignment in block synchronization [7]. The method of constructing the binary QSCs is to find out a pair of cyclic codes with special containing properties [7]. Fujiwara et al. improved the original construction method by widening the range of tolerable magnitude of misalignment and presented more examples of quantum synchronizable codes [6]. After that, there are many good QSCs from BCH codes, punctured Reed-Muller codes, certain finite geometric codes and quadratic or duadic codes [5, 6, 23]. Xie and Luo generalized the constructing of the binary QSCs to the q-ary QSCs [16, 22]. Xie et el. presented a general construction of QSCs from q-ary cyclic codes and derived the distance bound of the resulting QSCs of Calderbank-Shor-Steane (CSS) structure [22]. Luo and Ma constructed a new family of QSCs from repeated-root cyclic codes of lengths p^s and lp^s over $\mathbb{F}_q$ and proved that the QSCs with those lengths from the repeated-root cyclic codes can in general correct more Pauli errors than narrow-sense BCH codes of close lengths [16]. Li et al. utilized the cyclotomic classes of order four to obtain some cyclic codes with dual-containing properties and constructed two classes of QSCs [18]. Inspired by current work, we consider QECCs and QSCs from the cyclic codes, which are obtained by the cyclotomic classes of order r for any positive even integer.

In this paper, we give some results and properties of cyclic codes and the cyclotomic classes of order r in Section 2. In Section 3, we construct some dual-containing cyclic codes over $\mathbb{F}_q$. We also obtain the bound of minimum distance of those cyclic codes and some optimal or almost optimal cyclic codes. Hence, we construct many optimal or almost optimal LCP of codes. In Section 4, we construct some new QECCs with cyclic codes obtained. We also construct some QSCs whose synchronization capabilities attain the upper bound. We conclude the paper in Section 5.

We will compare some of the codes obtained in this paper with the known literatures and the tables of best known linear codes (referred to as the Database later) maintained by Markus Grassl at http://www.codetables.de. The examples in this paper are computed by Magma.

2 Auxiliary Results

In this section, we give some simple introductions to cyclic codes. Furthermore, we present the definition and the properties of cyclotomy of order r.

Throughout this paper, let $\mathbb{F}_q$ be a finite field, where q is an odd prime power. An $[n, k]$ linear code C over $\mathbb{F}_q$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$. The (Euclidean) dual code of C, denoted by $C^{\perp}$, is defined by

$$C^{\perp} = \{\mathbf{u} \in \mathbb{F}_q^n \mid \mathbf{u} \cdot \mathbf{c} = 0 \; \forall \, \mathbf{c} \in C\},$$

where $\mathbf{u} \cdot \mathbf{c}$ denotes the standard inner product.

An $[n, k]$ linear code C over $\mathbb{F}_q$ is called a cyclic code if it is invariant under cyclic-shift on $\mathbb{F}_q$, $(c_0, c_1, \cdots, c_{n-1}) \mapsto (c_{n-1}, c_0, \cdots, c_{n-2})$. By identifying a codeword with its polynomial representation in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, a linear code of length n over $\mathbb{F}_q$ is cyclic if and only if the corresponding set in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is just an ideal in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Since

$\mathbb{F}_q[x]/\langle x^n-1\rangle$ is a principal ring. Then there is a monic polynomial $g(x)$ of minimal degree in C such that $C=\langle g(x)\rangle$, where $g(x)|\ (x^n-1)$. Furthermore, $\dim(C)=n-\deg g(x)$. Let $h(x)=(x^n-1)/g(x)$, $h(x)$ is called the check polynomial of C. We have $C^{\perp}=\langle h(x)^*\rangle$, where $h(x)^*=h(0)^{-1}x^{\deg(h(x))}h(\frac{1}{x})$ is the reciprocal polynomial of $h(x)$.

The q-cyclotomic coset containing j modulo n is defined by $C_j=\{q^i j \bmod n\}\subset\mathbb{Z}_n$, where $\gcd(n,q)=1$. As we all known that $m_j(x)=\Pi_{i\in C_j}(x-\xi^i)$ is the minimal polynomial of ξ^j over $\mathbb{F}_q$, where ξ is a primitive n-th root of unity in some extension field of $\mathbb{F}_q$. Let $\Gamma_{(q,n)}$ be the set of all the coset representatives. Then we have

$$x^n-1=\prod_{j\in\Gamma_{(q,n)}} m_j(x),$$

There is a pair of cyclic codes (C,C') with generator polynomials $g(x)$ and $g'(x)$, respectively. The cyclic codes C and C' have parameters $[n,k]_q$ and $[n,k']_q$, where $k<k'$, respectively. Then, C' is said to be C-containing if $C\subseteq C'$. Specially, we called C' dual-containing if $C=C'^{\perp}$. Furthermore, assume that C' is C-containing, we have that the generator polynomial $g'(x)$ is a factor of every codeword of C. i.e., for any $c(x)\in C$, there must exists a polynomial $f_c(x)$ such that $c(x)=f_c(x)g'(x)$ in $\mathbb{F}_q[x]$. Let $f(x)=g(x)/g'(x)$. We have that $f(x)\in\mathbb{F}_q[x]$ has degree $k'-k$ and $f(0)\neq 0$. What's more, the cardinality of the set $\{x^a(\bmod f(x))|a\in N\}$ is called the order of the polynomial $f(x)$, where N is the set of positive integers.

Let $n=rf+1$ be an odd prime, where f is a positive integer and r is a positive even integer. Let α be a generator of $\mathbb{F}_n^*$. We consider cyclotomic classes $D_{i,\alpha}^{(r,n)}$ of order r, which are defined as follows

$$D_{i,\alpha}^{(r,n)}=\alpha^i(\alpha^r),\ \ 0\le i<r,$$

where (α^r) denotes the multiplication subgroup of $\mathbb{F}_n^*$ generated by α^r. Clearly, we have $f=|D_{i,\alpha}^{(r,n)}|$ for $0\le i\le r$, where $|A|$ denotes the cardinality of set A. Obviously, the $D_{i,\alpha}^{(r,n)}$ for $0\le i<r$ forms a partition of $\mathbb{F}_n^*$. Next we show that this partition is unconcerned with the selection of generator of $\mathbb{F}_n^*$.

Proposition 2.1 *Let symbols be the same as before. Let α and β be distinct primitive elements of $\mathbb{F}_n$ and denote the cyclotomic classes $D_{i,\alpha}^{(r,n)}$ and $D_{j,\beta}^{(r,n)}$, respectively. For anyone $0\le j<r$, there exists unique integer j ($0\le i<r$) such that*

$$D_{i,\alpha}^{(r,n)}=D_{j,\beta}^{(r,n)}.$$

Proof There exists an integer s such that $\beta=\alpha^s$ since α and β are distinct primitive elements of $\mathbb{F}_n$, where $0\le s<n$ and $\gcd(s,n-1)=1$. Then we have $D_{j,\beta}^{(r,n)}=\{\beta^{rk+j}=\alpha^{srk+sj}|\ 0\le k<f\}$. For any $b=\beta^{rk+j}=\alpha^{srk+sj}\in D_{j,\beta}^{(r,n)}$. If $0\le sj<r$, let $i=sj$, then $b\in D_{i,\alpha}^{(r,n)}$. If $sj\ge r$, by the division algorithm, there exist integers $0\le b<f$ and $0\le c<r$ such that $sj=br+c$. Let $i=c$, then $b\in D_{i,\alpha}^{(r,n)}$. Then we have $D_{j,\beta}^{(r,n)}\subseteq D_{i,\alpha}^{(r,n)}$. Note that $|D_{i,\alpha}^{(r,n)}|=|D_{j,\beta}^{(r,n)}|$. Then we have the desired conclusion immediately. □

From Proposition 2.1, we always let $D_i^{(r,n)}$ denote $D_{i,\alpha}^{(r,n)}$ for any α, which is a generator of $\mathbb{F}_n^*$. In the sequel, we always let $n\equiv r+1 \pmod{2r}$ and $q\in D_0^{(r,n)}$. We define $s=\mathrm{ord}_n(q)$ and $\xi=\beta^{(q^s-1)/n}$, where β is a generator of $\mathbb{F}_{q^s}^*$. Thus, ξ is a n-th primitive root of unity in $\mathbb{F}_{q^s}$. Next we define $d_i(x) = \prod_{i\in D_i^{(r,n)}}(x-\xi^i)$. Note that D_i are unions of q-cyclotomic cosets for $q \in D_0^{(r,n)}$, then $d_i(x) \in \mathbb{F}_q[x]$. In fact, we have

$$x^n - 1 = (x-1)\prod_{i=0}^{r-1} d_i(x). \tag{1}$$

Keep the notations as above, we can obtain the following useful lemma immediately.

Lemma 2.2 *Let symbols be the same as before. We have*

$$D_i^{(r,n)} = -D_{i+\frac{r}{2}}^{(r,n)}, \quad i = 0, 1, \cdots, \frac{r-2}{2}.$$

Proof Since $n = r + 1 \pmod{2r}$, put $n = 2rk + r + 1$, we have $-1 \equiv \alpha^{(n-1)/2} \equiv \alpha^{rk+r/2} \pmod{n}$, where α is a generator of $\mathbb{F}_n^*$. For any element $d \in D_{i+\frac{r}{2}}^{(r,n)}$, $d = \alpha^{rk_0+i+r/2}$ for some integer k_0, where $0 \le k_0 \le f-1$. Note that $-d = \alpha^{(k+k_0+1)r+i} \in D_i^{(r,n)}$. Then we have $-D_{i+\frac{r}{2}}^{(r,n)} \subseteq D_i^{(r,n)}$. What's more, we know that $|-D_{i+\frac{r}{2}}^{(r,n)}| = f = |D_i^{(r,n)}|$. This completes the proof. □

From Lemma 2.2, we assume that $\mathbb{Z}_r = \{0, 1, \cdots, r-1\}$ and $A \subseteq \mathbb{Z}_r$, define

$$-A = \{a + \frac{r}{2} \pmod{r} |\ a \in A\}.$$

Remark 1 From the range of values of length n in this paper, the length $n \equiv 5 \pmod 8$ in [18] is a special case when $r = 4$. However, we can obtain more general lengths.

3 Construction of Cyclic Codes

In this section, we utilize the cyclotomic classes of order r to construct dual-containing cyclic codes, where r is a positive even integer. Suppose $Z_{(i,r)} = \{i, i+1, \cdots, i+r/2-1\} \pmod{r}$ for any $0 \le i \le r-1$. Let $C_{(i,S)}$ be the cyclic code with generator polynomial $g_{iS}(x) = \prod_{j\in S} d_j(x)$, where $S \subseteq Z_{(i,r)}$. From the definition of $C_{(i,S)}$, we have that $C_{(i,S_1)} \subseteq C_{(i,S_2)}$ if $S_2 \subseteq S_1$. Let $\overline{C}_{(i,S)}$ be the cyclic codes with generator polynomial $\overline{g}_{iS}(x) = \prod_{j\in\mathbb{Z}_r\setminus(-S)} d_j(x)$.

Lemma 3.1 *Let the symbols be the same as before, $C_{(i,S)}$ and $\overline{C}_{(i,S)}$ be defined above. Then we have*

$$(1)\ C_{(i,S)}^{\perp} = \overline{C}_{(i,S)}; \quad (2)\ C_{(i,S)}^{\perp} \subset C_{(i,S)}.$$

Proof By Lemma 2.2, we know that $d_i(x)^* = d_{i+\frac{r}{2}}(x)$ for any $0 \le i \le r-1$. Since $C_{(i,S)} = \langle g_{iS}(x)\rangle = \langle \prod_{j\in S} d_j(x)\rangle$, where $S \subseteq Z_{(i,r)}$. It is clear that $C_{(i,S)}^{\perp} = \langle h(x)^*\rangle = \langle \prod_{j\in\mathbb{Z}_r\setminus(-S)} d_j(x)\rangle$, where $h(x) = (x^n-1)/g_{iS}(x)$. We have the desired conclusions immediately. □

Theorem 3.2 *Let d_{iS} denote the minimum distance of the cyclic code $C_{(i,S)}$ and n be the length of $C_{(i,S)}$. Then we have following conclusions*

(1) *If* $|S| = \frac{r}{2}$, $d_{iS}^2 - d_{iS} + 1 \geq n$;
(2) *Otherwise,* $d_{iS}^2 - d_{iS} + 1 \geq d_S$.
where d_S *is the minimum distance of cyclic code with generator polynomial* $\prod_{j\in S\cup(-S)} d_j(x)$.

Proof (1) Let $|S| = \frac{r}{2}$ and $a(x)$ be a codeword of $C_{(i,S)}$ with weight d_{iS}. From Lemma 2.2, we have $a(x^{-1})$ is a codeword of $C_{(i+\frac{r}{2},S)}$. It is clear that $a(x)a(x^{-1})$ is a codeword of $C_{(i,S)} \bigcap C_{(i+\frac{r}{2},S)}$ with generator polynomial

$$\prod_{j\in S\cup(-S)} d_j(x) = \prod_{j\in\mathbb{Z}_r} d_j(x) = \frac{x^n - 1}{x - 1} = \sum_{k=0}^{n-1} x^k.$$

Then we have that the weight of $a(x)a(x^{-1})$ is n. From above all, we have $d_{iS}^2 - d_{iS} + 1 \geq n$.

(2) Let $|S| \neq \frac{r}{2}$ and $b(x)$ be a codeword of $C_{(i,S)}$ with weight d_{iS}. Similar to (1), we obtain that $b(x)b(x^{-1})$ is a codeword of $C_{(i,S)} \bigcap C_{(i+\frac{r}{2},S)}$ with generator polynomial

$$\prod_{j\in S\cup(-S)} d_j(x).$$

Then we have that the weight of $b(x)b(x^{-1})$ is at least d_S. For the above reasons, we have $d_{iS}^2 - d_{iS} + 1 \geq d_S$. This completes the proof.

□

Example 3.3 We let $(r, n, q) = (2, 7, 2)$ and $S = \{i\}$. Clearly, $q \in D_0^{(r,n)}$. For any $0 \leq i \leq 1$, The cyclic code $C_{(i,S)}$ has parameters $[7, 4, 3]$ and $C_{(i,S)}^{\perp}$ has parameters $[7, 3, 4]$, which are both optimal and satisfy the bound of Theorem 3.2.

Example 3.4 We let $(r, n, q) = (6, 19, 7)$ and $S = \{i, i + 1\}$. Clearly, $q \in D_0^{(r,n)}$. For any $0 \leq i \leq 5$, The cyclic code $C_{(i,S)}$ has parameters $[19, 13, 5]$ and $C_{(i,S)}^{\perp}$ has parameters $[19, 6, 12]$, which are both optimal and satisfy the bound of Theorem 3.2 .

Next we give more good dual-containing cyclic codes $C_{(i,S)}$ in Table 1. The all results of Table 1 are obtained by the algebra system Magma.

It is well known that linear complementary pairs (LCP) of codes are good candidates against side-channel attacks (SCA) and fault injection attacks (FIA). The reader can refer to [2, 3, 11] for more information. From Theorems II.1 and II.4 of [2], we have following lemma immediately.

Lemma 3.5 *Let gcd(n, q)=1, for cyclic codes* $C = \langle g(x)\rangle$ *and* $D = \langle u(x)\rangle$ *with length n over* $\mathbb{F}_q$, *we have following sentences hold.*

1). *The (C, D) is LCP if and only if* $u(x) = (x^n - 1)/g(x)$.
2). *D and* $C^{\perp}$ *are equivalent if (C, D) is LCP.*

From Table 1, many cyclic codes and their dual codes are both optimal or almost optimal. Then we can construct many optimal or almost optimal LCP of codes by Lemma 3.5.

Table 1 Dual-containing cyclic codes $C_{(i,S)}$

r	S	$C_{(i,S)}$	$C^{\perp}_{(i,S)}$	Optimal or almost optimal
2	$\{i\}$	$[7,4,3]_2^*$	$[7,3,4]_2^*$	Both optimal
		$[11,6,5]_3^*$	$[11,5,6]_3^*$	Both optimal
6	$\{i\}$	$[19,16,3]_7^*$	$[19,3,15]_7^*$	Both optimal
	$\{i,i+1\}$	$[19,13,5]_7^*$	$[19,6,12]_7^*$	Both optimal
	$\{i,i+1,i+2\}$	$[19,10,7]_7$	$[19,9,8]_7$	Both almost optimal
	$\{i,i+2\}$	$[19,13,4]_7$	$[19,6,11]_7$	Both almost optimal
8	$\{i\}$	$[73,64,3]_2$	$[73,9,28]_2$	$C_{(i,S)}$ almost optimal
	$\{i,i+1\}$	$[73,55,6]_2^*$	$[73,18,24]_2^*$	Both optimal
	$\{i,i+1,i+2\}$	$[73,46,9]_2$	$[73,27,16]_2$	$C_{(i,S)}$ almost optimal
	$\{i,i+2\}$	$[73,55,6]_2^*$	$[73,18,24]_2^*$	Both optimal
	$\{i,i+3\}$	$[73,55,6]_2^*$	$[73,18,24]_2^*$	Both optimal
...	...	...	...	...

There is a pair of cyclic codes (C, C') with containing property $C \subset C'$. We call cyclic code C' the augmented cyclic code of C. It is equivalent to $g'(x)|g(x)$ if $C = \langle g(x)\rangle$ and $C = \langle g'(x)\rangle$.

Theorem 3.6 *Let n be an odd prime and $n \equiv r+1 \pmod{2r}$. Let x^n-1 be factored as (1) over $\mathbb{F}_q$ and the cardinality of C_1 be ℓ. Then we have the each factor $d_i(x)$ of x^n-1 can be factored into $e = \frac{n-1}{r\ell}$ irreducible polynomials of the same degree ℓ as follows*

$$d_i(x) = \prod_{j \in T_i} m_j(x),$$

where T_i is some proper subset of $\mathbb{Z}_n$ and $|T_i| = e$ for $0 \le i \le r-1$.

Proof Since $|C_1| = \ell$ and n is an odd prime, we have $|C_j| = \ell$ for any $j \in \mathbb{Z}_n^*$, which implies that each polynomial $m_j(x)$ has degree ℓ for any $j \in \mathbb{Z}_n^*$. Furthermore, $q \in D_0^{(r,n)}$, we have that $D_i^{(r,n)} = \bigcup_{j \in T_i} C_j$, where T_i is some proper subset of $\mathbb{Z}_n$ and $|T_i| = e = \frac{n-1}{r\ell}$. □

Let C be an augmented cyclic code of $C_{(i,S)}$. From the proof of Lemma 3.1 and Theorem 3.6, we suppose that the generator polynomial $g(x)$ of C is a factor of $g_{iS}(x)$. Note that C is a dual-containing cyclic code. Then we have following lemma immediately.

Lemma 3.7 *Let the symbols be the same as before, $C_{(i,S)}$ and T_i be defined above. For any $0 \le i \le r-1$ and $S \subseteq Z_{(i,r)}$, then we have $C_{(i,S)} \subset C$ if $g(x)$ has following form*

$$g(x) = g_{iS}(x) / \prod_{k \in B} m_k(x),$$

where B is some proper subset of $\bigcup_{k \in S} T_k$.

Obviously, the cyclic codes C are also dual-containing, i.e., $C^{\perp} \subseteq C$.

4 QECCs and QSCs from Cyclotomic Codes

In this section, utilizing the optimal or almost optimal dual-containing cyclotomic codes obtained in Section 3, we construct some new QECCs and some QSCs with good parameters.

4.1 New QECCs from Cyclotomic Codes

In this subsection, firstly, we introduce the basic concept and results of QECCs. Secondly, we construct some new QECCs with the dual-containing cyclic codes obtained in Section 3.

A q-ary QECC $\mathbb{Q}$ of length n is a K-dimensional subspace of the q^n-dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$, where $\otimes n$ denotes the tensor product of vector spaces. If $K = q^k$, a q-ary QECC of length n and minimum distance d denote by $[[n, k, d]]_q$. For a QECC with parameter $[[n, k, d]]_q$, the Quantum Singleton Bound (QSB) asserts that $k + 2d \leq n + 2$. If the equality holds then the code is called a maximum distance separable (MDS) code. For more details on QECCs, the reader can refer to [13–15, 20]. The following lemma give the classical construction method of QECCs in [1, 17].

Lemma 4.1 1). *(Calderbank-Shor-Steane (CSS) Construction) If there exists a classical linear $[n, k, d]_q$ code C such that $C^{\perp} \subseteq C$, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer quantum code that is pure to d.*

2). *(Steane's Construction) If there exists a classical linear $[n, k, d]_q$ code C which contains its Euclidean dual $C^{\perp}$ and which can be enlarged to an linear code $C' = [n, k', d']_q$, where $k' - k \geq 2$, then there exists an $[[n, k + k' - n, \geq min\,\{d, \lceil \frac{q+1}{q} d' \rceil\}]]_q$ stabilizer quantum code.*

Clearly, our main goal is to obtain optimal or the almost optimal codes C such that $C^{\perp} \subseteq C$. From Section 3, we know that the cyclic codes $C_{(i,S)}$ are always dual-containing. Then they are good source to construct QECCs by 1) of Lemma 4.1. Furthermore, we have that $C_{(i,S_1)} \subseteq C_{(i,S_2)}$ if $S_2 \subseteq S_1$. Then we also can construct many QECCs by 2) of Lemma 4.1. Next we give some examples to illustrate the QECCs are new.

Example 4.2 Let $(r, n, q) = (2, 11, 5)$ and $S = \{i\}$, we have that $q \in D_0^{(2,11)}$. Let $C_{(i,S)} = \langle d_i(x) \rangle$ with parameters $[11, 6, 5]^*$. We get a QECC with parameters $[[11, 1, \geq 5]]_5$. This QECC has the same length and dimension $[[11, 1, \geq 4]]_5$ appeared in [15].

Example 4.3 Let $(r, n, q) = (12, 61, 9)$, $S_1 = \{i, i + 1\}$ and $S_2 = \{i\}$, we have that $q \in D_0^{(12,61)}$. Let $C_{(i,S_1)} = \langle d_i(x) d_{i+1}(x) \rangle$ with parameters $[61, 56, 4]^*$ and $C_{(i,S_2)} = \langle d_i(x) \rangle$ with parameters $[61, 51, 6]^*$. We get a QECC with parameters $[[61, 46, \geq 5]]_9$. This QECC has the same minimum distance $[[64, 48, \geq 5]]_5$ appeared in [19]. However, our QECC has larger code rate.

Next we give more new QECCs in Table 2. Our QECCs have the larger minimum distance with the same code rate or the larger code rate with the same minimum distance than know ones.

Note that some QECCs have parameters satisfying $n + 2 - 2d - k \leq 2$ in Table 2. The QECCs with parameters $[[11, 1, \geq 5]]_3$ and $[[73, 52, \geq 7]]_8$ in Table 2 have same parameters in recent literature, but we use different classical codes.

Table 2 New QECCs

r	New QECCs	Known QECCs
2	$[[11, 1, \geq 5]]_5$ from 1) of Lemma 4.1	$[[11, 1, \geq 4]]_5$ in [15]
2	$[[11, 1, \geq 5]]_3$ from 1) of Lemma 4.1	$[[11, 1, \geq 5]]_3$ in [10]
6	$[[19, 13, \geq 3]]_{11}$ from 1) of Lemma 4.1	$[[24, 16, \geq 3]]_{11}$ in [9]
12	$[[61, 46, \geq 5]]_9$ from 2) of Lemma 4.1	$[[64, 48, \geq 5]]_9$ in [19]
12	$[[61, 51, \geq 4]]_9$ from 1) of Lemma 4.1	$[[61, 51, \geq 3]]_9$ in [15]
12	$[[61, 51, \geq 4]]_9$ from 1) of Lemma 4.1	$[[64, 52, \geq 4]]_9$ in [19]
14	$[[71, 51, \geq 5]]_5$ from 1) of Lemma 4.1	$[[71, 51, \geq 4]]_5$ in [14]
24	$[[73, 64, \geq 4]]_5$ from 2) of Lemma 4.1	$[[73, 61, \geq 4]]_5$ in [15]
24	$[[73, 52, \geq 7]]_8$ from 2) of Lemma 4.1	$[[73, 52, \geq 7]]_8$ in [8]
10	$[[151, 106, \geq 8]]_2$ from 2) of Lemma 4.1	$[[151, 106, \geq 6]]_2$ in [4]
...	...	...

4.2 QSCs from Cyclotomic Codes

In this subsection, we give the basic concept and results of QSCs. Furthermore, from the cyclic codes obtained in Section 3 and their augmented cyclic codes, we get a class of QSCs .

A (c_l, c_r)-$[[n, k]]$ is a quantum stabilizer code that corrects not only bit errors and phase errors but also misalignment to the left by c_l qubits and to the right by c_r qubits for non-negative integers c_l and c_r. The desired QSCs not only seamlessly achieve quantum error correction and synchronization recovery, but also correct linear combinations of I, X, Z, and Y that act on physical qubits. As we all know, the QSCs have been proved to be well apply in the quantum domain. They allow to extract the information about the magnitude and direction of misalignment and simultaneously correcting the Pauli errors on qubits, with nondisturbing measurement involved. For more details of QSCs, we can refer to articles [5, 16, 23].

The general method of constructing QSCs directly exploits classical codes with special containing properties over finite fields. We give the following lemma that can be found in [16].

Lemma 4.4 *Let $D_1 = \langle g_1(x)\rangle$ be a dual-containing $[n, k_1, d_1]_q$ cyclic code and $D_2 = \langle g_2(x)\rangle$ be a D_1-containing $[n, k_2, d_2]_q$ cyclic code with $k_2 > k_1$ i.e., $D_1^{\perp} \subseteq D_1 \subseteq D_2$. Define the polynomial $f(x)$ of degree $k_2 - k_1$ to be the quotient of $g_1(x)$ divided by $g_2(x)$. Then for any pair of non-negative integers (c_l, c_r) such that $c_l + c_r < ord(f(x))$, there exists an (c_l, c_r)-$[[n + c_l + c_r, 2k_1 - n]]_q$ QSC that corrects at least up to $\lfloor \frac{d_1-1}{2} \rfloor$ bit errors and at least up to $\lfloor \frac{d_2-1}{2} \rfloor$ phase errors.*

The resulting $2(n - k_2)$ Pauli operators on n qubits form stabilizer generators S_{D_2} of the Pauli group on n qubits that fixes a subspace of dimension q^{k_2}. Let $S^Z_{D_2}$ denote the set of the Pauli operators on n qubits in S_{D_2}, which include Zs and Is. Let S_{D_2} be an encoder CSS code with parameters $[[n, 2k_2 - n]]$. Let $R = \{r_i(x)|0 < i \leq q^{2k_2-n}\}$ be a system of representatives of the cosets $D_2/D_2^{\perp}$. For any $(2k_2-n)$-qubit state $|\psi\rangle$, we encode the state $|\psi\rangle$ into n-qubit state $|\psi\rangle_{enc} = \sum_i \alpha_i|v_i\rangle$, where each v_i is an n-dimensional vector with the orthogonal basis being $\{|D_2^{\perp} + r_i(x)|r_i(x) \in R\}$. Let U_g denote the unitary operator that adds the coefficient vector g_2 of the generator polynomial $g_2(x)$. Then we have $U_g|\psi\rangle_{enc} = \sum_i \alpha_i|v_i + g_2\rangle$.

Through a unitary transformation using $S^Z_{D_2}$, we can obtain the error syndrome for the window in the same way as when detecting errors with the CSS code defined by S_{D_2} as follows $E|\psi\rangle_{enc}|0\rangle^{\otimes n-k_2} \rightarrow E|\psi\rangle_{enc}|\chi\rangle$, where $|\chi\rangle$ is the $(n-k_2)$-qubit syndrome by $S^Z_{D_2}$ and E is the n-fold tensor product of linear combinations of the Pauli matrices. If E introduced at most $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors on qubits, these quantum errors are detected and then corrected by applying the X operators accordingly. We can refer to [5, 6, 16] for more information of encoding and decoding.

From Section 3, we obtain some cyclic codes $C_{(i,S)}$ and C in Lemma 3.7 with the same length that satisfies $C_{(i,S)} \subset C$. These cyclic codes is a good source to construct QSCs. Put $C_{(i,S)} = D_1$ and $C = D_2$, then we can get positive dimension QSCs if $k_2 > k_1 > \lceil \frac{n}{2} \rceil$ by Lemma 4.4.

From Lemma 4.4, for a QSC, there are four important parameters a_r, a_l, d_1 and d_2, which determine the performance of a QSC. It is clear that the order of the polynomial $f(x)$ is n for $f(x)|(x^n-1)$ and n is an odd prime, where the polynomial $f(x)$ is defined in Lemma 4.4. And we know that the upper bound of the tolerable magnitude of the QSCs are its length n.

From Table 1, It is known that the cyclic codes obtained are usually optimal or almost optimal. Then we can construct many QSCs, which possess good error-correcting capability toward bit error and phase error. What's more, the synchronization capability of those QSCs attain the upper bound. Next we give following theorems.

Theorem 4.5 *Let n be an odd prime with $n \equiv r+1 \pmod{2r}$, where r is a positive even integer. We always assume that $q \in D_0^{(r,n)}$, $s = |S|$ and ℓ is the order of q modulo n. Then for any nonnagetive integer c_r and c_l such that $c_r + c_l < n$, the following sentences are hold.*

(1) *If $s = 1$ and $e = \frac{n-1}{r\ell} \geq 2$, there exists a QSC with parameters $(c_r, c_l) - [[n + c_r + c_l, \frac{(r-2)n+2}{r} + 2p\ell]]_q$, where $0 \leq p \leq e - 2 = \frac{n-2r\ell-1}{r\ell}$.*

(2) *If $s > 1$, there exists a QSC with parameters $(c_r, c_l) - [[n + c_r + c_l, \frac{(r-2s)n+2s}{r} + 2p\ell]]_q$, where $0 \leq p \leq es - 2 = \frac{s(n-1)-2r\ell}{r\ell}$.*

Proof (1) If $s = 1$, we have that the generator $g_{iS}(x)$ of $C_{(i,S)}$ has more than one irreducible factor if and only if $e = \frac{n-1}{r\ell} \geq 2$. From Lemma 3.7, the $C = \langle g(x) \rangle$ and $g(x) = g_{iS}(x)/\prod_{k\in B} m_k(x)$, where B is some proper subset of T_i. Let p be the cardinality of B, where $0 \leq p \leq e-2 = \frac{n-2r\ell-1}{r\ell}$. Then the cyclic code C has parameters $[n, \frac{(r-1)n+1}{r} + p\ell]$. Let $C' = \langle g'(x) \rangle$ and $g'(x) = g_{iS}(x)/\prod_{k\in B'} m_k(x)$, where $B \subset B' \subset T_i$. It is clear that $C \subset C'$. By using the pair cyclic codes (C, C') and Lemma 4.4, there exists a QSC with parameters $(c_r, c_l) - [[n + c_r + c_l, \frac{(r-2)n+2}{r} + 2p\ell]]$, where $0 \leq p \leq e-2 = \frac{n-2r\ell-1}{r\ell}$ and c_r and c_l are arbitrary integers such that $c_r + c_l < n$.

(2) If $s > 1$, we have that the generator $g_{iS}(x)$ of $C_{(i,S)}$ always has more than one irreducible factor. From Lemma 3.7, the $C = \langle g(x) \rangle$ and $g(x) = g_{iS}(x)/\prod_{k\in B} m_k(x)$, where B is some proper subset of $\bigcup_{k\in S} T_k$. Let p be the cardinality of B, where $0 \leq p \leq es - 2 = \frac{s(n-1)-2r\ell}{r\ell}$. Then the cyclic code C has parameters $[n, \frac{(r-s)n+s}{r} + p\ell]$. Let $C' = \langle g'(x) \rangle$ and $g'(x) = g_{iS}(x)/\prod_{k\in B'} m_k(x)$, where $B \subset B' \subset \bigcup_{k\in S} T_k$. It is clear that $C \subset C'$. By using the pair cyclic codes (C, C') and Lemma 4.4, there exists a QSC with parameters $(c_r, c_l) - [[n + c_r + c_l, \frac{(r-2s)n+2s}{r} + 2p\ell]]$, where $0 \leq p \leq es - 2 = \frac{s(n-1)-2r\ell}{r\ell}$ and c_r and c_l are arbitrary integers such that $c_r + c_l < n$. This completes the proof. □

Remark 2 The QSCs constructed in Theorem 4.5 provide the highest possible tolerance against synchronization errors since $\mathrm{ord}(f(x)) = n$.

Example 4.6 Let $(r, n, q) = (2, 19, 7)$ and $S = \{i\}$, we have that $q \in D_0^{(2,19)}$, $e = \ell = 3$, $T_0 = \{1, 4, 5\}$ and $T_1 = \{2, 8, 10\}$. Let $C = \langle d_i(x)\rangle$ with parameters $[19, 10, 8]^*$ for $i \in \{0, 1\}$. Let $C' = \langle d_i(x)/m_j(x)\rangle$ with parameters $[19, 13, 4]$ for $j \in T_i$. Let $C'' = \langle d_i(x)/m_j(x)m_k(x)\rangle$ with parameters $[19, 16, 3]$ for $j \neq k \in T_i$. It is clear that $C \subset C' \subset C''$. By the (1) of Theorem 4.5, for (C, C'), we get a QSC with parameters $(c_r, c_l) - [[19 + c_r + c_l, 1]]_7$ that corrects at least up to 3 bit errors and at least up to 1 phase errors, where $c_r + c_l < 19$. Similarly, for (C', C''), we get a QSC with parameters $(c_r, c_l) - [[19 + c_r + c_l, 7]]_7$ that corrects at least up to 1 bit errors and at least up to 1 phase errors, where $c_r + c_l < 19$.

Example 4.7 Let $(r, n, q) = (6, 31, 2)$, $s_1 = |S_1| > 0$ and $s_2 = |S_2| > 0$, we have that $q \in D_0^{(3,19)}$ and $e = 1$. We obtain the pair of cyclic codes $C_{(i,S_1)}$ and $C_{(i,S_2)}$ for $S_1 \subseteq S_2$. It is clear that $C_{(iS_2)} \subset C_{(iS_1)}$. By the (2) of Theorem 4.5, we get a QSC with parameters $(c_r, c_l) - [[31 + c_r + c_l, 31 - 10s_2 + 10p]]_2$, where $c_r + c_l < 31, 0 \leq p \leq s_2 - 2$ and $2 \leq s_2 \leq 3$. For example, let $(s_1, s_2) = (1, 2)$, then $C_{(iS_1)}$ and $C_{(iS_2)}$ have parameters $[31, 26, 3]^*$ and $[31, 21, 5]^*$, respectively. Then the QSC has parameters $(c_r, c_l) - [[31 + c_r + c_l, 11]]_2$ that corrects at least up to 2 bit errors and at least up to 1 phase errors, where $c_r + c_l < 31$.

5 Conclusion

In this paper, we obtained many optimal or almost optimal dual-containing cyclic codes from the cyclotomic classes of order r. Numerical data showed that in general the parameters of these codes seems good comparing with the Database. These cyclic codes is a great source to construct QECCs and QSCs. Furthermore, we constructed some new QECCs. And we obtained many QSCs with good error-correcting ability toward bit errors and phase errors. It is interesting problem to construct more good QECCs and QSCs in future.

References

1. Aly, S.A., Klappenecker, A.: On quantum and classical BCH codes. IEEE Trans. Inform. Theory **53**, 1183–1188 (2007)
2. Carlet, C., Güneri, C., Mesnager, S., Özbudak, F.: Construction of some codes suitable for both side channel and fault injection attacks. In: Proceedings of International Workshop on the Arithmetic of Finite Fields (WAIFI 2018), Bergen (2018)
3. Carlet, C., Güneri, C., Özbudak, F., Özkaya, B., Solé, P.: On linear complementary pairs of codes. IEEE Trans. Inform. Theory **64**, 6583–6589 (2018)
4. Edel, Y.: Some good quantum twisted codes. Available at, https://www.mathi.uni-heidelberg.de/yves/
5. Fujiwara, Y., Vandendriessche, P.: Quantum synchronizable codes from finite geometries. IEEE Trans. Inf. Theory **60**, 7345–7354 (2014)
6. Fujiwara, Y., Tonchev, V.D., Wong, T.W.H.: Algebraic techniques in designing quantum synchronizable codes. Phy. Rev. A, Gen. Phys. **88**, 012318 (2013)
7. Fujiwara, Y.: Block synchronization for quantum information. Phys. Rev. A, Gen. Phys. **87**, 109–120 (2013)
8. Galindo, C., Hernando, F., Matsumoto, R.: Quasi-cyclic constructions of quantum codes. Finite Fields Their Appl. **52**, 261–280 (2018)
9. Gao, J., Wang, Y.K.: Quantum codes derived from negacyclic codes. Int. J. Theor. Phys. **57**, 682–686 (2018)

10. Gao, J., Wang, Y.: New non-binary quantum codes derived from a class of linear codes. IEEE Access **7**, 26418–26421 (2019)
11. Güneri, C., Özkaya, B., Sayıcı, S.: On linear complementary pair Of *n*D cyclic codes. IEEE Commun. Lett. **22**, 2204–2406 (2018)
12. Kai, X.S., Zhu, S.X.: New quantum MDS codes from negacyclic codes. IEEE Trans. Inform. Theory **59**, 1193–1197 (2013)
13. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Inform. Theory **52**, 4892–4914 (2006)
14. La Guardia, G.: On the construction of nobinary quantum BCH codes. IEEE Trans. Inform. Theory **60**, 1528–1535 (2014)
15. La Guardia, G.G.: Quantum codes derived from cyclic codes. Int. J. Theor. Phys. **56**, 2479–2484 (2017)
16. Luo, L., Ma, Z.: Non-binary quantum synchronizable codes from repeated-root cyclic codes. IEEE Trans. Inf. Theory **64**, 1461–1470 (2018)
17. Ling, S., Luo, J.Q., Xing, C.P.: Generalization of Steane's enlargement construction of quantum codes and applications. IEEE Trans. Inf. Theory **56**, 4080–4084 (2010)
18. Li, L.Q., Zhu, S.X., Liu, L.: Quantum synchronizable codes from the cyclotomy of order four. IEEE Commun. Lett. **21**, 12–15 (2019)
19. Liu, X.S., Yu, L., Liu. H. L.: New quantum codes from Hermitian dual-containing codes. Int J Quantum Inf **17**, 1950006 (2019)
20. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
21. Qian, J.F., Zhang, L.N.: Improved constructions for nonbinary quantum BCH codes. Int. J. Theor. Phys. **56**, 1355–1363 (2017)
22. Xie, Y., Yang, L., Yuan, J.: Q-ary chain-containing quantum synchronizable codes. IEEE Commun. Lett. **20**, 414–417 (2016)
23. Xie, Y., Yuan, Y., Fujiwara, Y.: Quantum synchronizable codes from quadratic residue codes and their supercodes. In: Proc. IEEE Inf. Theory Workshop (ITW), pp. 172–176 (2014)