Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 29 (2026), No. 7, pp. 2205–2216
DOI : 10.47974/JIM-2382

Quantum synchronizable codes through generalized cyclotomy of order 2^r over Z_{2n}

Manju Pruthi [†]
Department of Mathematics
Indira Gandhi University
Meerpur
Rewari 122502
Haryana
India

Arun Kumar Yadav *
School of Basic and Applied Sciences
K. R. Mangalam University
Sohna Road
Haryana
India

Pooja Soni [§]
Department of Mathematics
Indira Gandhi University
Meerpur
Rewari 122502
Haryana
India

Abstract

In this work, we introduce the construction of a generalized cyclotomic class of order 2^r over Z_{2n}, and the work further shows that the resulting codes are cyclic codes containing their dual, along with their augmented counterparts. In addition, the research provides a comprehensive analysis of two categories of quantum synchronization capabilities that can

[†] *E-mail:* **manju.pruthi@yahoo.com**
* *E-mail:* **arun.math.rs@igu.ac.in (Corresponding Author)**
[§] *E-mail:* **pooja.math.rs@igu.ac.in**

reach their maximum potential in specific circumstances. The error correction capacity of the proposed quantum synchronizable codes includes both bit errors and phase errors.

Subject Classification: *94B05, 94B15, 94B50.*

Keywords: *Cyclotomic classes, Dual containing codes, QECC's.*

1. Introduction

The rapid advancement of quantum technologies has firmly positioned quantum computing and communication as pivotal areas of modern scientific research. At the core of this progress lies quantum information theory, which has achieved significant breakthroughs in addressing one of the most critical challenges in quantum systems: mitigating the effects of noise and decoherence. Among the most important innovations in this field are $QECC's$which serve as essential tools for preserving quantum information by counteracting errors that occur during computation or transmission. These codes rely on the mathematical framework of "Pauli operators (I, X, Y, Z)" to model and correct disturbances in quantum channels effectively. The implementation of $(QECC's)$ is crucial for advancing quantum computing & the guaranteeing of the dependability of quantum communication. Using these codes enhances the storage and transmission of quantum information, making quantum computing reliable by reducing the impact of noise.

Quantum synchronizable codes $(QSC's)$ serve as specialized quantum error-correction codes $(QECC's)$ that may effectively rectify the impact on qubits of quantum noise and address misalignment issues in block synchronization [1]. A further source of error lies in the misalignment between the qubit stream and the block structure. Quantum information processing may experience catastrophic failure, leading to potential misidentification of the border of an information block by the quantum information receiver.

Fujiwara [2] introduced a novel technique for constructing $QSC's$ through cyclic codes. Subsequently, Fujiwara, Tonchev, and Wong [3] refined this framework using an algebraic approach. Fujiwara and Vandendriessche [4] initiated $QSC's$ from finite geometric codes. The study conducted by Li, Zhu, and Liu [5] focused on two types of $QSC's$ based on cyclic codes and their connection to fourth-order cyclotomic classes. Furthermore, Pang et al. [6] investigated cyclotomy of order r and created $QSC's$ with optimal synchronization. Wang et al. [7] introduced new for generating two different categories of $QSC's$ from cyclic codes by 2-order cyclotomy over Z_{2q}. Additionally, Dinh, Nguyen, and Yamaka [8] applied CSS and Hermitian constructions to define quantum MDS codes and also developed $QSC's$ of length $2p^s$ of negacyclic code over F_{p^m}. Annamalai and Durairajan [9] developed the concept of the *exponent* of a cyclic code over a finite field and explored its properties in relation to the dual codes. They showed that for a cyclic code and its dual, the exponent of the dual code is given by $n = lcm(e, r)$, where e and r denote the exponents of the code and its dual, respectively. Heboub et al. [10] gave the structure of minimal and maximal cyclic codes of length $2p$ over finite

fields F_q, where p and q are distinct odd primes. They proved that every maximal cyclic code of length $2p$ can be expressed as a direct sum of three minimal cyclic codes. Bhowmick *et al.* [11] investigated linear complementary pairs (LCP) and checkable group codes over finite non-commutative Frobenius rings**,** providing conditions under which one code in an LCP is equivalent to the other. Recently, Yadav, Pruthi, and Kumar [12] constructed quaternary cyclotomy over Z_{2n} for quantum synchronizable codes.

Paper organization: In section 1 give the elementary concepts of quantum synchronization coding, laying the groundwork for the study. In section 2 explores the essential results concerning cyclic codes & their duals. In section 3, we construct a generalized cyclotomic class of order 2^r over Z_{2n}. In section 4 focuses on deriving cyclic codes using generalized cyclotomy, with particular attention to dual-containing cyclic codes $(DCC's)$ over Z_{2n}, exploring their structure and their augmented. In section 5 presents the construction of quantum codes using the CSS framework. In section 6, we formulate two $QSC's$ variants and systematically assess their decoding capabilities, proving their optimality against established performance bounds. The cyclic codes' minimum distances are algorithmically verified using Magma's computational algebra software, providing empirical reinforcement to theoretical claims. Eventually, Section 7 concludes the paper.

2. Preliminaries

Consider F_r denote a finite field, with$r$ being a prime number. A linear code $C = [n, k, d]_r$ is a subspace of dimension k in F_r^n, among the minimum distance d defined as:$d = min\{wt(v): v \in C, v \neq 0\}$.

Definition 2.1: A linear code C over F_r, be termed as a cyclic code if, for each codeword $c = (c_0, c_1, c_2, \dots, c_{n-1}) \in C$, the cyclic shift of its coordinates also belongs to C, that is, $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$. To associate the code to polynomial representation, consider the ideal:

$$I(C) = \{\sum_{i=0}^{n-1} c_i x^i : (c_i) \in C\}$$

Then, its ideal representation $\frac{F_r[x]}{\langle x^n-1\rangle}$. Therefore, the cyclic code C is cleverly constructed by a monic polynomial $g(x)$ of degree $(n-k)$. Moreover, $g(x)|(x^n-1)$. Let $C = \langle g(x)\rangle$ and the Euclidean inner product (EIP) $\langle x, y\rangle = \sum_{i=0}^{n-1} x_i y_i$. The Euclidean dual associated with a code C given as $C^{\perp} = \{x \in F_r^n : (x, c) = 0, \forall\, c \in C\}$ and the dimension of this dual space is $(n-k)$.

Definition 2.2: Let C repersent a cyclic code with a generator polynomial $(g.p.), g(x)$ such that $\deg\big(g(x)\big) = n-k$. It follows that $g(x)/\langle x^n-1\rangle$. The parity check polynomial of C is given by $h(x) = (x^n-1)/g(x)$. The generator poly. of the dual code $C^{\perp}$ is given by, $\tilde{h}(x) = h(0)^{-1}.x^k.h(x^{-1})$ (1), where $\tilde{h}(x)$ is reciprocal polynomial of $h(x)$.

Consider $C_1 = [n, k_1]_r$, and $C_2 = [n, k_2]_r$ are cyclic codes, where $k_1 < k_2$. If $C_1 \subseteq C_2$, then C_2 is said to be C_1- containing. If $C_2^{\perp} \subset C_2$, then C_2 is called dual-containing. If $C_1 \subseteq C_2$, then $g_2(x)$ can divide any codeword of C_1.

3. Construction of generalized cyclotomy of order 2^r

Let n be an odd prime with $n = 2^r t + 1(\ t \geq 1)$, and we fix α as primitive root mod (n).

Define $N_i^{(n)} = \{\alpha^{2^r s+i} : 0 \leq s \leq \frac{\phi(n)}{2^r} - 1 \ for\ i = 0, 1, 2, \dots, (2^r - 1)\}$, where these sets represent quadratic residue &non-residues sets.

Definition 3.1. Take α so that it acts as a primitive element for the arithmetic of both n and $2n$ (that is,α generates the multiplicative group Z_n^* as well as Z_{2n}^*). Its multiplicative order with respect to the modulus $2n$ equals $(n-1)$. The quaternary cyclotomic classes defined within $\mathbb{Z}_{2n}$are then given by,

$$N_i^{(2n)} = \{\alpha^{2^r s+i} : 0 \leq s \leq \frac{\phi(n)}{2^r} - 1 \ and\ i = 0,1,2, \dots 2^r - 1\}$$

$$T_i^{(2n)} = 2A_i^{(n)} = \{2v : v \in N_i^{(2n)}, i = 0,1,2, \dots 2^r - 1\}.$$

We have $Z_{2n}^* = \bigcup_{i=0}^{2^r-1} N_i^{(2n)} \bigcup_{i=0}^{2^r-1} T_i^{(2n)} \cup \{n\}, Z_n^* = \bigcup_{i=0}^{2^r-1} N_i^{(n)}$

Since all the $n-1$ elements in $\bigcup_{i=0}^{2^r-1} T_i^{(2q)}$ are even, it follows that each of the $n-1$ elements in the corresponding union $\bigcup_{i=0}^{2^r-1} N_i^{(2q)}$ must be odd.

Lemma 3.2: *Based on the notations introduced above; we have*

a) $N_i^{(2n)} = -N_{i+k(mod 2^r)}^{(2n)}$

b) $T_i^{(2n)} = -T_{i+k(mod 2^r)}^{(2n)}$, *where* $i, k \in \{0,1,, \dots 2^r - 1\}$.

We choose a primitive $2n$-th root of unity, denoted by β, that lies in the field $\mathbb{F}_{p^m}$.Here $m$is selected so that $p$has multiplicative order $m$when considered modulo $2n$.For each index $i$belonging to $\{0,1, \dots, 2^r - 1\}$, the polynomials $g_{A_i}^{(2n)}(x)$and $g_{R_i}^{(2n)}(x)$over $\mathbb{F}_p$are introduced as follows

$$g_{n_i^{(2n)}}(x) = \prod_{j \in N_i^{(2n)}} (x - \beta^j),\ g_{T_i^{(2n)}}(x) = \prod_{j \in T_i^{(2n)}} (x - \beta^j)\ (2),$$

where $i \in \{0,1, n+1, \dots, 2^r - 1\}$.

4. Cyclic codes by generalized cyclotomy of order 2^r

This part preset the construction and properties of a specific class of codes, like dual-containing cyclic codes formed through the use of generalized cyclotomy of order 2^r over Z_{2n}. Also, we associated $ACC's$ and analyzed their minimum Hamming distances.

4.2 *Dual containing codes* ($DCC's$)

Let β be a $2n$-th primitive root of unity in the finite field F_{p^m}, where $p \in N_0^{(2n)}$, and $m = ord_{2n}(p)$ denotes the multiplicative order of p mod$(2n)$. Since $\beta^{2n} = 1$ over F_{p^m}, $\beta^n = -1$. Here,

$$x^{2n} - 1 = \prod_{j=0}^{2n-1}(x - \beta^j) = (x+1)(x-1)\prod_{i=0}^{2^r-1} g_{N_i^{(2n)}}(x)\, g_{T_i^{(2n)}}(x) \quad (3)$$

Let the cyclic codes $C_{N_i^{(2n)}}$, $C_{T_i^{(2n)}}$, $C_{N_iT_j^{(2n)}}$ generated by these polynomials. The generators can be expressed as $g_{N_i^{(2n)}}(x), g_{T_i^{(2n)}}(x)$, $g_{N_i^{(2n)}}(x) g_{T_j^{(2n)}}(x)$ resp., where $i, j \in \{0,1, \dots 2^r - 1\}$.

Lemma 4.2: *Let* $n = 2^r t + 1 (t \geq 1)$ *is an odd prime. Then,*

$a)\ (C_{N_i^{(2n)}})^{\perp} \subset C_{T_i^{(2n)}}$, b) $(C_{N_i^{(2n)}})^{\perp} \subset C_{T_i^{(2n)}}$, $c)\ (C_{N_iT_j^{(2n)}})^{\perp} \subset C_{N_iT_j^{(2n)}}$

Proof: Using equation (1), the recip. poly. of $g_{N_i^{(2n)}}(x)$ is given by

$$\tilde{g}_{N_i^{(2n)}}(x) = \left(g_{N_i^{(2n)}}(0)\right)^{-1} x^{deg\left(g_{N_i^{(2n)}}(x)\right)} g_{N_i^{(2n)}}(x^{-1})$$

Now, $g_{N_i^{(2n)}}(x) = (x - \beta^{v_{i_1}})(x - \beta^{v_{i_2}}) \dots (x - \beta^{v_{i_{\frac{e}{2}}}})$

Then

$$\tilde{g}_{N_i^{(2n)}}(x) = (-\beta^{v_{i_1}})^{-1}(-\beta^{v_{i_2}})^{-1} \dots \left(-\beta^{v_{i_{\frac{e}{2}}}}\right)^{-1} . x^{\frac{e}{2}} .$$

$$(x^{-1} - \beta^{v_{i_1}})(x^{-1} - \beta^{v_{i_2}}) \dots (x^{-1} - \beta^{v_{i_{\frac{e}{2}}}})$$

$$= (x - \beta^{-v_{i_1}})(x - \beta^{-v_{i_2}}) \dots (x - \beta^{-v_{i_{\frac{e}{2}}}})$$

According to Lemmas 3.2, $N_i^{(2n)} = -N_{i+k(mod 2^r)}^{(2n)}$, then $\tilde{g}_{N_i^{(2n)}}(x) = g_{N_{i+k}^{(2n)}}(x)$, where $i = \{0,1,2, \dots, 2^r - 1\}$ (4)

Since $-T_i^{(2n)} = T_{i+k(mod 2^r)}^{(2n)}$, it is obvious that

$$\left(-N_i^{(2n)}\right) \cup \left(-T_j^{(2n)}\right) = \left(N_{i+k(mod 2^r)}^{(2n)}\right) \cup \left(T_{j+k(mod 2^r)}^{(2n)}\right).$$

Then

$$\tilde{g}_{N_i^{(2n)}}(x) = g_{N_{i+k}^{(2n)}}(x),\ \tilde{g}_{N_i^{(2n)}}(x)\tilde{g}_{T_j^{(2n)}}(x) = g_{N_{i+k}^{(2n)}}(x) g_{T_{j+k}^{(2n)}}(x) \quad (5)$$

Consequently, the parity-check polynomial corresponding $C_{A_i}^{(2n)}$ is:

$$h(x) = \frac{x^{2n}-1}{g_{N_i^{(2n)}(x)}} = (x-1)(x+1) g_{N_{i+k}^{(2n)}}(x) \prod_{i=0}^{2^r-1} g_{T_i^{(2n)}}(x)$$

and using equation (1) and (4),

$$\tilde{h}(x) = (x-1)(x+1)g_{N_i^{(2n)}}(x)\prod_{i=0}^{2^r-1} g_{T_i^{(2n)}}(x).$$

Thus the dual of $C_{N_i}^{(2n)}$is generated by the reciprocal polynomial $\tilde{h}(x)$. Observing that $\tilde{h}(x)$ divides $g_{N_i}(x)$, it follows directly that $(C_{N_i}^{(2n)})^{\perp} \subset C_{N_i}^{(2n)}$. The remaining statements of this result follow immediately from this inclusion.

4.3 *Cyclotomy Cosets*

Consider p as a prime number satisfying $p = \alpha^{2^r k} \in N_0^{(2n)}$and $gcd(p, 2n) = 1$. The set of elements forming the collection of integers obtained by repeatedly multiplying s by p and reducing modulo $2n$ is described as:

$$C_{(s,2n)} = \{sp^i mod 2n : i \in N\}, \quad (6)$$

The order of p is given by $ord_{2n}(p) = |p| = \frac{|\alpha|}{gcd(|\alpha|,2^r k)} = \frac{|q-1|}{gcd(|q-1|,2^r k)}$. If $|p| = l_k$ then $sp^{l_m} \cong s \; mod \; 2n$. Furthermore $2n/s(p^{l_k} - 1)$, leading to the following lemma:

Lemma 4.4: [7] *Suppose that* $p = \alpha^{2^r k} \in N_0^{(2n)}$ *is an odd prime.* $\left|C_{(s,2n)}\right|$ *repersents the cardinality of* $C_{(s,2n)}$. *If* $l_m \leq l_k$ *is an integer, satisfies* $sp^{l_m} \cong s \; mod \; 2n$, *then*

$$\left|C_{(s,2n)}\right| = \begin{cases} l_m = 1, \text{if } \gcd(2n, s) = n \\ l_m = l_k, otherwise \end{cases}$$

4.4 *Augmented cyclic codes* $(ACC's)$

A cyclic code $C' = \langle g'(x)\rangle$ is referred to as an $ACC's$ of $C = \langle g(x)\rangle$ if $C \subset C'$. Then, $g'(x)/g(x)$ represents a unique irreducible polynomial of β^s in $F_p[x]$,

$$U_s(x) = \prod_{j \in C_{(s,2n)}} (x - \beta^j)$$

Lemma 4.6: *Consider the cyclic codes* $C_{N_i^{(2n)}} = \langle g_{N_i^{(2n)}}(x)\rangle$. *If the size of* $C_{(1,2n)}$ *is* l_k, *then the gen. poly.*$g_{N_i^{(2n)}}(x)$ *may be indicated as the product of* $\tau = \frac{n-1}{2^r l_k}$ *irreducible poly. of degree* l_k *over* $F_p[x]$ *as follows:* $g_{N_i^{(2n)}}(x) = \prod_{j=1}^{\tau} U_{d_{i_j}}(x)$, *where* d_{i_j} *are some numbers such that* $N_i^{(2n)} = \bigcup_{j=1}^{\tau} C_{(d_{i_j},2n)}$, *and* $deg\left(U_{d_{i_j}}\right) = l_k \forall \; d_{i_j}$.

Proof: For an odd prime n, the cyclotomic coset cardinality satisfies $\left|C_{(1,2n)}\right| = l_k$. From Lemma 4.4, for any integer $s \in \{1,2,\ldots,n-1,n+1,\ldots,2n-1\}$, we have $\left|C_{(s,2n)}\right| = l_k$. Since $p \in N_0^{(2n)}$, it follows that $N_i^{(2n)} = \bigcup_{j=1}^{\tau} C_{(d_{i_j},2n)}$,

where $d_{i_1}, d_{i_2}, \dots, d_{i_\tau} \in \{1, n+1, \dots 2n-1\}$. Moreover, we have $\tau = \frac{\left|N_i^{(2n)}\right|}{\left|C_{(i,2n)}\right|} = \frac{n-1}{2^r l_k}$.□

Example 4.7: Consider the cyclotomic classes of order eight modulo 146.

$N_0^{(146)} = \{1, 75, 77, 81, 89, 105, 137, 55, 37\}$,
$T_0^{(146)} = \{2, 4, 8, 16, 32, 64, 128, 110, 74\}$,
$N_1^{(146)} = \{5, 83, 93, 113, 7, 87, 101, 129, 39\}$,
$T_1^{(146)} = \{10, 20, 40, 80, 14, 28, 56, 112, 78\}$,
$N_2^{(146)} = \{25, 123, 27, 127, 35, 143, 67, 61, 49\}$,
$T_2^{(146)} = \{50, 100, 54, 108, 70, 140, 134, 122, 98\}$
$N_3^{(146)} = \{125, 31, 135, 51, 29, 131, 43, 13, 99\}$,
$T_3^{(146)} = \{104, 62, 124, 102, 58, 116, 86, 26, 52\}$,
$N_4^{(146)} = \{41, 9, 91, 109, 145, 71, 69, 65, 57\}$,
$T_4^{(146)} = \{82, 18, 36, 72, 144, 142, 138, 130, 114\}$,
$N_5^{(146)} = \{59, 45, 17, 107, 141, 63, 53, 33, 139\}$,
$T_5^{(146)} = \{118, 90, 34, 68, 136, 126, 106, 66, 132\}$,
$N_6^{(146)} = \{3, 79, 85, 97, 121, 23, 119, 19, 111\}$,
$T_6^{(146)} = \{6, 12, 24, 48, 96, 46, 92, 38, 76\}$
$N_7^{(146)} = \{15, 103, 133, 47, 21, 115, 11, 95, 117\}$,
$T_7^{(146)} = \{30, 60, 120, 94, 42, 84, 22, 44, 88\}, \{74\}$

Let $p = \alpha^{8k} \in N_0^{(2n)}$, where $k = \{0\ to\ 16\}$ and $ord_{2n}(p) = |p| = \frac{|\alpha|}{gcd(|\alpha|, 4k)} = \frac{|n-1|}{gcd(|n-1|, 8k)}$. For $k = 6, \alpha = 5$, we have $p = 5^{48} = 137$ and $|p| = \frac{72}{gcd(72,48)} = 3$. Then by (6), the cyclotomy cosets modulo 146 is

$C_{(1,146)} = \{81, 137, 1\}, C_{(2,146)} = \{16, 128, 2\}, C_{(3,146)} = \{97, 119, 3\},$
$C_{(4,146)} = \{32, 110, 4\}, C_{(5,146)} = \{113, 101, 5\}, C_{(6,146)} = \{48, 92, 6\},$
$C_{(10,146)} = \{145, 65, 10\}, C_{(7,146)} = \{129, 83, 7\}, C_{(8,146)} = \{64, 74, 8\},$
$C_{(9,146)} = \{64, 74, 8\}, C_{(11,146)} = \{15, 47, 11\}, C_{(12,146)} = \{96, 38, 12\},$
$C_{(13,146)} = \{31, 29, 13\}, C_{(14,146)} = \{112, 20, 14\}, C_{(17,146)} = \{63, 139, 17\},$
$C_{(18,74)} = \{144, 130, 18\}, C_{(19,146)} = \{79, 121, 19\}, C_{(21,146)} = \{95, 103, 21\},$
$C_{(22,146)} = \{30, 94, 22\}, C_{(23,146)} = \{111, 85, 23\}, C_{(24,146)} = \{46, 76, 24\},$

$C_{(25,146)} = \{127,67,25\},\ C_{(26,146)} = \{62,58,26\},\ C_{(27,146)} = \{143,49,27\},$
$C_{(28,146)} = \{78,40,28\}, C_{(33,146)} = \{45,141,33\}, C_{(34,146)} = \{126,132,34\},$
$C_{(35,146)} = \{61,123,35\}, C_{(36,146)} = \{142,114,36\}, C_{(37146)} = \{77,105,37\},$
$C_{(39,146)} = \{93,87,39\}, C_{(41,146)} = \{109,69,41\}, C_{(42,146)} = \{44,60,42\},$
$C_{(43,146)} = \{125,51,43\}, C_{(50,146)} = \{108,134,50\}, C_{(52,146)} = \{124,116,52\},$
$C_{(53,146)} = \{59,107,53\}, C_{(54,146)} = \{140,98,54\}, C_{(55,146)} = \{75,89,55\},$
$C_{(57,146)} = \{91,71,57\}, C_{(59,146)} = \{107,53,59\}, C_{(66,146)} = \{90,136,66\},$
$C_{(68,146)} = \{106,118,68\}, C_{(70,146)} = \{122,100,70\}, C_{(72,146)} = \{138,82,72\},$
$C_{(73,146)} = \{73\}, C_{(84,146)} = \{88,120,84\}, C_{(86,146)} = \{104,102,86\},$
$C_{(99,146)} = \{135,131,99\}, C_{(115,146)} = \{117,133,115\}.$

Thus $N_0^{(146)} = C_{(1,146)} \cup C_{(37,146)} \cup C_{(55,146)}$ which is equivalent to $g_{N_0^{(146)}} = U_1(x)U_{37}(x)U_{55}(x)$.

Similarly,

$$N_1^{(146)} = \bigcup_{i=5,7,39} C_{(i,146)}, N_2^{(146)} = \bigcup_{i=25,27,35} C_{(i,146)},$$
$$N_3^{(146)} = \bigcup_{i=13,43,99} C_{(i,146)}, N_4^{(146)} = \bigcup_{i=9,41,57} C_{(i,146)},$$
$$N_5^{(146)} = \bigcup_{i=17,33,53} C_{(i,146)},\ N_6^{(146)} = \bigcup_{i=3,19,23} C_{(i,146)},$$
$$N_7^{(146)} = \bigcup_{i=11,47,115} C_{(i,146)}$$
$$T_0^{(146)} = \bigcup_{i=2,4,8} C_{(i,146)}, T_1^{(146)} = \bigcup_{i=10,14,28} C_{(i,146)},$$
$$T_2^{(146)} = \bigcup_{i=50,54,70} C_{(i,146)},\ T_3^{(146)} = \bigcup_{i=26,52,23} C_{(i,146)},\ T_4^{(146)} = \bigcup_{i=18,36,72} C_{(i,146)}, T_5^{(146)} = \bigcup_{i=34,66,68} C_{(i,146)},\ T_6^{(146)} = \bigcup_{i=6,12,24} C_{(i,146)},$$
$$T_7^{(146)} = \bigcup_{i=22,42,84} C_{(i,146)}.$$

It becomes evident that $C'_{N_0} = \langle U_s(x) \rangle$ the $ACC's$of $C_{N_0^{(146)}}$ for$s \in \{1,37,55\}$.

Lemma 4.8: [6] *Suppose that* n *be the odd prime of the form* $(2^r t + 1)$ *be an odd prime, where* $t \in N$ *and* $C_{N_i^{(2n)}}$, $C_{T_i^{(2n)}}$ *and* $C_{N_i T_j^{(2n)}}$ *be the DCC's for* $i, j \in \{0,1,2, \dots, 2^r\}$, *then*

a) If $C'_{N_i} = \langle \frac{g_{N_i^{(2n)}}(x)}{\prod i \in P U_i(x)} \rangle$, then $C_{N_i^{(2n)}} \subset C'_{N_i}$, where $P \subset \{d_{i_1}, d_{i_2}, \dots, d_{i_\tau}\}$.

b) If $C'_{T_i} = \langle \frac{g_{T_i^{(2n)}}(x)}{\prod i \in Q U_i(x)} \rangle$, then $C_{T_i^{(2n)}} \subset C'_{T_i}$, where $Q \subset \{e_{i_1}, e_{i_2}, \dots, e_{i_\tau}\}$.

c) If $C'_{N_i T_j} = \langle \frac{g_{N_i^{(2n)}}(x) g_{T_i^{(2n)}}(x)}{\prod i \in T U_i(x)} \rangle$, then $C_{N_i T_j^{(2n)}} \subset C'_{N_i T_j}$, where $T \subset \{d_{i_1}, d_{i_2}, \dots, d_{i_\tau}\} \cup \{e_{i_1}, e_{i_2}, \dots, e_{i_\tau}\}$.

Example 4.9: Let n be an odd prime with $n = 16t + 9$, and $p \in N_0^{(2n)}$. In Table 1, we illustrate cyclic codes and their dual, and all computations from MAGMA [13].

Table 1

Codes	$g(x)$	Duals
$C_{N_0}^{(146)} = [146, 144, 2]_{73}$	$(x+1)(x+72)$	$C_{N_0}^{(146)^\perp} = [146, 2, 73]_{73}$
$C_{T_0}^{(146)} = [146, 144, 2]_{73}$	$(x+1)(x+72)$	$C_{T_0}^{(146)^\perp} = [146, 2, 73]_{73}$

5. Quantum codes design via CSS construction method:

This section presents foundational principles for constructing quantum error-correcting codes through the framework of dual-containing cyclic codes. As demonstrated in the following lemma, CSS method provides a systematic approach to generating quantum codes from classical linear codes. Specifically, by leveraging the structural properties of dual-containing cyclic codes, this technique enables the derivation of multiple classes of quantum codes with controlled error-correction capabilities.

Lemma 5.1: [14] *(CSS Construction) If* $\exists$ *a classical linear code* C, $[n, k, d]_p$ *s.t.*$C^\perp \subset C$, *then* $\exists$ *an quantum codes* $\left[[n, 2k-n, \geq d]\right]_p$.

Example 5.2: Consider $2n = 2(8t+5) = 146$, and $137 \in N_0^{(146)}$. The cyclic code $C_{N_i}^{(2n)}$, defined by generator polynomial by $g_{N_i}^{(2n)}(x)$, possesses the parameters $[146, 144, 2]_{73}$, we get quantum code $[146, 142, \geq 2]_{146}$.

6. Quantum synchronizable codes from cyclic codes

Lemma 6.1: [15] The two cyclic codes$C_1 = \langle g_1(x) \rangle$ & $C_2 = \langle g_2(x) \rangle$ with parameters $[n, k_1, d_1]_p$, and $[n, k_2, d_2]_p$ over F_p, where $k_1 > k_2$. This implies that C_2 *is a subset of* C_1 and ${C_2}^\perp \subseteq C_1$. Define $f(x) = \frac{g_2(x)}{g_1(x)}$over $\frac{F_p[x]}{\langle x^n - 1 \rangle}$. Any pair of non-negative integers ϱ_l, ϱ_r with $\varrho_l + \varrho_r < ord\big(f(x)\big)$, then $\exists$ a(ϱ_l,ϱ_r) $-\left[[n + \varrho_l + \varrho_r, 2k_2 - n]\right]$ $QSCs$, it corrects both errors up to $\lfloor \frac{d_1 - 1}{2} \rfloor$.

6.2 *Maximum misalignment tolerance*

By Lemma 6.1, the $ord(f(x))$ influences the ability of $QSC's$ to misalignment errors. $QSC's$ requires cyclic codes that not only maintain sufficient minimum distances but also ensure the $ord(f(x))$ remains as large as possible. Given that $f(x) = \frac{g_2(x)}{g_1(x)}$, and $g_1(x)/(x^n - 1)$, $g_2(x)/(x^n - 1)$, then $f(x)/(x^n - 1)$. Consequently, the upper limit for the achievable magnitude of $QSC's$ is determined by their length n.

Theorem 6.3: *Let* $n = 2^r t + 1$ *is an odd prime,* $p \in N_0^{(2n)}$*, and* $ord_{2n}(p) = l_k$*,* $\tau = \frac{n-1}{2^r l_k}$*, Then for* $n \in N$ *such that* $\varrho_l + \varrho_r < 2n$*, there exists a QSCs,* $(\varrho_l, \varrho_r) - [[2n + \varrho_l + \varrho_r, 2ul_k + n + 1]]_p$*, where* $0 \le u \le \tau - 2^r = \frac{n-2^{r+1}l_k-1}{2^r l_k}$.

Proof: If n be an odd prime of the form $2^r t + 1$, then $|N_i^{(2n)}| = |T_i^{(2n)}| = \frac{n-1}{2^r} = 2t + 1$. By Lemma 4.6, $|C_{(s,2n)}| = l_k$ for any $s \in \{1, n + 1, \ldots, 2n - 1\}$, and $l_k \,|(2t + 1)$. Then, $C_{N_i^{(2n)}}$ under these conditions, one can extend the code $C_{N_i}^{(2n)}$to obtain its augmented variants. The generator polynomial $g_{N_i}^{(2n)}(x)$ contains no fewer than $2t + 1$ irreducible components when viewed over $\mathbb{F}_p$.. If $= \frac{n-1}{2^r l_k}$, then based on Lemma 4.8 (a), $C_{N_i^{(2n)}}$ has an augmented code C'_{N_i}, $[2n, 2n - (\frac{n-1}{2^r} - |P|l_k)]_p = [2n, \frac{(2^r-1)n+1}{2^r} + |P|l_k)]_p$. Moreover, let P' be one more set with P is contained in $P' \subset \{d_{i_1}, d_{i_2}, \ldots, d_{i_\tau}\}$ then the parameter of augmented cyclic code C''_{N_i} of C'_{N_i}, is $[2n, \frac{(2^r-1)n+1}{2^r} + |P'|l_k)]_p$. Let $|P'| = u$. Since $|P| < |P'| < \tau$, then $0 \le u \le \tau - 2^r = \frac{n-(2^{r+1})l_k-1}{2^r l_k}$. Furthermore, since $ord(U_s(x)) = 2n$ where $s \in \bigcup_{i=0}^{3} N_i^{(2n)}$, consequently the $QSC's$ obtained by $C_{N_i^{(2n)}}$ and their $ACC's$ achieve the optimal synchronization limit. Based on Lemma 6.1, we get $QSCs$, $(\varrho_l, \varrho_r) - [[2n + \varrho_l + \varrho_r, 2ul_k + n + 1]]_p$, where $\varrho_l + \varrho_r < 2n$.

The cyclic code $C_{N_i T_j^{(2n)}}$ can be leveraged along side $ACC's$ to create 2nd class of $QSC's$ offering superior synchronization performance.

Theorem 6.4: *Let* $n = 2^r t + 1$ *is an odd prime,* $p \in N_0^{(2n)}$*,* $ord_{2n}(p) = l_k$*,* $\tau = \frac{n-1}{2^r l_k}$*, then for any nonnegative integers* ϱ_l *and* ϱ_r *with* $\varrho_l + \varrho_r < 2n$*,* $\exists$ *a quantum synchronizable code,* $(\varrho_l, \varrho_r) - \left[[2n + \varrho_l + \varrho_r, 2vl_k + 2^r]\right]_p$*, where* $0 \le v \le \tau - 2^r = \frac{n-2^{r+1}l_k-1}{2^r l_k}$.

Proof: Since $n = 2^r t + 1$ is an odd prime, then $\left|N_i^{(2n)}\right| = \left|T_i^{(2n)}\right| = \frac{n-1}{2^r} = 2t + 1$. By Lemma 4.6, $\left|C_{(s,2n)}\right| = l_k$ for any $s \in \{1, n + 1, \ldots, 2n - 1\}$, and $l_k \,|(2t + 1)$. Then, $DCC's C_{N_i T_j^{(2n)}}$ has $AC's \Leftrightarrow g_{N_i^{(2n)}}(x) g_{T_i^{(2n)}}(x)$ has at least $\tau = \frac{2^r(2t+1)}{2^r l_k}$ irreducible factors over F_p. By Lemma 4.8 (c), "DCC" $C_{N_i T_j^{(2n)}}$ has an "AC" $C'_{N_i T_j}[2n, n + |T|l_k + 1]_p$. Choose a second subset P' such that the earlier set T is included in T', where T' is drawn from $\{d_{i_1}, d_{i_2}, \ldots, d_{i_\tau}\} \cup \{e_{i_1}, e_{i_2}, \ldots, e_{i_\tau}\}$. Under this choice $ACC's$ $C''_{N_i T_j}$ of $C'_{N_i T_j}$ is $[2n, n + |T'|l_k + 1]$.

Taking $|T'| = v$. Since $|T| < |T'| < 2\tau$, then $0 \leq v \leq 2\tau - 2^r = \frac{n-8l_k-1}{2^r l_k}$. Since $ord(U_s(x)) = 2n$ where $s \in \bigcup_{i=0}^{2^r-1} N_i^{(2n)}$. Consequently, the synchronization capability of $QSC's$ obtained through $C_{N_i T_j^{(2n)}}$ and their $ACC's$ reach the upper bound. Applying lemma 6.1, we derive a$QSC(\varrho_l, \varrho_r) - [[2n + \varrho_l + \varrho_r, 2vl_k + 2^r]]_p$, where $\varrho_l + \varrho_r < 2n$.

7. Conclusion

This paper delves into two distinct classes of $QSC's$ using from DCC's using generalized cyclotomy of order 2^r. The analysis highlights that these $QSCs$ exhibit a remarkable ability to tolerate misalignment errors, achieving synchronization capacities that approach the theoretical upper bound under certain optimal conditions. To further evaluate their error-correcting capabilities, the Magma Algebra System extensively computes and analyzes the minimum distance between distinct codewords in the supporting cyclic codes structure. This rigorous computational approach provided deeper insights into the structural properties. It enhanced the accuracy of the performance assessment of the proposed $QSCs$, solidifying their potential applications in quantum communication systems where synchronization errors are critical.

References

[1] T. Wang, T. Yan, V. Sidorenko, and X. Wang, "Quantum synchronizable codes from cyclotomic classes of order two over Z_(2q)," arXiv preprint arXiv:2106.02470, pp. 1–9 (2021).

[2] Y. Fujiwara, "Block synchronization for quantum information," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 87, no. 2 (2013), doi: 10.1103/PhysRevA.87.022344.

[3] Y. Fujiwara, V. D. Tonchev, and T. W. H. Wong, "Algebraic techniques in designing quantum synchronizable codes," *Phys. Rev. A*, vol. 88, no. 1, p. 012318 (Jul. 2013), doi: 10.1103/PhysRevA.88.012318.

[4] Y. Fujiwara and P. Vandendriessche, "Quantum Synchronizable Codes From Finite Geometries," *IEEE Trans. Inf. Theory,* vol. 60, no. 11, pp. 7345–7354 (Nov. 2014), doi: 10.1109/TIT.2014.2357029.

[5] L. Li, S. Zhu, and L. Liu, "Quantum Synchronizable Codes From the Cyclotomy of Order Four," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 12–15 (2019), doi: 10.1109/LCOMM.2018.2877989.

[6] B. Pang, S. Zhu, J. Li, and L. Li, "New Quantum Codes Derived from Cyclic Codes," *Int. J. Theor. Phys.*, vol. 59, no. 4, pp. 1058–1068 (2020), doi: 10.1007/s10773-020-04388-2.

[7] T. Wang, T. Yan, V. Sidorenko, and X. Wang, "Quantum Synchronizable Codes From Cyclotomic Classes of Order Two over Z_{2q}," https://arxiv.org/abs/2106.02470, pp. 1–9 (2021).

[8] H. Q. Dinh, B. T. Nguyen, and W. Yamaka, "Quantum MDS and Synchronizable Codes From Cyclic and Negacyclic Codes of Length 2 p s Over F p m," *IEEE Access,* vol. 8, pp. 124608–124623 (2020), doi: 10.1109/ACCESS.2020.3006001.

[9] N. Annamalai and C. Durairajan, "Exponent of cyclic codes over Fq," *J. Discret. Math. Sci. Cryptogr.,* vol. 26, no. 1, pp. 115–120 (2023), doi: 10.1080/09720529.2021.1933707.

[10] L. Heboub and D. Mihoubi, "Minimal and maximal cyclic codes of length 2p," *J. Discret. Math. Sci. Cryptogr.*, vol. 27, no. 1, pp. 63–74 (2024), doi: 10.47974/JDMSC-1569.

[11] S. Bhowmick, J. de la Cruz, E. Martınez-Moro, and A. Sharma, "On LCP and checkable group codes over finite non-commutative Frobenius rings," *J. Discret. Math. Sci. Cryptogr.,* vol. 28, no. 3, pp. 891–905 (2025), doi: 10.47974/JDMSC-2187.

[12] A. K. Yadav, M. Pruthi, and V. Kumar, "Quantum Synchronizable Codes from Quaternary Cyclotomy over Z2n," *Int. J. Theor. Phys.,* vol. 62, no. 6, p. 112 (May 2023), doi: 10.1007/s10773-023-05390-0.

[13] W. Bosma, J. Cannon, and C. Playoust, "The Magma Algebra System I : The User Language †," *J. Symb. Comput.*, no. 24, pp. 235–265 (1997).

[14] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF (4)," *IEEE Trans. Inf. Theory,* vol. 44, no. 4, pp. 1369–1387 (1998), doi: 10.1109/18.681315.

[15] L. Luo and Z. Ma, "Non-binary quantum synchronizable codes from repeated-root cyclic codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1461–1470 (2018), doi: 10.1109/TIT.2018.2795479.

Received February, 2025