Quantum Synchronizable Codes From Quadratic Residue Codes and Their Supercodes

Yixuan Xie[1], Jinhong Yuan[1], and Yuichiro Fujiwara[2]
[1] School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia
[2] Division of Physics, Mathematics and Astronomy, California Institute of Technology, Pasadena, California 91125, USA
Email: Yixuan.Xie@student.unsw.edu.au, J.Yuan@unsw.edu.au, yuichiro.fujiwara@caltech.edu

***Abstract*—Quantum synchronizable codes are quantum error-correcting codes designed to correct the effects of both quantum noise and block synchronization errors. While it is known that quantum synchronizable codes can be constructed from cyclic codes that satisfy special properties, only a few classes of cyclic codes have been proved to give promising quantum synchronizable codes. In this paper, using quadratic residue codes and their supercodes, we give a simple construction for quantum synchronizable codes whose synchronization capabilities attain the upper bound. The method is applicable to cyclic codes of prime length.**

I. Introduction

Quantum information theory has experienced remarkable progress towards developing and realizing large scale quantum computation and quantum communication. One of the most important early landmarks in quantum information science is the discovery of quantum error-correcting codes [1], [2], which enable us to suppress decoherence and other unwanted changes to quantum states that store quantum information. Because quantum bits, or *qubits*, that carry quantum information are highly vulnerable to quantum noise, various types of noise model and specialized quantum error-correcting codes have extensively been studied [3]. For instance, among the widely studied are Pauli errors and qubit loss [4], which roughly correspond to additive noise and erasures in classical information theory respectively.

Misalignment in block synchronization is another type of error that causes catastrophic failure, where the information processing device misidentifies the boundaries of an information block. For instance, assume that each chunk of information is encoded into a block of consecutive three bits in a stream of bits b_i so that the data has a frame structure. If four blocks of information are encoded, we have twelve ordered bits $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11})$ in which each of the four blocks (b_0, b_1, b_2), (b_3, b_4, b_5), (b_6, b_7, b_8), and (b_9, b_{10}, b_{11}) forms an information chunk. If, for example, misalignment occurs to the right by two bits when attempting to retrieve the second block of information, the device will wrongly read out b_5, b_6, and b_7 instead of the correct set of bits b_3, b_4, and b_5. The same kind of error in block synchronization may be considered for a stream of qubits.

A *quantum synchronizable code* is a coding scheme that corrects general quantum noise represented by Pauli errors as well as block synchronization errors. A theoretical framework of quantum synchronizable coding was first introduced in [5] as a quantum analogue of synchronizable coding in classical coding theory that attempts to correct both bit flips and block synchronization errors [6]. Subsequent studies have improved the original construction method and given further examples of quantum synchronizable codes [7], [8].

While we now have a theoretical framework of quantum synchronizable coding, there are only a few infinite classes of quantum synchronizable codes in the literature. In general, quantum synchronizable codes can be constructed from classical cyclic codes with additional properties through a method similar to the one studied in [9]. However, while the quantum analogue of cyclic codes given in [9] only requires a cyclic code that contains its dual, the known general construction for quantum synchronizable codes requires a chain of three cyclic codes satisfying further complicated properties, making it harder to explicitly construct promising examples.

In this work, we construct quantum synchronizable codes by exploiting special classical cyclic codes over the finite field $\mathbb{F}_2$ of order 2, called quadratic residue codes. Quadratic residue codes tend to have large minimum distances[10]. Thus, it is reasonable to expect that quantum error-correcting codes that exploit quadratic residue codes possess good error correction performance. We show that quantum synchronizable codes from quadratic residue codes also have good block synchronization capabilities. In fact, our codes attain the known upper bound on the maximum tolerable magnitude of misalignment in some cases. Note that the concept of the proposed method also applies to the general cyclic codes.

In Section II, we review basic facts in classical coding theory. Section III revisits the framework of quantum synchronizable coding and briefly explains the procedure of synchronization recovery. Section IV discusses our construction for quantum synchronizable codes based on quadratic residue codes. Concluding remarks are given in Section V.

II. Preliminaries

Here we briefly review basic facts in classical coding theory. Their proofs can be found in a standard textbook in coding theory such as [10].

A *binary linear* code $[n, k, d]$ is a k-dimensional subspace $\mathcal{L}$ of the n-dimensional vector space $\mathbb{F}_2^n$ such that $\min\{\mathrm{wt}(\mathbf{v}) \mid \mathbf{v} \in \mathcal{L}, \mathbf{v} \neq \mathbf{0}\} = d$, where $\mathrm{wt}(\mathbf{v})$ is the number of nonzero entries in $\mathbf{v}$. A binary vector in the subspace is a *codeword*.

Throughout this paper, we only consider binary codes and omit the term binary.

A *cyclic code* $\mathcal{C}$ of *length* n, *dimension* k, and *minimum distance* d is a linear code $[n, k, d]$ such that every cyclic shift of any codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ is also a codeword of $\mathcal{C}$. When the focus is on the length and dimension of a code, we may drop the third argument from the parameter notation. The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp = \{\mathbf{c}' \in \mathbb{F}_2^n \mid \mathbf{c}' \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}.$$

The dimension $\dim\left(\mathcal{C}^\perp\right)$ of $\mathcal{C}^\perp$ is $n - \dim(\mathcal{C}) = n - k$. Trivially, the dual code of a cyclic code is also a cyclic code.

By regarding a codeword as a coefficient vector of a polynomial in $\mathbb{F}_2[x]$, an $[n, k]$ cyclic code $\mathcal{C}$ generated by the unique monic polynomial $g(x)$ of minimum degree can be seen as the principal ideal $\langle g(x) \rangle$ closed by the ring $\mathbb{F}_2[x]/\left(x^n - 1\right)$. This unique polynomial $g(x)$ is called the *generator polynomial* of the cyclic code. Its degree $\deg\left(g(x)\right)$ is $n - k$. We may understand the cyclic code as

$$\mathcal{C} = \{m(x)g(x) \mid m(x) \in \mathbb{F}_2[x], \deg(m(x)) < k\}.$$

The polynomial $h(x)$ such that $g(x)h(x) = x^n - 1$ is called the *check polynomial* of $\mathcal{C}$. The dual code $\mathcal{C}^\perp$ has generator polynomial $g^\perp(x)$ of the form

$$g^\perp(x) = x^{\deg(h(x))} h(x^{-1}). \tag{1}$$

Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be two cyclic codes of length n. If $\mathcal{C}_2 \subseteq \mathcal{C}_1$, that is, if $\mathcal{C}_1$ contains all codewords of $\mathcal{C}_2$, then the generator polynomial $g_1(x)$ divides every codeword of $\mathcal{C}_2$, which means that for every $c(x) \in \mathcal{C}_2$ there exits a polynomial $f_c(x)$ of degree $\deg(c(x)) - (n - \dim(\mathcal{C}_1))$ such that $c(x) = f_c(x)g_1(x)$ in $\mathbb{F}_2[x]$. The smaller code $\mathcal{C}_2$ is a *subcode* of $\mathcal{C}_1$ while $\mathcal{C}_1$ is a *supercode* of $\mathcal{C}_2$. A cyclic code is *dual-containing* if it is a supercode of its dual code.

III. Quantum Synchronizable Code

In this section, we review the framework of quantum synchronizable codes and the synchronization recovery procedures. The basic notions and proofs of the facts in quantum information theory we use in this section can be found in [4]. For complete treatments of block synchronization in the context of quantum information, the interested reader is referred to the original articles [5], [7].

A. Quantum Synchronizable Codes

An $[[n, k]]$ *quantum error-correcting code* is a coding scheme that encodes k logical qubits into n physical qubits. As in the classical case, n and k are the *length* and *dimension* of the code, respectively. Typically, quantum error-correcting codes are designed to correct the effects of bit errors and phase errors caused by Pauli operators X and Z respectively under the assumption that both bit error due to X and phase error due to Z may occur on the same qubit. A (c_l, c_r)-$[[n, k]]$ *quantum synchronizable code* is an $[[n, k]]$ quantum error-correcting 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 some nonnegative integers c_l and c_r.

The general construction method for quantum synchronizable codes developed in [5], [7] employs a notion in finite algebra. Let $f(x) \in \mathbb{F}_2[x]$ be a polynomial over $\mathbb{F}_2$ such that $f(0) = 1$. The *order* $\operatorname{ord}(f(x))$ of the polynomial $f(x)$ is the cardinality $|\{x^a \pmod{f(x)} \mid a \in \mathbb{N}\}|$, where $\mathbb{N}$ is the set of positive integers.

Theorem 3.1: [7] Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be two cyclic codes of parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$ with $k_1 > k_2$ respectively such that $\mathcal{C}_2 \subset \mathcal{C}_1$ and $\mathcal{C}_2^\perp \subseteq \mathcal{C}_2$. Define $f(x)$ of degree $k_1 - k_2$ to be the quotient of $\frac{g_2(x)}{g_1(x)}$ over $\mathbb{F}_2[x]/(x^n - 1)$. For any pair of nonnegative integers c_l, c_r satisfying $c_l + c_r < \operatorname{ord}(f(x))$, there exists a (c_l, c_r)-$[[n + c_l + c_r, 2k_2 - n]]$ quantum synchronizable code 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.

Theorem 3.1 requires a pair of cyclic codes $\mathcal{C}_1, \mathcal{C}_2$ of the same length and dimension $k_1 > k_2 > \lceil \frac{n}{2} \rceil$ to construct a quantum synchronizable code of positive dimension. To design a good quantum synchronizable code, it is generally desirable to choose cyclic codes with good minimum distances while ensuring $\operatorname{ord}(f(x))$ to be as large as possible. In addition to these criteria, the cyclic codes must satisfy the chain condition that $\mathcal{C}_2^\perp \subseteq \mathcal{C}_2 \subset \mathcal{C}_1$. Note that this is stronger than the dual-containing condition for the quantum cyclic codes given in [9]. In what follows, when a pair of cyclic codes are written as $\mathcal{C}_1$ and $\mathcal{C}_2$, we always assume that they satisfy the chain condition and that their generator polynomials are $g_1(x)$ and $g_2(x) = f(x)g_1(x)$ for some polynomial $f(x)$, respectively.

B. Encoding

Since $\dim(\mathcal{C}_2) = k_2$ and $\dim\left(\mathcal{C}_2^\perp\right) = n - k_2$, the dimension of cosets is $\dim\left(\mathcal{C}_2/\mathcal{C}_2^\perp\right) = k_2 - n + k_2 = 2k_2 - n$. Hence, the number of cosets is $2^{2k_2 - n}$. Let $\mathcal{B} = \{b_i(x) \mid 0 < i \leq 2^{2k_2 - n}\}$ be a system of representatives of the cosets. Then the set

$$V = \left\{ \left| \mathcal{C}_2^\perp + b_i(x) \right\rangle \;\middle|\; b_i(x) \in \mathcal{B} \right\}$$

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

$$\left| \mathcal{C}_2^\perp + b_i(x) \right\rangle = \frac{1}{\sqrt{|\mathcal{C}_2^\perp|}} \sum_{c(x) \in \mathcal{C}_2^\perp} |c(x) + b_i(x)\rangle .$$

Take an arbitrary $2^{2k_2 - n}$-qubit state $|\psi\rangle$ to be encoded. Using the standard encoder for Calderbank-Shor-Steane (CSS) codes [4], the state $|\psi\rangle$ is transformed into n-qubit state $|\psi\rangle_{enc} = \sum_i \alpha_i |v_i\rangle$, where $v_i \in V$.

Recall that $g_1(x)$ is the generator polynomial of $\mathcal{C}_1$. Apply the unitary operator U_g that adds the coefficient vector of $g_1(x)$:

$$U_g |\psi\rangle_{enc} \rightarrow \sum_i \alpha_i |v_i + g_1\rangle.$$

Let c_r, c_l be nonnegative integers such that $c_l + c_r < \operatorname{ord}(f(x))$. By attaching extra c_l and c_r ancilla qubits to the left and to the right of the original state respectively and then applying CNOT gates, the state is taken to the final encoded $(n + c_l + c_r)$-qubit state

$$|0\rangle^{\otimes c_l} U_g(|\psi\rangle_{enc})|0\rangle^{\otimes c_r} \to \sum_i \alpha_i |l_i, v_i + g_1, r_i\rangle = |\Psi\rangle_{enc},$$

where l_i and r_i are the last c_l and the first c_r portions of the vector $v_i + g_1$, respectively.

C. Synchronization Recovery

Here we give a brief overview of the procedures for error correction and synchronization recovery. For the mathematical details, see [5], [7].

Assume that the device gathered qubits of one block length, that is, consecutive $n + c_l + c_r - 1$ qubits, and tries to correct errors caused by Pauli operators and misalignment if necessary. Let $\mathcal{T} = (t_0, t_1, \dots, t_{n+c_l+c_r-1})$ be the collection of $n+c_l+c_r$ qubits at the output of the quantum channel. If block synchronization is correct, $\mathcal{T}$ forms a properly aligned block encoded as $|\Psi\rangle_{enc}$. We assume that $\mathcal{T}$ may be misaligned by θ qubits to the right, where $-c_l \le \theta \le c_r$. When θ is negative, it means that misalignment is to the left by $|\theta|$ qubits.

Let $\mathcal{S} = (s_0, s_1, \dots, s_{n+c_l+c_r-1})$ be the $n + c_l + c_r$ qubits of $|\Psi\rangle_{enc}$. The device first focuses on consecutive n qubits $\mathcal{W} = (t_{c_l}, t_{c_l+1}, \dots, t_{c_l+n-1})$ in the middle of $\mathcal{T}$. Because of the potential misalignment, this set of qubits is $\mathcal{W} = (s_{c_l+\theta}, s_{c_l+1+\theta}, \dots, s_{c_l+n-1+\theta})$.

Let E be the $(n + c_l + c_r)$-fold tensor product of single Pauli operators that represents errors that occurred on $|\Psi\rangle_{enc}$. The corrupted state at the quantum channel output is given by

$$E|\Psi\rangle_{enc} = \sum_i \alpha_i (-1)^{(l_i, v_i+g_1, r_i)\cdot \mathbf{e_p}} |(l_i, v_i + g_1, r_i) + \mathbf{e_b}\rangle,$$

where $\mathbf{e_b}$ and $\mathbf{e_p}$ are binary vectors representing bit and phase errors, respectively.

The device first corrects bit errors on $\mathcal{W}$ and then detects misalignment. Let $\mathcal{H}_{\mathcal{C}_1}$ be the full-rank parity-check matrix of $\mathcal{C}_1$ used for encoding. Using the stabilizer generators defined by $\mathcal{C}_1$, the decoding circuit obtains the syndrome for bit errors as in the standard two-step decoding of a CSS code:

$$E|\Psi\rangle_{enc}|0\rangle^{\otimes n-k_1} \to E|\Psi\rangle_{enc}|\mathbf{e_b}\mathcal{H}_{\mathcal{C}_1}^T\rangle.$$

If the number of bit errors is at most $\lfloor \frac{d_1-1}{2} \rfloor$ in $\mathcal{W}$, applying X Pauli operators to the qubits specified by $\mathbf{e_b}\mathcal{H}_{\mathcal{C}_1}^T$ eliminates all bit errors within the window $\mathcal{W}$.

The next step is to identify how many qubits away $\mathcal{W}$ is from the correct position $\mathcal{S}$, that is, identifying the magnitude θ. To this end, we manipulate the polynomials used as the labels of each basis state. Such operations can be done, for example, by a quantum shift register given in [9].

Note that the condition that $\mathcal{C}_2^\perp \subset \mathcal{C}_2 \subset \mathcal{C}_1$ implies that any codeword $c_i^\perp(x) \in \mathcal{C}_2^\perp$ also belongs to $\mathcal{C}_2$ and $\mathcal{C}_1$. Hence, each basis of the state of $\mathcal{S}$ is a sum of states of the form

$$\begin{aligned}&\left|c_i^\perp(x) + b_i(x) + g_1(x)\right\rangle = \\ &\qquad |v_1(x)f(x)g_1(x) + v_2(x)f(x)g_1(x) + g_1(x)\rangle,\end{aligned}$$

for some polynomials $v_1(x)$ and $v_2(x)$ whose degrees are less than k_2. Because of the misalignment, each basis of the state of $\mathcal{W}$ is a linear combination of states of the form $\left|x^\theta \left(c_i^\perp(x) + b_i(x) + g_1(x)\right)\right\rangle$. Thus, the quotient of the label of each basis of the state of $\mathcal{W}$ divided by $g_1(x)$ is $x^\theta(v_1(x)f(x)+v_2(x)f(x)+1)$. Dividing this quotient by $f(x)$ gives x^θ as the remainder. Thus, if $c_l + c_r < \mathrm{ord}(f(x))$, the synchronization error θ is uniquely determined.

Because we identified the magnitude and direction of misalignment, synchronization can be recovered. Possible bit errors on qubits outside $\mathcal{W}$ and phase errors can be corrected by treating the quantum synchronizable code as a CSS code. For more details on the final steps, we refer the reader to [5].

IV. Use of Cyclic Supercodes

We now provide a construction for quantum synchronizable codes designed from special cyclic codes. Recall that Theorem 3.1 requires a pair of cyclic codes $\mathcal{C}_1$, $\mathcal{C}_2$ of parameters $[n, k_1]$ and $[n, k_2]$ with $k_1 > k_2$ that satisfy the condition $\mathcal{C}_2^\perp \subseteq \mathcal{C}_2 \subset \mathcal{C}_1$. We first construct a cyclic code $\mathcal{C}_2$ in such a way that its dual code $\mathcal{C}_2^\perp$ is a subspace of $\mathcal{C}_2$. We then obtain a cyclic supercode $\mathcal{C}_1$ by inserting codewords into $\mathcal{C}_2$. While we only apply this idea to a small, specific class of cyclic codes, this general principle of producing supercodes may be applicable to other cyclic codes to ensure good synchronization recoverability if code lengths are primes.

A. Dual-containing Cyclic Codes: $\mathcal{C}_2^\perp \subset \mathcal{C}_2$

Let p be a prime of the form $p \equiv \pm 1 \pmod 8$. Define $\mathcal{Q}^{\mathcal{R}} = \{x^2 \pmod p \mid 1 \le x \le \frac{p-1}{2}\}$ and $\mathcal{Q}^{\mathcal{NR}} = \{1, 2, \dots, p-1\} \setminus \mathcal{Q}^{\mathcal{R}}$ to be the sets of $\frac{p-1}{2}$ nonzero quadratic residues and $\frac{p-1}{2}$ quadratic non-residues respectively. Take a primitive p-th root α of unity in $\mathbb{F}_{2^t}$, where t is the smallest positive integer such that p divides $2^t - 1$. Let

$$g_{\mathcal{R}}(x) = \prod_{i \in \mathcal{Q}^{\mathcal{R}}} \left(x - \alpha^i\right) \quad \text{and} \quad g_{\mathcal{NR}}(x) = \prod_{i \in \mathcal{Q}^{\mathcal{NR}}} \left(x - \alpha^i\right).$$

Note that $g_{\mathcal{R}}(x)$ and $g_{\mathcal{NR}}(x)$ are both in $\mathbb{F}_2[x]$. The pair $\mathcal{C}_{\mathcal{R}} = \langle g_{\mathcal{R}}(x)\rangle$ and $\mathcal{C}_{\mathcal{NR}} = \langle g_{\mathcal{NR}}(x)\rangle$ are $[p, \frac{p+1}{2}]$ cyclic codes known as *quadratic residue codes* over $\mathbb{F}_2$. By the same token, the two polynomials

$$\bar{g}_{\mathcal{R}}(x) = (x-1) \prod_{i \in \mathcal{Q}^{\mathcal{R}}} \left(x - \alpha^i\right)$$

and

$$\bar{g}_{\mathcal{NR}}(x) = (x-1) \prod_{i \in \mathcal{Q}^{\mathcal{NR}}} \left(x - \alpha^i\right)$$

generate $[p, \frac{p-1}{2}]$ cyclic codes $\bar{\mathcal{C}}_{\mathcal{R}} = \langle \bar{g}_{\mathcal{R}}(x)\rangle$ and $\bar{\mathcal{C}}_{\mathcal{NR}} = \langle \bar{g}_{\mathcal{NR}}(x)\rangle$. The latter pair may also be referred to as quadratic residue codes in the literature. It is known that quadratic residue codes tend to have large minimum distances. The following is a well-known general lower bound, known as the square root bound.

Theorem 4.1 (Square Root Bound): The minimum distance d of a quadratic residue code of length p is at least $\sqrt{p}$. If $p \equiv -1 \pmod 4$, then $d^2 - d + 1 \ge p$.

For small quadratic residue codes, tables of exact parameters can be found in [12].

To take advantage of quadratic residue codes for constructing quantum synchronizable codes, we use the fact that the larger one of each pair is dual-containing if the length is -1 modulo 8. A detailed account on the properties of quadratic residue codes and their duals can be found in [10, Ch. 16]. For convenience, we give a short proof of the simple fact.

Lemma 4.2: The quadratic residue codes $\mathcal{C}_{\mathcal{R}}$, $\mathcal{C}_{\mathcal{NR}}$, $\bar{\mathcal{C}}_{\mathcal{R}}$ and $\bar{\mathcal{C}}_{\mathcal{NR}}$ of length $p \equiv -1 \pmod 8$ have the following properties:

1) $\mathcal{C}_{\mathcal{R}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{R}}, \quad \mathcal{C}_{\mathcal{NR}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{NR}}.$

2) $\mathcal{C}_{\mathcal{R}}^{\perp} \subset \mathcal{C}_{\mathcal{R}}, \quad \mathcal{C}_{\mathcal{NR}}^{\perp} \subset \mathcal{C}_{\mathcal{NR}}.$

Proof: Since $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$ are disjoint and do not contain 0, we have $x^p - 1 = (x-1)\, g_{\mathcal{R}}(x) g_{\mathcal{NR}}(x)$. The zeros of $g_{\mathcal{R}}(x)$ and $g_{\mathcal{NR}}(x)$ are $\{\alpha^i \mid i \in \mathcal{Q}^{\mathcal{R}}\}$ and $\{\alpha^i \mid i \in \mathcal{Q}^{\mathcal{NR}}\}$, respectively. Hence by Equation (1), the zeros of $\mathcal{C}_{\mathcal{R}}^{\perp}$ are 1 and α^{-i} for $i \in \mathcal{Q}^{\mathcal{NR}}$, and the zeros of $\mathcal{C}_{\mathcal{NR}}^{\perp}$ are 1 and α^{-i} for $i \in \mathcal{Q}^{\mathcal{R}}$. Note that $\alpha^i \in \mathcal{Q}^{\mathcal{R}}$ if and only if i is even and that $\alpha^i \in \mathcal{Q}^{\mathcal{NR}}$ if and only if i is odd. When $p \equiv -1 \pmod 8$, we have $i \in \mathcal{Q}^{\mathcal{R}}$ if and only if $-i \in \mathcal{Q}^{\mathcal{NR}}$. Hence, $\mathcal{C}_{\mathcal{R}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{R}}$ and $\mathcal{C}_{\mathcal{NR}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{NR}}$. Since $\mathcal{C}_{\mathcal{R}} = \langle g_{\mathcal{R}}(x) \rangle$ and $\mathcal{C}_{\mathcal{R}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{R}} = \langle \bar{g}_{\mathcal{R}}(x) \rangle$, it is trivial that $\mathcal{C}_{\mathcal{R}}$ is dual-containing. By the same token, $\mathcal{C}_{\mathcal{NR}}$ is a dual-containing code. ■

Example 1: Consider the set of nonzero quadratic residues modulo 31

$$\begin{aligned}\mathcal{Q}^{\mathcal{R}} &= \{1, 2^2, 3^2, 4^2, \ldots, 15^2\}\\ &= \{1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8\}.\end{aligned}$$

The generator polynomial of the quadratic residue code $\mathcal{C}_{\mathcal{R}}$ of length $p = 31$ is then

$$g_{\mathcal{R}}(x) = x^{15} + x^{12} + x^7 + x^6 + x^2 + x + 1.$$

Multiplying by $x+1$ gives the generator polynomial of $\bar{\mathcal{C}}_{\mathcal{R}}$

$$\bar{g}_{\mathcal{R}}(x) = x^{16} + x^{15} + x^{13} + x^{12} + x^8 + x^6 + x^3 + x + 1.$$

Plugging $g_{\mathcal{R}}(x)$ into Equation (1) also gives $\bar{g}_{\mathcal{R}}(x)$, which means that this is the generator polynomial of the dual code $\mathcal{C}_{\mathcal{R}}^{\perp}$ as well. ■

B. Cyclic supercodes of $\mathcal{C}_2$

Lemma 4.2 provides a $[p, \frac{p+1}{2}, d]$ dual-containing cyclic code $\mathcal{C}_2$ for prime $p \equiv -1 \pmod 8$ with $d \geq \sqrt{p}$. To obtain another cyclic code $\mathcal{C}_1$ such that $\mathcal{C}_2 \subset \mathcal{C}_1$, we increase the number of codewords by deleting a factor from the generator polynomial of $\mathcal{C}_2$ we already have. Note that, by definition, a cyclic code is a subcode of another if its generator polynomial is divisible by the other. Thus, if the generator polynomial of $\mathcal{C}_2$ has more than one factor, deletion always gives a supercode. As the following proposition shows, a particularly interesting case is when p is a Mersenne prime.

Proposition 4.3: Let $\mathcal{C} = \mathcal{C}_{\mathcal{R}}$ be the quadratic residue code of length p generated by $g_2(x) = \prod_{i \in \mathcal{Q}^{\mathcal{R}}} \left(x - \alpha^i\right)$. If $p = 2^l - 1$, then $g_2(x)$ can be factored into $\frac{2^{l-1}-1}{l}$ irreducible polynomials of degree l, that is,

$$g_2(x) = \prod_j M_j(x), \tag{2}$$

where $M_s(x)$ is the minimal polynomial of α^s over $\mathbb{F}_2$ and $\deg(M_j(x)) = l$ for all j.

The above proposition can be proved through the concept of cyclotomy [10]. For nonnegative integers s and n, the *cyclotomic coset* $C_{s,n}$ of s modulo n over $\mathbb{F}_2$ is the set

$$C_{s,n} = \{s2^i \mod n \mid i \in \mathbb{N}\}.$$

Since $C_{s,n} = C_{s',n}$ for $s' \in C_{s,n}$, we may take

$$S_n = \{\min\{t \mid t \in C_{s,n}\} \mid s \in \mathbb{N} \cup \{0\}\}$$

as a system of representatives of the cyclotomic cosets by picking the smallest element from each set. The integers modulo n are partitioned into cyclotomic cosets in a way described as

$$\{0, 1, \ldots, n-1\} = \bigcup_{s \in S_n} C_{s,n}.$$

Let α be a primitive nth root of unity in $\mathbb{F}_{2^{|C_{1,n}|}}$. By definition, the minimal polynomial $M_s(x)$ of α^s over $\mathbb{F}_2$ can be expressed as

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

Note that for any s, the cardinality $|C_{s,n}|$ is a divisor of $|C_{1,n}|$. When n is a Mersenne prime $2^l - 1$, we have $|C_{1,n}| = l$. Because l is also a prime, when n is a prime of the form $n = p = 2^l - 1$, each $C_{s,n}$ is of size l as well, proving Proposition 4.3.

Because of the one-to-one correspondence between cyclic codes and monic divisors of $x^n - 1$, deleting one or more factors $M_j(x)$ gives another generator polynomial that results in a cyclic code of higher dimension containing the dual-containing cyclic code $\mathcal{C}_{\mathcal{R}}$. Trivially, if we delete z factors, the dimension of the supercode is higher than that of $\mathcal{C}_{\mathcal{R}}$ by zl. Applying Theorem 3.1 to this supercode as $\mathcal{C}_1$ together with the dual-containing quadratic residue code gives a quantum synchronizable code.

It is also notable that any supercode $\mathcal{C}_1$ obtained by deleting a minimal polynomial of the quadratic residue code is also dual-containing. Thus, we have a chain of cyclic codes, each of which is dual-containing itself and contains all smaller ones. Therefore, we can construct a quantum synchronizable code from any pair of codes in the chain.

C. Maximum misalignment tolerance

In the context of quantum synchronizable codes, we would like to maximize $\operatorname{ord}(f(x))$, where $f(x)$ is the quotient in Theorem 3.1, in order to tolerate as large magnitude of misalignment as possible. It is known that the maximum tolerable magnitude of a quantum synchronizable code is upper bounded by its length [7]. We prove that the quantum synchronizable codes from quadratic residue codes given in the previous subsection attain this bound.

Lemma 4.4: Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be cyclic codes of length p such that $\mathcal{C}_2 \subset \mathcal{C}_1$ and $\mathcal{C}_1 \neq \mathcal{C}_2$. Define $f(x)$ to be the polynomial such that $g_2(x) = f(x) g_1(x)$. If p is a prime, then $\operatorname{ord}(f(x)) = p$.

Proof: Because the generator polynomial of a cyclic code of length p divides $x^p - 1$, its factor also divides $x^p - 1$. Hence, the factor $f(x)$ of $g_2(x)$ divides $x^p - 1$ as well, which implies that $x^p \equiv 1 \pmod{f(x)}$. Hence, because $\mathrm{ord}(f(x)) = |\{x^a \pmod{f(x)} \mid a \in \mathbb{N}\}|$, the order of $f(x)$ is a divisor of p. Since p is a prime and $f(x) \neq 1$ by assumption, we have $\mathrm{ord}(f(x)) = p$ as desired. ■

We now give our main theorem.

Theorem 4.5: Let $p = 2^l - 1$ be a Mersenne prime. For nonnegative integers c_l, c_r and z such that $c_l + c_r < p$ and $z \leq \frac{2^{l-1}-l-1}{l}$, there exits a quantum synchronizable code of parameters (c_l, c_r)-$[[p + c_l + c_r, 2zl + 1]]$.

Proof: Take a quadratic residue code of length $p = 2^l - 1$ generated by the nonzero quadratic residues. By Proposition 4.3, its generator polynomial has $\frac{2^{l-1}-1}{l}$ minimal polynomials of degree l as its factors. Thus we have a chain of $\frac{2^{l-1}-1}{l}$ cyclic codes in which a code contains all other smaller ones. Note that a supercode of a dual-containing code is also dual-containing. Thus, by applying Theorem 3.1 and Lemma 4.4 the cyclic code generated by the polynomial that is obtained by deleting z factors and another one obtained by deleting $z+y$ factors for some positive integer y, we obtain a quantum synchronizable code of desired parameters. ■

Example 2: As in Example 1, let $p = 2^5 - 1$ and take the set $\mathcal{Q}^{\mathcal{R}} = \{x^2 \pmod{p} \mid 1 \leq x \leq 2^{l-1} - 1\}$ of nonzero quadratic residues modulo 31. Then $\mathcal{Q}^{\mathcal{R}}$ is the union of $\frac{2^4-1}{5} = 3$ cyclotomic cosets of field $\mathbb{F}_{2^5}$ as follows.

$$\mathcal{Q}^{\mathcal{R}} = C_{1,31} \cup C_{5,31} \cup C_{7,31},$$

where $C_{1,31} = \{1, 2, 4, 8, 16\}$, $C_{5,31} = \{5, 10, 20, 9, 18\}$ and $C_{7,31} = \{7, 14, 28, 25, 19\}$.

Let $\mathcal{C}_2 = \langle g_{\mathcal{R}}(x) \rangle$. Since $g_{\mathcal{R}}(x)$ is the product of the minimal polynomials $M_s(x)$ of α^s over $\mathbb{F}_2$ for $s \in \mathcal{Q}^{\mathcal{R}}$, we have

$$g_{\mathcal{R}}(x) = M_1(x)M_5(x)M_7(x),$$

with

$$\begin{aligned} M_1(x) &= x^5 + x^2 + 1, \\ M_5(x) &= x^5 + x^4 + x^2 + x + 1, \text{ and} \\ M_7(x) &= x^5 + x^3 + x^2 + x + 1. \end{aligned}$$

Note that each one of $M_1(x)$, $M_5(x)$ and $M_7(x)$ divides $x^{31} - 1$. Let $\mathcal{C}_1 = \langle g_1(x) = \frac{g_{\mathcal{R}}(x)}{f(x)} \rangle$. If we delete $z = 1$ minimal polynomial, $f(x) = M_j(x)$ for $j \in \{1, 5, 7\}$, the dimension of $\mathcal{C}_1$ is equal to $\dim(\mathcal{C}_1) = p - \deg(g_{\mathcal{R}}(x)) + zl = 31 - 15 + 5 = 21$. If we delete $z = 2$ factors, then $f(x) = M_{j_1}(x)M_{j_2}(x)$ for $j_1, j_2 \in \{1, 5, 7\}$ and $j_1 \neq j_2$, so the dimension of $\mathcal{C}_1$ in this case is $\dim(\mathcal{C}_1) = 31 - 15 + 10 = 26$. In both cases, the $\mathrm{ord}\,(f(x)) = 2^l - 1 = p = 31$. Since $\deg(g_{\mathcal{R}}(x)) = 15$ and $\dim(\mathcal{C}_2) = 16$, for arbitrary pair of non-negative integer c_l and c_r such that $c_l + c_r < 31$, we have a (c_l, c_r)-$[[31 + c_l + c_r, 1]]$ quantum synchronizable code.

Further, let $z = 1$ and $\mathcal{C}_2 = \langle g_{\mathcal{R}}(x) \rangle \subset \mathcal{C}_3$ with $\mathcal{C}_3 = \langle M_{j_1}(x)M_{j_2}(x) \rangle$ for $j_1, j_2 \in \{1, 5, 7\}$ and $j_1 \neq j_2$. If $y = 1$, by removing $z + y = 2$ minimal polynomials $M_i(x)$ from $g_{\mathcal{R}}(x)$, we obtain another cyclic code $\mathcal{C}_4$ such that $\mathcal{C}_2 \subset \mathcal{C}_3 \subset \mathcal{C}_4$. Since $\dim(\mathcal{C}_3) = 21 > \lceil \frac{n}{2} \rceil$, by Theorm 3.1 for $c_l + c_r < 31$, $\mathcal{C}_3$ and $\mathcal{C}_4$ form a (c_l, c_r)-$[[31 + c_l + c_r, 2zl + 1 = 11]]$ quantum synchronizable code. ■

V. Conclusion

We studied a method for constructing quantum error-correcting codes that can also recover block synchronization. Quantum synchronizable codes were derived from sets of quadratic residues by designing chains of dual-containing cyclic codes. We showed that these quantum synchronizable codes possess the highest possible tolerance against synchronization errors. Our construction is particularly flexible when the length is a Mersenne prime because we may be able to choose a pair from a long chain of dual-containing cyclic codes. This adds variety in dimension and minimum distance to the resulting quantum synchronizable codes.

Our method allows for easily calculating the lengths, dimensions, and synchronization recovery abilities of our quantum synchronizable codes. However, the exact minimum distances seem quite difficult to compute. In general. it is a very difficult problem to find the exact minimum distance of a cyclic code even for codes of modest length. While there are some known general bounds on the minimum distance of a cyclic code and quadratic residue code such as the square root bound and BCH bound [10], the search for sharper bounds is still one of the central problems in coding theory today. Because quadratic residue codes and their variants are among the more interesting classical codes, the minimum distances and weight distributions of quadratic residue codes and their supercodes are of interest not only for the purpose of block synchronization for qubit streams but also of importance on their own right. We hope that further progress will be made in this direction in future work.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, vol. 52, pp. 2493-2496, 1995.

[2] A. M. Steane, "Error Correcting Codes in Quantum Theory," *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.

[3] *Quantum Error Correction*, D. A. Lidar and T. A. Brun, Eds. *Cambridge Uni. Press*, New York, 2013.

[4] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", *Cambridge Uni. Press*, New York, 2000.

[5] Y. Fujiwara, "Block Synchronization for Quantum Information", *Phys. Rev. A*, vol. 87, 022344, 2013.

[6] R. C. Bose and J. G. Caldwell, "Synchronizable error-correcting codes," *Inf. Contr.*, vol. 10, pp. 616–630, 1967.

[7] Y. Fujiwara, V. D. Tonchev, and T. W. H. Wong, "Algebraic techniques in designing quantum synchronizable codes", *Phy. Rev. A*, vol. 88, 012318, 2013.

[8] Y. Fujiwara and P. Vandendriessche, "Quantum Synchronizable Codes From Finite Geometries", arXiv:1311.3416.

[9] M. Grassl and T. Beth, "Cyclic quantum error-correcting codes and quantum shift registers," *Proc. R. Soc. London Ser. A* vol. 456, 2689–2706 2000.

[10] F. J. MacWilliams and N. J. A. Sloane, "The theory of error-correcting codes", North-holland Publishing Comp. 2nd edition, 1978.

[11] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098-1105, 1996.

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