Block synchronization for quantum information

Yuichiro Fujiwara[*]

Division of Physics, Mathematics and Astronomy, California Institute of Technology, MC 253-37, Pasadena, California 91125, USA

Locating the boundaries of consecutive blocks of quantum information is a fundamental building block for advanced quantum computation and quantum communication systems. We develop a coding theoretic method for properly locating boundaries of quantum information without relying on external synchronization when block synchronization is lost. The method also protects qubits from decoherence in a manner similar to conventional quantum error-correcting codes, seamlessly achieving synchronization recovery and error correction. A family of quantum codes that are simultaneously synchronizable and error-correcting is given through this approach.

I. INTRODUCTION

The field of quantum information theory has experienced rapid and remarkable progress toward understanding and realizing large-scale quantum computation and quantum communication. One of the most important missions is to develop theoretical foundations for robust and reliable quantum information processing. The discovery of the fact that it is even possible for us to correct the effects of decoherence on quantum states was one of the most important landmarks in quantum information theory in this regard [1]. The field has since made various kinds of remarkable progress, from developing quantum analogues of important concepts in classical information theory to finding surprising phenomena that are uniquely quantum information theoretic [2]. Quantum error correction has been realized in various experiments as well [3–11].

One of the most important problems of reliable quantum information processing that remain unaddressed, however, is block synchronization (or, more commonly, "frame synchronization," in the language of classical communications [12]). In classical digital computation and communications, virtually all data have some kind of block structure, which means that in order for one to make sense of data, one must know the exact positions of the boundaries of each block of information, or word, in a stream of bits.

This fact will stay the same in the quantum domain. In fact, not only will the actual quantum information one wishes to process most likely have a block structure for the same reason as in the classical domain, but procedures for manipulating quantum information also typically demand very precise alignment. For instance, we have a means to encode one qubit of information into five physical qubits to reduce the effects of decoherence to the theoretical limit [13]. However, this does not mean that we can apply the procedure to, say, the last three qubits from an encoded quantum state and the first two qubits from the following information block to correct errors. If that worked, one would still not be able to correctly interpret the information carried by the qubits; after all, "quantum information theory" is not quite the same as "antumin formationth eory" with "qu" before it.

Block synchronization is critical when correct block alignment cannot be provided or is difficult to provide by a simple external mechanism. For instance, block synchronization is a critical problem in virtually any area of classical digital communications, where two parties are physically distant, so that synchronization must be achieved through some special signaling procedure, such as inserting "marker" bits or using a specially allocated bit pattern as a "preamble" to signal the start of each block (see, for example, [14,15] for the basics of block synchronization techniques for digital communications).

It is true that if we assume that a qubit always goes through wires as expected in a quantum circuit and that storing, retrieval, and transmission of quantum information are always securely synchronized by external physical mechanisms, then block synchronization is certainly not a problem. However, such a strict assumption imposes demanding requirements on hardware and limits what quantum information processing can offer. For example, without a software solution to block synchronization, quantum communication would have to always be supported by perfectly synchronized classical communications to a large degree [16].

One of the most substantial barriers to establishing block synchronization in the quantum domain is the fact that measuring qubits usually destroys the quantum information they contain. Existing classical block synchronization techniques typically require that the information receiver or processing device constantly monitor the data to pick up on inserted boundary signals, which translates into constant measurement of all qubits in the quantum case. Hence, if an analog of a classical synchronization scheme such as inserting a preamble were to be employed in a naive manner, one would have to know exactly where those inserted boundary signals are in order not to disturb quantum information contained in data blocks, which would require accurate synchronization to begin with.

One might then expect that a sophisticated block synchronization scheme based on information theory would be more attractive and promising in the quantum world. Another big hurdle lies exactly here; sophisticated coding for synchronization is already a notoriously difficult problem in classical information theory (see, however, [17] for a recent survey of coding theoretical approaches to fighting various kinds of synchronization error for the classical case). Making things more challenging, quantum bits are thought to be more vulnerable to environmental noise than classical bits, which

_____

[*]yuichiro.fujiwara@caltech.edu

implies that we ought to simultaneously answer the need for strong protection from the effects of decoherence.

The primary purpose of the present paper is to show that it is, indeed, possible to encode information about the boundaries of blocks into qubits in such a way that block synchronization recovery and quantum error correction are seamlessly integrated. The proposed scheme does not rely on external synchronization mechanisms or destroy quantum information by searching for boundaries. We make use of classical error-correcting codes with certain algebraic properties, so that the problem of finding such quantum synchronizable error-correcting codes is reduced to that of searching for special classical codes.

In the next section, we give a simple mathematical model of block synchronization in the quantum domain and define quantum synchronizable error-correcting codes. The details of our scheme are presented in Sec. III. Concluding remarks are given in Sec. IV.

II. BLOCK SYNCHRONIZATION

Here we give a simple mathematical model of block synchronization in the quantum setting. Note that while the term block might seem to suggest that each block is encoded by the same block code, we may treat them as more general structures, so that different blocks can contain different numbers of qubits encoded by different coding schemes.

Let $Q = (q_0, \ldots, q_{x-1})$ be an ordered set of length x, where each element represents a qubit. A *block* F_i is a set of consecutive elements of Q. Let $\mathcal{F} = \{F_0, \ldots, F_{y-1}\}$ be a set of blocks. The ordered set $(Q, \mathcal{F})$ is called a *blockwise structured sequence* if $|\{\cup_i F_i\}| = x$ and $F_i \cap F_j = \emptyset$ for $i \neq j$. In other words, the elements of a sequence are partitioned into groups of consecutive elements called blocks.

Take a set $G = \{q_j, \ldots, q_{j+g-1}\}$ of g consecutive elements of Q. G is said to be *misaligned* by a qubits to the *right* with respect to $(Q, \mathcal{F})$ if there exits an integer a and a block F_i such that $F_i = \{q_{j-a}, \ldots, q_{j+g-a-1}\}$ and $G \notin \mathcal{F}$. If a is negative, we may say that G is misaligned by $|a|$ qubits to the *left*. G is *properly aligned* if $G \in \mathcal{F}$.

To make this mathematical model clearer, take three qubits and encode each qubit into nine qubits by Shor's nine-qubit code [1]. The resulting 27 qubits may be seen as $Q = (q_0, \ldots, q_{26})$, where the three encoded nine-qubit blocks $|\varphi_0\rangle$, $|\varphi_1\rangle$, and $|\varphi_2\rangle$ form blocks $F_0 = (q_0, \ldots, q_8)$, $F_1 = (q_9, \ldots, q_{17})$, and $F_2 = (q_{18}, \ldots, q_{26})$, respectively. These 27 qubits may be sent to a different place, stored in quantum memory, or immediately processed for quantum computation. A device, knowing the size of each information block, operates on nine qubits at a time. If misalignment occurs by, say, two qubits to the left, then the device that tries to correct errors on qubits in $|\varphi_1\rangle$ applies the error-correction procedure to the set G of nine qubits $q_7, \ldots, q_{15}$, two of which come from F_0 and seven of which come from F_1. In this case, when measuring the stabilizer generator $IZZIIIIII$ of the nine-qubit code to obtain the syndrome, what the device actually does to the whole system can be expressed as

$$I^{\otimes 8} Z Z I^{\otimes 17} |\varphi_0\rangle |\varphi_1\rangle |\varphi_2\rangle,$$

which, if block synchronization were correct, would be

$$I^{\otimes 10} Z Z I^{\otimes 15} |\varphi_0\rangle |\varphi_1\rangle |\varphi_2\rangle.$$

$I^{\otimes 8} Z$ does not stabilize $|\varphi_0\rangle$, nor does $ZI^{\otimes 8}|\varphi_1\rangle$. Hence, errors are introduced to the system, rather than detected or corrected. Similarly, if the same misalignment happens during fault-tolerant computation, then the device that tries to apply logical $\bar{X}$ to the third logical block $|\varphi_2\rangle$ will apply $I^{\otimes 16} X^{\otimes 9} II$ to the 27-qubit system.

Other kinds of synchronization error such as deletion may be considered in the quantum setting (see [17] for mathematical models of such errors in the classical case). As in the classical coding theory, however, we would like to separately treat them and do not consider fundamentally different types of synchronization in the current paper. Instead, we assume that no qubit loss or gain in the system occurs and that a device regains access to all of the qubits in proper order in the system if misalignment is correctly detected.

Our objective is to ensure that the device identifies, without destroying quantum states, how many qubits off it is from the proper alignment should misalignment occur. A code that is designed for detecting this type of misalignment is called a *synchronizable code* in the modern information theory literature. Borrowing this term, we call a coding scheme a *quantum synchronizable* (a_l, a_r)-$[[n,k]]$ *code* if it encodes k logical qubits into n physical qubits and corrects misalignment by up to a_l qubits to the left and up to a_r qubits to the right.

We assume that a linear combination of I, X, Z, and Y acts on each qubit independently over a noisy quantum channel. For error correction against such errors, we employ a version of syndrome decoding and show how to correct errors. In principle, the true values of the minimum distances of our quantum synchronizable codes can be computed. However, we focus on how many nontrivial quantum errors our decoding procedure can correct. Hence, the actual minimum distances of our quantum synchronizable codes may be larger than what our decoding algorithm suggests.

In what follows, we give a general construction for quantum synchronizable error-correcting codes and describe the procedures of encoding, error correction, synchronization recovery, and decoding. An infinite class of such quantum codes will be given at the end of the next section as an example.

III. CODING SCHEME

In this section, we give the mathematical details of our solution and show how to realize quantum synchronizable codes. We employ classical and quantum coding theory. For the basic facts and notions in classical and quantum coding theories, the reader is referred to [2,18].

A. Preliminaries

As usual, we define a binary linear $[n,k]$ code as a k-dimensional subspace of the n-dimensional vector space $\mathbb{F}_2^n$ over the finite field of order two. Because we do not consider a code over another field, we always assume that a classical code is binary unless otherwise stated.

A *cyclic* code $\mathcal{C}$ is a linear $[n,k]$ code with the property that if $\boldsymbol{c} = (c_0, \ldots, c_{n-1})$ is a codeword of $\mathcal{C}$, then so is

every cyclic shift of $\boldsymbol{c}$. It is known that by regarding each codeword as the coefficient vector of a polynomial in $\mathbb{F}_2[x]$, a cyclic code can be seen as a principal ideal in the ring $\mathbb{F}_2[x]/(x^n - 1)$ generated by the unique monic nonzero polynomial $g(x)$ of minimum degree in the code which divides $x^n - 1$. Computations in $\mathbb{F}_2[x]/(x^n - 1)$ are modulo $x^n - 1$. A cyclic shift thus corresponds to multiplying by x, and the code can be written as $\mathcal{C} = \{i(x)g(x)| \deg(i(x)) < k\}$. Multiplying by x is an automorphism. The orbit of a given codeword $i(x)g(x)$ by this group action is written as $\mathrm{Orb}(i(x)g(x)) = \{i(x)g(x), xi(x)g(x), x^2 i(x)g(x), \dots\}$.

Let $\mathcal{C}$ and $\mathcal{D}$ be two linear codes of the same length. $\mathcal{D}$ is $\mathcal{C}$-*containing* if $\mathcal{C} \subseteq \mathcal{D}$. It is *dual-containing* if it contains its dual $\mathcal{D}^\perp = \{\boldsymbol{d}^\perp \in \mathbb{F}_2^n \mid \boldsymbol{d} \cdot \boldsymbol{d}^\perp = \boldsymbol{0}, \boldsymbol{d} \in \mathcal{D}\}$. The Calderbank-Shor-Steane construction [19,20] turns a $\mathcal{C}$-containing linear code into a quantum error-correcting code, called a *CSS* code. If we apply a dual-containing $[n,k,d]$ linear code, the resulting CSS code is of parameters $[[n,2k-n,d']]$ for some $d' \geqslant d$. In terms of block synchronization, this CSS code is a quantum synchronizable (0,0)-$[[n,2k-n]]$ code, as the code tolerates no synchronization error. Any combination of up to $\lfloor \frac{d-1}{2} \rfloor$ quantum errors can be corrected through a separate two-step error-correction procedure by directly exploiting the error-correction mechanism of the corresponding classical code. A higher quantum error-correction capability may be achieved if the code is degenerate. For the sake of simplicity, however, we do not investigate the degeneracy of each individual quantum error-correcting code. In the remainder of this paper, we assume familiarity with the structure of CSS codes as well as their basic encoding and decoding mechanisms given in a standard textbook such as [2].

B. Main theorem

Our main theorem employs a pair of cyclic codes $\mathcal{C}$ and $\mathcal{D}$ satisfying $\mathcal{C}^\perp \subseteq \mathcal{C} \subset \mathcal{D}$ to generate a quantum synchronizable code.

Theorem. If there exist a dual-containing cyclic $[n,k_1,d_1]$ code $\mathcal{C}$ and a $\mathcal{C}$-containing cyclic $[n,k_2,d_2]$ code with $k_1 < k_2$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < k_2 - k_1$ there exists a quantum synchronizable (a_l,a_r)-$[[n + a_l + a_r, 2k_1 - n]]$ code that corrects at least up to $\lfloor \frac{d_1-1}{2} \rfloor$ phase errors and at least up to $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors.

To prove the above theorem, we realize a quantum synchronizable code as a carefully translated vector space similar to a CSS code. The proof of the above theorem will be completed in Sec. III D 5 after describing encoding and decoding procedures in Secs. III C and III D 1–4.

Let $\mathcal{C}$ be a dual-containing cyclic $[n,k_1,d_1]$ code that lies in another cyclic $[n,k_2,d_2]$ code $\mathcal{D}$ with $k_1 < k_2$. Define $g(x)$ as the the generator of $\mathcal{D} = \langle g(x) \rangle$, which is the unique monic nonzero polynomial of minimum degree in $\mathcal{D}$. Define also $h(x)$ as the generator of $\mathcal{C}$, which is the unique monic nonzero polynomial of minimum degree in $\mathcal{C}$. Since $\mathcal{C} \subset \mathcal{D}$, the generator $g(x)$ divides every codeword of $\mathcal{C}$. Hence, $h(x)$ can be written as $h(x) = f(x)g(x)$ for some polynomial $f(x)$ of degree $n - k_1 - \deg(g(x)) = k_2 - k_1$.

For every polynomial $j(x) = j_0 + j_1 x + \cdots + j_{n-1}x^{n-1}$ of degree less than n, define $|j(x)\rangle$ as the n-qubit quantum state $|j(x)\rangle = |j_0\rangle|j_1\rangle \cdots |j_{n-1}\rangle$. For a set J of polynomials of

degree less than n, we define $|J\rangle$ as

$$|J\rangle = \frac{1}{|J|} \sum_{j(x) \in J} |j(x)\rangle.$$

For a polynomial $k(x)$, we define $J + k(x) = \{j(x) + k(x) \mid j(x) \in J\}$.

Let $R = \{r_i(x)|0 \leqslant i \leqslant 2^{2k_1 - n - 1}\}$ be a system of representatives of the cosets $\mathcal{C}/\mathcal{C}^\perp$. Consider the set $V_g = \{|\mathcal{C}^\perp + r_i(x) + g(x)\rangle |r_i(x) \in R\}$ of $2^{2k_1 - n}$ states. Because R is a system of representatives, these $2^{2k_1 - n}$ states form an orthonormal basis. Let $\mathcal{V}_g$ be the vector space of dimension $2^{2k_1 - n}$ spanned by V_g. We employ this translated space $\mathcal{V}_g$ to prove our main theorem.

C. Encoding

Take a full-rank parity-check matrix $H_\mathcal{D}$ of $\mathcal{D}$. For each row of $H_\mathcal{D}$, replace zeros with I's and ones with X's. Perform the same replacement with I's for zeros and Z's for ones. Because $\mathcal{C}^\perp \subset \mathcal{C} \subset \mathcal{D}$ implies $\mathcal{D}^\perp \subset \mathcal{D}$, the code $\mathcal{D}$ is a dual-containing cyclic code of dimension k_2. Hence, the resulting $2(n - k_2)$ Pauli operators on n qubits form stabilizer generators $\mathcal{S}_\mathcal{D}$ of the Pauli group on n qubits that fixes a subspace of dimension 2^{k_2}. The set of the Pauli operators on n qubits in $\mathcal{S}_\mathcal{D}$ that consist of only Z's and I's is referred to as $\mathcal{S}_\mathcal{D}^Z$. Construct stabilizer generators $\mathcal{S}_\mathcal{C}$ in the same manner by using $\mathcal{C}$.

Take an arbitrary $(2k_1 - n)$-qubit state $|\varphi\rangle$, which is to be encoded. By using an encoder for the CSS code of parameters $[[n, 2k_1 - n]]$ defined by $\mathcal{S}_\mathcal{C}$, the state $|\varphi\rangle$ is encoded into n-qubit state $|\varphi\rangle_{\mathrm{enc}} = \sum_i \alpha_i |\boldsymbol{v}_i\rangle$, where each $\boldsymbol{v}_i$ is an n-dimensional vector with the orthogonal basis being $\{|\mathcal{C}^\perp + r_i(x)\rangle |r_i(x) \in R\}$. Let $U_{\boldsymbol{g}}$ be the unitary operator that adds the coefficient vector $\boldsymbol{g}$ of $g(x)$. By applying $U_{\boldsymbol{g}}$, we have

$$U_{\boldsymbol{g}}|\varphi\rangle_{\mathrm{enc}} = \sum_i \alpha_i |\boldsymbol{v}_i + \boldsymbol{g}\rangle.$$

Take a pair of non-negative integers a_l, a_r that satisfy $a_l + a_r < k_2 - k_1$. Using $a_l + a_r$ ancilla qubits and CNOT gates, we take this state to an $(n + a_l + a_r)$-qubit state as follows:

$$|0\rangle^{\otimes a_l} U_{\boldsymbol{g}}|\varphi\rangle_{\mathrm{enc}}|0\rangle^{\otimes a_r} \to \sum_i \alpha_i |\boldsymbol{w}_i^1, \boldsymbol{v}_i + \boldsymbol{g}, \boldsymbol{w}_i^2\rangle,$$

where $\boldsymbol{w}_i^1$ and $\boldsymbol{w}_i^2$ are the last a_l and the first a_r portions of the vector $\boldsymbol{v}_i + \boldsymbol{g}$, respectively. The resulting state $|\psi\rangle_{\mathrm{enc}} = \sum_i \alpha_i |\boldsymbol{w}_i^1, \boldsymbol{v}_i + \boldsymbol{g}, \boldsymbol{w}_i^2\rangle$ then goes through a noisy quantum channel.

D. Error correction and block synchronization

Gather $n + a_l + a_r$ consecutive qubits $G = (q_0, \dots, q_{n+a_l+a_r-1})$. We assume the situation where correct block synchronization means that G is exactly the qubits of $|\psi\rangle_{\mathrm{enc}}$, but G can be misaligned by a qubits to the right, where $-a_l \leqslant a \leqslant a_r$.

Let $P = (p_0, \dots, p_{n+a_l+a_r-1})$ be the $n + a_l + a_r$ qubits of the encoded state. If $a = 0$, then $P = G$. Define $G_m = (q_{a_l}, \dots, q_{a_l+n-1})$. By assumption, $G_m = (p_{a_l+a}, \dots, p_{a_l+n-1+a})$. Let n-fold tensor product E of linear combinations of the Pauli matrices be the errors that occurred on P.

We first outline the bit error correction procedure on the window G_m. Synchronization is recovered after making G_m free from bit errors. The bit errors outside of G_m are then corrected. The phase errors on qubits will be treated at the final step after reversing the extension process.

1. Bit error correction on the initial window

We correct bit errors that occurred on qubits in G_m in the same manner as the separate two-step error-correction procedure for a CSS code. Since $\mathcal{C} \subset \mathcal{D}$, the vector space spanned by the orthogonal basis stabilized by $\mathcal{S}_\mathcal{D}$ contains $\mathcal{V}_g$ as a subspace. Hence, through a unitary transformation using $\mathcal{S}_\mathcal{D}^Z$, we can obtain the error syndrome in the same manner as when detecting errors with the CSS code defined by $\mathcal{S}_\mathcal{D}$ as follows:

$$E|\psi\rangle_{\text{enc}}|0\rangle^{\otimes n-k_2} \to E|\psi\rangle_{\text{enc}}|\chi\rangle,$$

where $|\chi\rangle$ is the $(n - k_2)$-qubit syndrome by $\mathcal{S}_\mathcal{D}^Z$. If E introduced at most $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors on qubits in G_m, these quantum errors are detected and then corrected by applying the X operators if necessary.

More formally, rewrite the original encoded state $|\psi\rangle_{\text{enc}} = \sum_i \alpha_i |\boldsymbol{w}_i^1, \boldsymbol{v}_i + \boldsymbol{g}, \boldsymbol{w}_i^2\rangle$ as

$$|\psi\rangle_{\text{enc}} = \sum_i \alpha_i |\boldsymbol{l}_i, \boldsymbol{c}_i, \boldsymbol{r}_i\rangle,$$

where $\boldsymbol{c}_i$ correspond to the window misaligned by a qubits to the right, which can be obtained by cyclically shifting $\boldsymbol{v}_i + \boldsymbol{g}$. Hence, the binary vectors $\boldsymbol{l}_i$, and $\boldsymbol{r}_i$ are of lengths $a_l + a$ and $a_r - a$, respectively.

Without loss of generality, we consider E the discretized bit errors and phase errors on the $n + a_l + a_r$ qubits of $|\psi\rangle_{\text{enc}}$. Let $\boldsymbol{e}^b$ be the $(n + a_l + a_r)$-dimensional binary error vector such that $i \in \text{supp}(\boldsymbol{e}^b)$ if and only if a bit error occurred on qubit p_i. In other words, the positions of 1's in $\boldsymbol{e}^b$ represent which qubits are bitwise flipped. Define the phase error vector $\boldsymbol{e}^p$ in the same way for the phase errors that occurred on $|\psi\rangle_{\text{enc}}$. Then, the transformation due to the noisy quantum channel that introduced quantum error E is

$$|\psi\rangle_{\text{enc}} \to E|\psi\rangle_{\text{enc}} = \sum_i \alpha_i (-1)^{(\boldsymbol{l}_i, \boldsymbol{c}_i, \boldsymbol{r}_i) \cdot \boldsymbol{e}^p} |(\boldsymbol{l}_i, \boldsymbol{c}_i, \boldsymbol{r}_i) + \boldsymbol{e}^b\rangle.$$

Write the bit error vector as $\boldsymbol{e}^b = (\boldsymbol{e}_l^b, \boldsymbol{e}_c^b, \boldsymbol{e}_r^b)$, where $\boldsymbol{e}_l^b$, $\boldsymbol{e}_c^b$, and $\boldsymbol{e}_r^b$ are the first $a_l + a$, next n, and last $a_r - a$ bits of $\boldsymbol{e}^b$, respectively. Recall that $H_\mathcal{D}$ is the full-rank parity-check matrix of $\mathcal{D}$ corresponding to the stabilizer generators. We perform the following unitary transformation using $\mathcal{S}_\mathcal{D}^Z$ with $n - k_2$ ancilla qubits:

$$E|\psi\rangle_{\text{enc}}|0\rangle^{\otimes n-k_2} \to E|\psi\rangle_{\text{enc}}|H_\mathcal{D}\boldsymbol{e}_c^b\rangle.$$

Because $H_\mathcal{D}$ is a parity-check matrix of $\mathcal{D}$, measuring the ancilla gives the error syndrome in the same manner as the corresponding classical linear code does. Thus, as in the standard bit error correction procedure for a CSS code, if we assume that E introduced at most $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors on qubits in G_m, then applying X operators to qubits specified by the error syndrome $H_\mathcal{D}\boldsymbol{e}_c^b$ takes the encoded state with errors to

$$E'|\psi\rangle_{\text{enc}} = \sum_i \alpha_i (-1)^{(\boldsymbol{l}_i, \boldsymbol{c}_i, \boldsymbol{r}_i) \cdot \boldsymbol{e}^p} |(\boldsymbol{l}_i, \boldsymbol{c}_i, \boldsymbol{r}_i) + (\boldsymbol{e}_l^b, \boldsymbol{0}, \boldsymbol{e}_r^b)\rangle,$$

where E' represents the partially corrected quantum errors.

2. Synchronization recovery

We perform synchronization recovery by exploiting the bit error free G_m we just obtained. Recall that all codewords of $\mathcal{C}^\perp$ and $r_i(x) \in R$ belong to $\mathcal{C}$, and hence to $\mathcal{D}$ as well. Because $g(x)$ is the generator of $\mathcal{D}$, it divides any polynomial of the form $s(x) + r_i(x) + g(x)$ over $\mathbb{F}_2[x]/(x^n - 1)$, where $s(x) \in \mathcal{C}^\perp$. Since we have

$$s(x) + r_i(x) + g(x) = i_0(x)f(x)g(x) + i_1(x)f(x)g(x) + g(x)$$

for some polynomials $i_0(x)$ and $i_1(x)$ of degree less than k_1, the quotient is of the form $j(x)f(x) + 1$ for some polynomial $j(x)$. Dividing the quotient by $f(x)$ gives 1 as the remainder. Note that $g(x)$ is a monic polynomial of degree $n - k_2$ that divides $x^n - 1$, where k_2 is strictly larger than $\lceil \frac{n}{2} \rceil$. Let i be an integer satisfying $1 \leqslant i \leqslant \lceil \frac{n}{2} \rceil \leqslant k_2 - 1$. Then,

$$\deg(x^i g(x)) = n - k_2 + i \neq \deg(g(x)).$$

Hence, we have $|\text{Orb}(g(x))| \geqslant k_2 > \lceil \frac{n}{2} \rceil$. Because $|\text{Orb}(g(x))|$ must divide n, we have $|\text{Orb}(g(x))| = n$. Thus, applying the same two-step division procedure to any polynomial appearing as a state in cyclically shifted V_g by a qubits gives $x^a \pmod{f(x)}$ as the remainder. By assumption, we have

$$0 < a_l + a_r < k_2 - k_1 = \deg(f(x))$$

and $-a_l \leqslant a \leqslant a_r$. Thus, the remainder $x^a \pmod{f(x)}$ is unique to each possible value of a.

Recall that every state in V_g is of the form $|\mathcal{C}^\perp + r_i(x) + g(x)\rangle$. Because G_m contains no bit errors, the basis states of the corresponding portion in $E'|\psi\rangle_{\text{enc}}$ are the cyclically shifted coefficient vectors of the correct polynomials. Let $D_{q_{t(x)}}$ and $D_{r_{t(x)}}$ be the polynomial division operations on n qubits that give the quotient and remainder, respectively, through quantum shift registers defined by a polynomial $t(x)$ of degree less than n [21] (see also [22] for an alternative way to implement quantum shift registers). Let $\mathfrak{Q} = I^{\otimes a_l + a} D_{q_{g(x)}} I^{\otimes a_r - a}$ and $\mathfrak{R} = I^{\otimes n + a_l + a_r} D_{r_{f(x)}}$, so that the two represent applying $D_{q_{g(x)}}$ to the window and $D_{r_{f(x)}}$ to the ancilla qubits of $D_{q_{g(x)}}$ that contain the calculated quotient. These operations give the syndrome for the synchronization error as

$$E'|\psi\rangle_{\text{enc}}|0\rangle^{\otimes n} \xrightarrow{\mathfrak{R}\mathfrak{Q}} E'|\psi\rangle_{\text{enc}}|x^a \pmod{f(x)}\rangle,$$

where $|0\rangle^{\otimes n}$ is the ancilla for $D_{q_{g(x)}}$. Hence, by regarding the remainder $x^a \pmod{f(x)}$ as the syndrome of synchronization error a, the magnitude and direction are identified.

3. Bit error correction outside the initial window

Because we obtained the information about how many qubits away $G = (q_0, \ldots, q_{n+a_l+a_r-1})$ is from the proper position $P = (p_0, \ldots, p_{n+a_l+a_r-1})$ and in which direction, by assumption, we can correctly shift the window to the last n qubits $(p_{a_l+a_r}, \ldots, p_{n+a_l+a_r-1})$ of P. Note that if a is negative, then the last $|a|$ qubits are outside of G, which means that the receiver may be required to gather $|a|$ more qubits in addition to the consecutive $n + a_l + a_r$ qubits initially received. Because we employed classical cyclic codes, the same error-correction procedure can be performed on $(p_{a_l+a_r}, \ldots, p_{n+a_l+a_r-1})$, allowing for correcting bit errors that may have occurred on the last n qubits of P. By the same

token, moving the window to the first n qubits of P enables us to correct the remaining bit errors on P. Thus, if the channel introduced at most $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors on any consecutive n qubits, we can correct all bit errors that occurred on P to obtain $E''|\psi\rangle_{\text{enc}}$, where E'' only introduces phase errors.

4. Phase error correction

Next we correct the effect of the phase errors that occurred on qubits in P. The first step we take is to reverse the extension operation and the unitary operation U_g that transformed the n-qubit encoded state $|\varphi\rangle_{\text{enc}} = \sum_i \alpha_i |v_i\rangle$ into the $(n + a_l + a_r)$-qubit state $|\psi\rangle_{\text{enc}} = \sum_i \alpha_i |w_i^1, v_i + g, w_i^2\rangle$. Here we straightforwardly apply the same CNOT operations to the qubits in $E''|\psi\rangle_{\text{enc}}$ as we did when extending $U_g |\varphi\rangle_{\text{enc}}$, then discard the $a_l + a_r$ qubits that were initially ancilla qubits for extension, and finally apply U_g again to the resulting n-qubit state.

Write the phase error vector as $e^p = (e_l^p, e_c^p, e_r^p)$, where the binary error vectors e_l^p, e_c^p, and e_r^p correspond to the phase errors that occurred on the first a_l, next n, and last a_r qubits of P. Then, the above reversing operation can be described by the following transformation:

$$E''|\psi\rangle_{\text{enc}} \to \sum_i \alpha_i (-1)^{(v_i+g)\cdot(e_c^p+(0,e_l^p)+(e_r^p,0))} |v_i\rangle$$
$$= e^{i\theta} \sum_i \alpha_i (-1)^{v_i \cdot (e_c^p+(0,e_l^p)+(e_r^p,0))} |v_i\rangle,$$

where θ is some multiple of π, and $(0, e_l^p)$ and $(e_r^p, 0)$ are the n-dimensional binary vectors obtained by padding $n - a_l$ and $n - a_r$ zeros to the head of e_l^p and the tail of e_r^p, respectively. Note that by writing as n_p the number of qubits on which the phase errors occurred among the $n + a_l + a_r$ qubits, we have

$$\left| \text{supp}\left(e_c^p + (0, e_l^p) + (e_r^p, 0) \right) \right|$$
$$\leqslant \left| \text{supp}(e_c^p) \right| + \left| \text{supp}((0, e_l^p)) \right| + \left| \text{supp}((e_r^p, 0)) \right|$$
$$= n_p.$$

The encoded state $|\varphi\rangle_{\text{enc}}$ is stabilized by $\mathcal{S}_{\mathcal{C}}$. Thus, ignoring the global phase factor $e^{i\theta}$, if $n_p \leqslant \lfloor \frac{d_1-1}{2} \rfloor$, we can correctly diagnose the effect of $e_c^p + (0, e_l^p) + (e_r^p, 0)$ through the standard phase error correction procedure for the CSS code based on the dual-containing cyclic code $\mathcal{C}$:

$$E'''|\varphi\rangle_{\text{enc}} |0\rangle^{\otimes n-k_1} \to E'''|\varphi\rangle_{\text{enc}} \big| H_{\mathcal{C}}\big(e_c^p + (0, e_l^p) + (e_r^p, 0) \big)\big\rangle,$$

where $H_{\mathcal{C}}$ is a full-rank parity-check matrix of $\mathcal{C}$ and E''' is the phase error operator on $|\varphi\rangle_{\text{enc}}$ that represents the effect of $e_c^p + (0, e_l^p) + (e_r^p, 0)$. Applying Z operators on the qubits specified by the syndrome completes the error correction procedure.

5. Proof of the Theorem and example codes

We are now able to prove our main theorem.

Proof of Theorem. Take a dual-containing cyclic $[n, k_1, d_1]$ code $\mathcal{C}$ that is contained in a cyclic $[n, k_2, d_2]$ code, where $k_1 < k_2$. Encode $2k_1 - n$ logical qubits into $n + a_l + a_r$ physical qubits as described above. The error-correction and synchronization recovery procedures described above correct misalignment by a qubits to the right, as long as a lies in the range $-a_l \leqslant a \leqslant a_r$, and correct up to $\lfloor \frac{d_1-1}{2} \rfloor$ phase errors on the $n + a_l + a_r$ qubits and up to $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors on any consecutive n qubits. The final decoding step is completed

by reducing the state $|\varphi\rangle_{\text{enc}} = \sum_i \alpha_i |v_i\rangle$ to the original state $|\varphi\rangle$ by a decoding circuit of the CSS code based on the dual-containing cyclic code $\mathcal{C}$. Thus, the scheme is a quantum synchronizable (a_l, a_r)-$[[n + a_l + a_r, 2k_1 - n]]$ code with the desired error-correction capability. ∎

To take full advantage of this Theorem, we need dual-containing cyclic codes that achieve large minimum distance and contain dual-containing cyclic codes of smaller dimension. A class of the well-known Bose-Chaudhuri-Hocquenghem (BCH) codes [18] gives such classical codes. The dual-containing properties of BCH codes have been thoroughly investigated in [23,24]. The following is an infinite series of quantum synchronizable error-correcting codes based on a class of such codes, called the *primitive, narrow-sense* BCH codes (see [18] for the definition and basic properties of primitive, narrow-sense BCH codes):

Corollary. Let n, d_1, and d_2 be odd integers satisfying $n = 2^m - 1$ and $3 \leqslant d_2 < d_1 \leqslant 2^{\lceil \frac{m}{2} \rceil} - 1$, where $m \geqslant 5$. Then, for some $d_1' \geqslant d_1$, some $d_2' \geqslant d_2$, and any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < \frac{m(d_1-d_2)}{2}$, there exists a quantum synchronizable (a_l, a_r)-$[[n + a_l + a_r, n - m(d_2 - 1)]]$ code that corrects up to $\frac{d_1'-1}{2}$ phase errors on the $n + a_l + a_r$ qubits and up to $\frac{d_2'-1}{2}$ bit errors on any consecutive n qubits.

Proof. Let n, d_1, and d_2 be integers satisfying the condition given in the statement. Let $\mathcal{D}$ be a primitive narrow-sense BCH code of length n and designed distance d_2 such that $3 \leqslant d_2 < 2^{\lceil \frac{m}{2} \rceil} - 1$. Construct a primitive narrow-sense BCH code $\mathcal{C}$ by joining one or more cyclotomic cosets, so that its designed distance d_1 is larger than d_2 but smaller than or equal to $2^{\lceil \frac{m}{2} \rceil} - 1$. The dimensions of $\mathcal{C}$ and $\mathcal{D}$ are $n - \frac{m(d_1-1)}{2}$ and $n - \frac{m(d_2-1)}{2}$, respectively. $\mathcal{D}$ contains $\mathcal{C}$, and the two cyclic codes are both dual-containing (see [23]), forming the desired quantum synchronizable codes. ∎

IV. CONCLUSION

We developed a coding scheme that seamlessly integrates block synchronization and quantum error correction. A close relation is found between quantum synchronizable error-correcting codes and pairs of cyclic codes with special properties. Through this relation, the well-known BCH codes were shown to generate desirable quantum codes for block synchronization.

In classical communications, a unified method for synchronization and error correction can reduce implementation complexity [25]. A similar method using cyclic codes has also been proposed recently in the classical domain for simple implementation of asynchronous code division multiple access (CDMA) systems with random delays [26]. We hope that our seamlessly unified solution to block synchronization and quantum error correction may help simplify requirements on hardware and open up new possibilities of quantum computation and quantum communication, such as transmission of a large amount of consecutive quantum information blocks with little aid from classical communications.

One potential weakness of the approach presented in this paper is that our quantum synchronizable codes of length $n + a_l + a_r$ may face a larger number of quantum errors

than the underlying standard CSS codes of length n would because of their extended lengths. For instance, in a scenario where the receiver missed the first several qubits, the window may be suffering from severe quantum errors, which may not be correctable. Phase error correction requires particular attention in this regard because while the current scheme takes advantage of the subcode $\mathcal{C}$, which typically has a larger minimum distance than $\mathcal{D}$ for bit errors, the error-correction scheme for phase errors is expected to handle all phase errors at once, unlike the bit error correction procedure. While the ability to recover from misalignment is highly valuable because even the slightest synchronization error is fatal to information transmission, these weaknesses should be noted and are worthy of further investigation.

One aspect we may be able to improve is the maximum magnitude of a correctable synchronization error. The scheme presented in this paper relies on the uniqueness of the syndrome for each possible combination of the magnitude and direction. While the remainder $x^a \pmod{f(x)}$ after the two-step division procedure for synchronization recovery is certainly unique if we limit $a_l + a_r$ to be less than $\deg(f(x))$, this may be overly conservative in a sense. In fact, there are $2^{\deg(f(x))}$ possible polynomials of degree $\deg(f(x))$ or smaller while we only need at most n distinct synchronization error syndromes even if we extend a CSS code of length n to a full $2n$-qubit code by copying all n qubits with CNOT gates. While our scheme does not appear to allow a better general bound on the maximum correctable magnitude

in a simple form without a deeper observation and careful modification, it is plausible that a sophisticated treatment of syndromes may yield quantum synchronizable codes with better synchronization error tolerance than is proved in this paper.

Finally, while we have focused on binary dual-containing cyclic codes, it is certainly of interest to look into more general approaches to quantum error correction, such as orthogonal pairs of cyclic codes that are not dual-containing and the quantum error-correcting codes from additive codes over $\mathbb{F}_4$ found in [27]. While CSS codes and similar quantum error-correcting codes based on classical cyclic codes that admit decoding through quantum shift registers have not been studied very well in the literature, there are some examples that have very similar structures, such as quantum Reed-Solomon codes [28] (see also [21] for a possible decoding scheme for this type of quantum error-correcting code through quantum shift registers). A further look into these types of quantum cyclic code would be of interest.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2000).

[3] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo Phys. Rev. Lett. **81**, 2152 (1998).

[4] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne, Phys. Rev. Lett. **86**, 5811 (2001).

[5] J. Chiaverini *et al.*, Nature (London) **432**, 602 (2004).

[6] N. Boulant, L. Viola, E. M. Fortunato, and D. G. Cory, Phys. Rev. Lett. **94**, 130501 (2005).

[7] P. Schindler *et al.*, Science **332**, 1059 (2011).

[8] O. Moussa, J. Baugh, C. A. Ryan, and R. Laflamme, Phys. Rev. Lett. **107**, 160501 (2011).

[9] M. D. Reed *et al.*, Nature (London) **482**, 382 (2012).

[10] X.-C. Yao *et al.*, Nature (London) **482**, 489 (2012).

[11] J. Zhang, R. Laflamme, and D. Suter, Phys. Rev. Lett. **109**, 100503 (2012).

[12] To avoid confusion with "shared reference frames" treated in [29], we use the term "block" as a synonym for "frame" throughout this paper.

[13] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).

[14] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed. (Prentice-Hall, Upper Saddle River, NJ, 2001).

[15] S. Bregni, *Synchronization of Digital Telecommunications Networks* (Wiley, West Sussex, England, 2002).

[16] One may argue that because of the no-cloning theorem, quantum communication would largely be restricted to point-to-point systems in which block synchronization is easier to establish than in broadcast networks. However, the very theorem forbids arguably the simplest and popular solution to any kind of error including synchronization errors, that is, requesting a perfect copy of lost information. Moreover, in quantum computing scenarios, because large-scale computing systems would benefit from internal communications between components and/or external communications, a fundamental building block of communications would become increasingly more relevant as the scale of realizable quantum computation grows.

[17] H. Mercier, V. K. Bhargava, and V. Tarokh, IEEE Commun. Surveys Tutorials **12**, 87 (2010).

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

[19] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[20] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[21] M. Grassl and T. Beth, Proc. R. Soc. London Ser. A **456**, 2689 (2000).

[22] M. M. Wilde, Phys. Rev. A **79**, 062325 (2009).

[23] A. M. Steane, IEEE Trans. Inf. Theory **45**, 2492 (1999).

[24] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, IEEE Trans. Inf. Theory **53**, 1183 (2007).

[25] L. F. Chang, N. R. Sollenberger, and S. Ariyavisitakul, IEEE Trans. Commun. **41**, 22 (1993).

[26] Y.-W. Wu and S.-C. Chang, IEEE Trans. Inf. Theory **56**, 3786 (2010).

[27] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).

[28] M. Grassl, W. Geiselmann, and T. Beth, in *Lecture Notes in Computer Science*, Proc. Applied Algebra, Algebraic Algorithm and Error-Correcting Codes No. 1719, edited by M. Fossorier, H. Imai, S. Lin, and A. Poli (Springer, Berlin, 1999), pp. 231–244.

[29] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555 (2007).