7-16-2013

Algebraic techniques in designing quantum synchronizable codes

Yuichiro Fujiwara
California Institute of Technology

Vladimir Tonchev
Michigan Technological University

Tony Wong
California Institute of Technology

Algebraic techniques in designing quantum synchronizable codes

Yuichiro Fujiwara,[1,*] Vladimir D. Tonchev,[2] and Tony W. H. Wong[1]

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

[2]*Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA*

(Received 31 March 2013; published 16 July 2013)

Quantum synchronizable codes are quantum error-correcting codes that can correct the effects of quantum noise as well as block synchronization errors. We improve the known general framework for designing quantum synchronizable codes through more extensive use of the theory of finite fields. This makes it possible to widen the range of tolerable magnitude of block synchronization errors while giving mathematical insight into the algebraic mechanism of synchronization recovery. Also given are families of quantum synchronizable codes based on punctured Reed-Muller codes and their ambient spaces.

DOI: 10.1103/PhysRevA.88.012318 PACS number(s): 03.67.Pp, 03.67.Hk

I. INTRODUCTION

Quantum error correction is a fundamental tool in quantum information science that allows for quantum information processing in a noisy environment. Quantum noise is typically described by operators that act on qubits, with the most general model being the linear combinations of the Pauli operators I, X, Y, and Z acting on each qubit [1]. In this sense, quantum error-correcting codes can be seen as coding techniques that allow for recovering the original quantum state when unintended operators may act on some qubits.

Active quantum error detection is an important method for suppressing quantum noise, where one extracts the information about what kind of quantum error occurred on which qubit through measurement without learning anything about the quantum information carried by qubits. With this information, the effect of quantum noise can be reversed by applying appropriate quantum operations.

Very recently, a scheme that actively deals with a different type of error due to misalignment with respect to the block structure of a qubit stream was introduced [2]. To describe the kind of misalignment the scheme considers, assume that we have three qubits q_0, q_1, q_2, and encode each of them by the perfect five-qubit code given in [3] (see [4,5] for different realizations of the perfect five-qubit code). Then the quantum information we have can be expressed by a sequence of fifteen qubits, where each five-qubit state $|\psi_i\rangle$, $i = 0,1,2$, represents one logical qubit of quantum information that corresponds to the original qubit q_i. In order to correctly process quantum information, we need to know the exact location of the boundary of each five-qubit block in the 15-qubit state $|\psi_0\rangle|\psi_1\rangle|\psi_2\rangle$. For instance, if misalignment occurs by two qubits to the left when handling the stream of 15 qubits, a quantum device trying to correct quantum errors on $|\psi_1\rangle$ will apply the quantum operation on the wrong set of five qubits, two of which come from $|\psi_0\rangle$ and three of which belong to $|\psi_1\rangle$. More complicated examples involving other types of errors include failure in detecting photons at the beginning of photonic quantum communication, where the receiver misses the first photon at the start of communications and wrongly assumes that the following five photons that are properly detected form an encoded five-qubit block. In this case, misalignment and a quantum error due to qubit loss occur simultaneously.

The current paper studies a coding scheme that allows for extracting the information about the magnitude and direction of misalignment through nondisturbing measurement while simultaneously figuring out the types and positions of standard quantum errors on qubits. In other words, we investigate a quantum analog of *synchronizable error-correcting codes* [6].

More formally, a coding scheme is called 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. To seamlessly achieve quantum error correction and synchronization recovery, we would like quantum synchronizable codes to correct linear combinations of I, X, Z, and Y that act on physical qubits as well. For this task, the known quantum synchronizable error-correcting scheme employs essentially the same two-step quantum error correction procedure as that for Calderbank-Shor-Steane (CSS) codes [7,8]. Hence, in addition to misalignment, the scheme handles discretized bit and phase errors in two separate steps.

The known general method for constructing quantum synchronizable error-correcting codes directly exploits special classical codes over the finite field $\mathbb{F}_2$ of order 2. A *binary linear* $[n,k,d]$ code of *length* n, *dimension* k, and *minimum distance* d is a k-dimensional subspace $\mathcal{L}$ of the n-dimensional vector space $\mathbb{F}_2^n$ such that $\min\{\mathrm{wt}(\boldsymbol{v}) \mid \boldsymbol{v} \in \mathcal{L}, \boldsymbol{v} \neq \boldsymbol{0}\} = d$, where $\mathrm{wt}(\boldsymbol{v})$ is the number of coordinates of $\boldsymbol{v}$ at which entries are nonzero. In what follows, we always assume that classical codes are over $\mathbb{F}_2$ and omit the term binary. A *cyclic* $[n,k,d]$ code $\mathcal{C}$ is a linear $[n,k,d]$ code with the property that every cyclic shift of every codeword $\boldsymbol{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ is also a codeword. 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 $\mathcal{D}^\perp = \{\boldsymbol{d}^\perp \in \mathbb{F}_2^n \mid \boldsymbol{d} \cdot \boldsymbol{d}^\perp = \boldsymbol{0} \text{ for all } \boldsymbol{d} \in \mathcal{D}\}$.

The known general framework for constructing quantum synchronizable codes relies on cyclic codes with special containing properties:

Theorem 1 ([2]). 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 a_l, a_r of non-negative integers

*yuichiro.fujiwara@caltech.edu

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.

Note that if a linear code $\mathcal{C}$ is dual containing, a $\mathcal{C}$-containing linear code is also dual containing [9]. Hence, what the above theorem requires is actually a pair of dual-containing cyclic codes, one of which is strictly contained in another and both of which guarantee large minimum distances. While it is already a challenging problem to construct cyclic codes with good minimum distances, it is not impossible to find infinitely many nontrivial examples satisfying the additional stringent conditions. The following is the family of quantum synchronizable codes explicitly mentioned in the literature.

Theorem 2 ([2]). 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 a_l, a_r of non-negative integers 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 at least up to $\frac{d_1'-1}{2}$ phase errors and at least up to $\frac{d_2'-1}{2}$ bit errors.

The primary purpose of the present paper is to improve the code design framework given in Theorem 1 through careful analysis of the algebraic machinery behind synchronization recovery, as well as to give families of quantum synchronizable codes that are different from the one given in Theorem 2. Our refined framework naturally improves the synchronization recovery capabilities achievable by quantum synchronizable codes even if we use the same cyclic codes as the ones employed in Theorem 2.

In the next section, we briefly review quantum synchronizable coding that forms the basis of Theorem 1 and give a precise description of one key aspect in the form of a mathematical lemma. The coding scheme is reanalyzed in Sec. III to improve its synchronization recovery capabilities. Then Sec. IV enriches realizable parameters by giving families of quantum synchronizable codes based on cyclic codes that have not previously been employed in the context of synchronization recovery. Concluding remarks are given in Sec. V.

II. OVERVIEW OF BLOCK SYNCHRONIZATION FOR QUBITS

Here we review the basics of block synchronization recovery for quantum information. The simple mathematical model considered in [2] is explained in Sec. II A. Then Sec. II B provides the overview and necessary mathematical details of quantum synchronizable coding.

A. Preliminaries

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 $|\bigcup_i F_i| = x$ 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. The set G is said to be *misaligned* by a qubits to the *right* with respect to $(Q, \mathcal{F})$ if there exist 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 $G \in \mathcal{F}$.

With this simple model, the three five-qubit blocks given as an example in the previous section may be seen as $Q = (q_0', \ldots, q_{14}')$, where the three encoded five-qubit blocks $|\psi_0\rangle$, $|\psi_1\rangle$, and $|\psi_2\rangle$ form blocks $F_0 = (q_0', \ldots, q_4')$, $F_1 = (q_5', \ldots, q_9')$, and $F_2 = (q_{10}', \ldots, q_{14}')$, respectively. These 15 qubits are subject to quantum information processing and may be sent to a different place, stored in quantum memory, or immediately processed for quantum computation.

If misalignment occurs by, for instance, two qubits to the left during quantum error correction on $|\psi_1\rangle$, the device applies the quantum error correction procedure to the set G of five qubits $q_3', \ldots, q_7'$, two of which come from F_0 and three of which belong to F_1. For example, when measuring the stabilizer generator $XZZXI$ of the five-qubit code to obtain the syndrome, the operation the device actually performs to the entire system can be expressed as

$$I^{\otimes 3} XZZXI^{\otimes 8} |\psi_0\rangle|\psi_1\rangle|\psi_2\rangle,$$

which, if block synchronization were correct, would be

$$I^{\otimes 5} XZZXI^{\otimes 6} |\psi_0\rangle|\psi_1\rangle|\psi_2\rangle.$$

The operator $I^{\otimes 3} XZ$ does not stabilize $|\psi_0\rangle$, nor does $ZXI^{\otimes 3}$ $|\psi_1\rangle$. Thus the measurement process not only fails to obtain the correct syndrome but also introduces errors to the system. Similarly, if the same misalignment happens during fault-tolerant quantum computation, the device trying to perform the logical $\bar{X}$ operation applies $I^{\otimes 3} XX$ on the first five-qubit block and $XXXI^{\otimes 2}$ on the next five-qubit block.

The goal of quantum synchronizable coding is to make it possible to extract the information about how many qubits away the window is from proper alignment and in which direction should misalignment occur while keeping the quantum information carried by qubits intact. For the sake of simplicity, we assume that a device regains access to all the qubits in proper order in the system if misalignment is correctly detected and identified.

B. Quantum synchronizable coding

In this section we briefly review the mechanism of quantum synchronizable codes introduced in [2] and prove a lemma, which we will use in Sec. III. We assume familiarity with the structure of CSS codes and their encoding and decoding methods. For the basic facts and notions in classical and quantum coding theories, the reader is referred to Refs. [10] and [3].

As defined in Sec. I, a cyclic code $\mathcal{C}$ of length n is a linear code with the property that if $\boldsymbol{c} = (c_0, \ldots, c_{n-1})$ is a codeword of $\mathcal{C}$, then so is the cyclic shift $(c_{n-1}, c_0, \ldots, c_{n-2})$. It is known that by regarding each codeword as the coefficient vector of a polynomial in $\mathbb{F}_2[x]$, a cyclic code of length n 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 $x^n - 1$. When a cyclic code is of length n and dimension k, the set of codewords can be written as $\mathcal{C} = \{i(x)g(x) \mid \deg[i(x)] < k\}$, where the degree $\deg[g(x)]$

of the generator polynomial is $n-k$. A cyclic shift of a codeword naturally corresponds to multiplying by x modulo x^n-1, which is an automorphism of the code. The orbit of a given codeword $i(x)g(x)$ by this group action is written as $\mathrm{Orb}_x[i(x)g(x)] = \{x^a i(x)g(x) \pmod{x^n-1} \mid a \in \mathbb{N}\}$, where $\mathbb{N}$ is the set of positive integers.

Let $\mathcal{C}$ be a linear $[n,k_1,d_1]$ code. Recall that a linear $[n,k_2,d_2]$ code $\mathcal{D}$ is said to be $\mathcal{C}^\perp$ containing if $\mathcal{C}^\perp \subseteq \mathcal{D}$. The CSS construction turns a $\mathcal{C}^\perp$-containing linear code $\mathcal{D}$ into a quantum error-correcting $[[n,k_2-k_1]]$ code capable of correcting up to d_1 phase errors and up to d_2 bit errors through the standard two-step decoding procedure. The framework on which Theorem 1 is built exploits this quantum error correction mechanism, as is suggested by the fact that the theorem requires a pair of cyclic codes $\mathcal{C}$ and $\mathcal{D}$ satisfying $\mathcal{C}^\perp \subseteq \mathcal{C} \subset \mathcal{D}$.

Let $\mathcal{C}$ be a dual-containing cyclic $[n,k_1,d_1]$ code contained in another cyclic $[n,k_2,d_2]$ code $\mathcal{D}$ with $k_1 < k_2$. Define $g(x)$ as the the generator polynomial of $\mathcal{D}$, which is the unique monic nonzero polynomial of minimum degree in $\mathcal{D}$. Define also $h(x)$ as the generator polynomial of $\mathcal{C}$, which is the unique monic nonzero polynomial of minimum degree in $\mathcal{C}$. Since $\mathcal{C} \subset \mathcal{D}$, the generator polynomial $g(x)$ divides every codeword of $\mathcal{C}$, which means that $h(x)$ 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 a polynomial $j(x) = j_0 + j_1 x + \cdots + j_{n-1}x^{n-1}$ of degree less than n over $\mathbb{F}_2$, 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 over $\mathbb{F}_2$, we define $|J\rangle$ as

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

Addition between J and polynomial $k(x) \in \mathbb{F}_2[x]$ is defined as $J + k(x) = \{j(x)+k(x) \mid j(x) \in J\}$.

Let $R = \{r_i(x) \mid 0 \leqslant i \leqslant 2^{2k_1-n-1}\}$ be a system of representatives of the cosets $\mathcal{C}/\mathcal{C}^\perp$. Take the set $V_g = \{|\mathcal{C}^\perp + r_i(x) + g(x)\rangle \mid r_i(x) \in R\}$ 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. This space $\mathcal{V}_g$ plays the key role in extracting the information about the magnitude and direction of a synchronization error through nondisturbing measurement.

1. Encoding

Take a parity-check matrix $H_\mathcal{D}$ of $\mathcal{D}$. We assume that $H_\mathcal{D}$ is of full rank. For each row of $H_\mathcal{D}$, replace zeros with Is and ones with Xs. Perform the same replacement with Is for zeros and Zs for ones. Because the condition that $\mathcal{C}^\perp \subseteq \mathcal{C} \subset \mathcal{D}$ 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 Zs and Is is referred to as $\mathcal{S}_\mathcal{D}^Z$. Construct stabilizer generators $\mathcal{S}_\mathcal{C}$ in the same way by using $\mathcal{C}$.

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

To describe the final step of encoding, we need a notion from algebra. Let $f(x) \in \mathbb{F}_2[x]$ be a polynomial over $\mathbb{F}_2$ such that $f(0) = 1$. The cardinality $\mathrm{ord}[f(x)] = |\{x^a \pmod{f(x)} \mid a \in \mathbb{N}\}|$ is called the *order* of the polynomial $f(x)$. This cardinality is also known as the *period* or *exponent* of $f(x)$. Note that in our case the condition that $h(x)$ divides x^n-1 implies that its factor $f(x)$ also divides it, which dictates that $\mathrm{ord}[f(x)] \leqslant n$. In what follows, when we consider a representative of the equivalence class $f_0(x) \pmod{f_1(x)}$ for given two polynomials $f_0(x)$ and $f_1(x)$, we choose the one with the smallest non-negative degree, that is, the remainder of $f_0(x)$ divided by $f_1(x)$.

Take a pair a_l, a_r of non-negative integers such that $a_l + a_r < \mathrm{ord}[f(x)]$. Using $a_l + a_r$ ancilla qubits and controlled-NOT (CNOT) gates, we take this state to an $(n+a_l+a_r)$-qubit state as follows:

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

where $\boldsymbol{w}_i^1$ and $\boldsymbol{w}_i^2$ are the last a_l and the first a_r bits of the vector $\boldsymbol{v}_i + \boldsymbol{g}$, respectively. The resulting encoded 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.

2. Decoding

To recover the original state $|\varphi\rangle$, gather $n+a_l+a_r$ consecutive qubits $G = (q_0, \ldots, q_{n+a_l+a_r-1})$. If block synchronization is correct, then G is exactly the qubits of $|\psi\rangle_{\mathrm{enc}}$ on which quantum errors may have occurred. We assume the situation where G can be misaligned by a qubits to the right, where $-a_l \leqslant a \leqslant a_r$.

Let $P = (p_0, \ldots, p_{n+a_l+a_r-1})$ be the $n+a_l+a_r$ qubits of the encoded state $|\psi\rangle_{\mathrm{enc}}$. Trivially, if $a = 0$, then $P = G$. Define $G_m = (q_{a_l}, \ldots, q_{a_l+n-1})$. By assumption, we have $G_m = (p_{a_l+a}, \ldots, p_{a_l+n-1+a})$. Let E be the n-fold tensor product of linear combinations of the Pauli matrices which represents the errors that occurred on P.

We first 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. Because $\mathcal{C} \subset \mathcal{D}$, 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 for the window in the same way as when detecting errors with the CSS code defined by $\mathcal{S}_\mathcal{D}$ as follows:

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

where $|\chi\rangle$ is the $(n-k_2)$-qubit syndrome by $\mathcal{S}_\mathcal{D}^Z$ (see [2] for a rigorous proof). 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 accordingly.

Synchronization recovery is performed by taking advantage of the window G_m on which all bit errors are corrected. We describe the procedure as a proof of a lemma that will play an

important role in improving the maximum tolerable magnitude of synchronization errors.

Lemma 3. Let $\mathcal{C}$ be a dual-containing cyclic code of length n and dimension k_1 and $\mathcal{D}$ a $\mathcal{C}$-containing cyclic code of the same length, larger dimension $k_2 > k_1$, and minimum distance d_2. Assume that $h(x)$ and $g(x)$ are the generator polynomials of $\mathcal{C}$ and $\mathcal{D}$, respectively. Define polynomial $f(x)$ of degree $k_2 - k_1$ to be the factor of $h(x)$ such that $h(x) = f(x)g(x)$ over $\mathbb{F}_2[x]/(x^n - 1)$. Then for every pair a_l, a_r of non-negative integers such that $a_l + a_r < \mathrm{ord}[f(x)]$ there exists a quantum synchronizable (a_l,a_r)-$[[n + a_l + a_r, 2k_1 - n]]$ code under the assumption that no sequence of consecutive n qubits suffers from more than $\lfloor \frac{d_2-1}{2} \rfloor$ bit errors.

Proof. Encode an arbitrary $(2k_1 - n)$-qubit state $|\varphi\rangle$ by using a pair $\mathcal{C}$, $\mathcal{D}$ of cyclic codes such that $\mathcal{C}^\perp \subseteq \mathcal{C} \subset \mathcal{D}$ as described in Sec. II B 1. Let operator E be the quantum noise introduced to the encoded state $|\psi\rangle_{\mathrm{enc}}$. We assume the situation where misalignment occurred by a qubits to the right with the condition that $-a_l \leqslant a \leqslant a_r$, where the two non-negative integers satisfy the inequality $a_l + a_r < \mathrm{ord}[f(x)]$. Perform the bit error correction on window G_m as described earlier in Sec. II B 2. These transformations can be expressed as

$$|\varphi\rangle \to |\psi\rangle_{\mathrm{enc}} \to E|\psi\rangle_{\mathrm{enc}} \to E'|\psi\rangle_{\mathrm{enc}},$$

where operator E' represents the partially corrected quantum errors after bit error correction on G_m. Recall that all codewords of $\mathcal{C}^\perp$ and $r_i(x) \in R$ are also codewords of $\mathcal{C}$, and hence of $\mathcal{D}$ as well. Because the polynomial $g(x)$ 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 $i_1(x)$ whose degrees are both 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. It is easy to show that $|\mathrm{Orb}_x[g(x)]| = n$ (see [2] for an elementary proof). Thus, applying the same two-step division procedure to any polynomial appearing as a state in cyclically shifted V_g by a qubits gives the reminder of x^a divided by $f(x)$ in $\mathbb{F}_2[x]/(x^n - 1)$. Because $h(x)$ divides $x^n - 1$, its factor $f(x)$ also divides $x^n - 1$. Hence, the resulting remainder is exactly the representative of $x^a \pmod{f(x)}$ with a non-negative degree less than $k_2 - k_1$. Note that every state in V_g is of the form $|\mathcal{C}^\perp + r_i(x) + g(x)\rangle$. If G_m contains no bit errors after bit error correction, the basis states of the corresponding portion in $E'|\psi\rangle_{\mathrm{enc}}$ are the cyclically shifted coefficient vectors of the correct polynomials. Let $Q_{t(x)}$ and $R_{t(x)}$ be 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 [11]. Let $\mathfrak{Q} = I^{\otimes a_l + a} Q_{g(x)} I^{\otimes a_r - a}$ and $\mathfrak{R} = I^{\otimes n + a_l + a_r} R_{f(x)}$, so that the two represent applying $Q_{g(x)}$ to the window and $R_{f(x)}$ to the ancilla qubits of $Q_{g(x)}$ that contain the calculated quotient. This pair of operations gives the syndrome for the synchronization error as

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

where $|0\rangle^{\otimes n}$ is the ancilla for $Q_{g(x)}$ and $|x^a \pmod{f(x)}\rangle$ is the state defined by the representative of $x^a \pmod{f(x)}$. If $x^b \not\equiv x^c \pmod{f(x)}$ for any pair b, c of distinct non-negative integers less than or equal to $a_l + a_r$, the remainder given as the representative of $x^a \pmod{f(x)}$ uniquely identifies the magnitude and direction of the synchronization error a. By assumption, we have $a_l + a_r < \mathrm{ord}[f(x)]$. Thus we have the cardinality

$$|\{x^a \pmod{f(x)} \mid 0 \leqslant a \leqslant a_l + a_r\}| = a_l + a_r + 1$$

as desired. The proof is complete. ■

With the procedure described in the proof above, we can obtain 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. Thus, 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. 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 allows us to correct the remaining bit errors on P. Hence, 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 the qubits in P.

The remaining decoding procedure for recovering the original $(2k_1 - n)$-qubit state $|\varphi\rangle$ is to shrink the $(n + a_l + a_r)$-qubit state while correcting phase errors. This can be done by running backwards the translation and expansion operations we applied to $|\varphi\rangle_{\mathrm{enc}}$ and then applying a decoding circuit of the CSS code based on the dual-containing cyclic code $\mathcal{C}$ (see [2] for details).

III. IMPROVING SYNCHRONIZATION ERROR TOLERANCE

In this section we examine the maximum tolerable magnitude of synchronization errors.

The reason that Theorem 1 can only tolerate up to a $(k_2 - k_1 - 1)$-qubit shift is that the original proof given in [2] does not use the concept of the order of a polynomial. In fact, in view of Lemma 3, the original proof can be understood as a naive application of a rather conservative lower bound on the order of $f(x)$, namely, $\mathrm{ord}[f(x)] \geqslant \deg[f(x)]$. Here we aim to improve synchronization recovery capabilities by examining the exact value of $\mathrm{ord}[f(x)]$.

To avoid being overly general, we focus on the most relevant case where the code length is a Mersenne number $n = 2^m - 1$. This is because the known quantum synchronizable codes and the ones we will introduce in the next section all have lengths of this form.

Theorem 4. Let m, n be positive integers such that $n = 2^m - 1$, and $\mathcal{C}$, $\mathcal{D}$ a dual-containing cyclic $[n,k_1,d_1]$ code with generator polynomial $h(x)$ and $\mathcal{C}$-containing cyclic $[n,k_2,d_2]$ code with generator polynomial $g(x)$, respectively. Define polynomial $f(x)$ of degree $k_2 - k_1$ as the quotient of $h(x) = f(x)g(x)$ divided by $g(x)$ and write its factorization into irreducible polynomials as $f(x) = \prod_i f_i(x)$. For every pair a_l, a_r of non-negative integers such that $a_l + a_r < \mathrm{lcm}_i\{\mathrm{ord}[f_i(x)]\}$ 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. In particular, the maximum tolerable magnitude $\mathrm{lcm}_i\{\mathrm{ord}[f_i(x)]\} - 1$ attains $n-1$, which is the largest possible, if $f(x)$ has a primitive polynomial $f_i(x)$ of degree m as its factor.

To prove the above theorem, we employ the following four facts in finite fields.

Proposition 5. Let m be a positive integer and $f(x)$ the product of all irreducible polynomials over $\mathbb{F}_2$ whose degrees divide m. Then

$$f(x) = x^{2^m} - x.$$

Proposition 6. Let $f(x) = \prod_i f_i(x)$ be a polynomial over $\mathbb{F}_2$, where $f_i(x)$ are all nonzero and pairwise relatively prime in $\mathbb{F}_2[x]$. Then

$$\mathrm{ord}[f(x)] = \mathrm{lcm}_i\{\mathrm{ord}[f_i(x)]\}.$$

Proposition 7. If $f(x) \in \mathbb{F}_2[x]$ is an irreducible polynomial over $\mathbb{F}_2$, then $\mathrm{ord}[f(x)]$ divides $2^{\deg[f(x)]} - 1$.

Proposition 8. A polynomial $f(x) \in \mathbb{F}_2[x]$ is primitive if and only if $f(0) = 1$, and

$$\mathrm{ord}[f(x)] = 2^{\deg[f(x)]} - 1.$$

For the proofs of these propositions, we refer the reader to Theorems 3.20 and 3.9, Corollary 3.4, and Theorem 3.16 in Ref. [12].

Proof of Theorem 4. By Lemma 3 and the rest of the argument in Sec. II B, we only need to prove that $\mathrm{ord}[f(x)] = \mathrm{lcm}_i\{\mathrm{ord}[f_i(x)]\}$ and that $\mathrm{lcm}_i\{\mathrm{ord}[f_i(x)]\} = n$ if at least one irreducible factor $f_i(x)$ is primitive and of degree m. As mentioned in the proof of Lemma 3, because $h(x)$ is the generator polynomial of a cyclic code of length n, its factor $f(x)$ divides $x^n - 1$. Thus, by Proposition 5, all $f_i(x)$ in the factorization $f(x) = \prod_i f_i(x)$ are distinct. Hence, Proposition 6 proves that the order of our $f(x)$ is indeed the least common multiple of the orders of its irreducible factors $f_i(x)$. Assume that one of the irreducible factors of $f(x)$ is primitive and of degree m. Note that for a pair a, b of positive integers, $2^a - 1$ divides $2^b - 1$ if and only if a divides b. Hence, by Proposition 5 and the fact that $f(x)$ divides $x^n - 1$, for each i the integer $2^{\deg[f_i(x)]} - 1$ divides $2^m - 1 = n$. Because $f(x)$ divides $x^n - 1$, we have $f_i(0) = 1$ for every i. Thus by Propositions 7 and 8, we have

$$\mathrm{lcm}_i\{\mathrm{ord}[f_i(x)]\} = 2^m - 1 = n.$$

This completes the proof. ■

Because $\mathrm{lcm}_i\{\mathrm{ord}[f_i(x)]\}$ is always at least $k_2 - k_1$, Theorem 4 provides better synchronization recovery capabilities than Theorem 1. For instance, when $n = 2^m - 1$ is a prime, m must be a prime as well. In this case, Proposition 5 dictates that for each i the degree $\deg[f_i(x)]$ is either 1 or m. Because $x - 1$ is the only irreducible polynomial of degree 1 with a nonzero constant term, if $\deg[f(x)] \geqslant 2$, we have $\mathrm{ord}[f(x)] = n$, achieving the highest possible synchronization error tolerance.

IV. QUANTUM SYNCHRONIZABLE CODES FROM REED-MULLER CODES

In this section we study two special classes of algebraic codes to give families of quantum synchronizable error-correcting codes. The first class is a type of finite geometry code based on projective geometry, while the other class includes those used in Theorem 2 as a subclass. To make the connection to our quantum synchronizable scheme as clear as possible, we define these classical codes by their generator polynomials with the minimum amount of mathematics. The proofs of the basic facts we use can be found in [10]. For more finite geometric and algebraic views of our cyclic codes, the interested reader is referred to [10,13,14].

For a non-negative integer s and a positive integer 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 $C_{s,n} = C_{s',n}$ if $s' \in C_{s,n}$, we may take a system

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

of representatives of the cyclotomic cosets by picking the smallest element from each set. We call S_n the *canonical* system of representatives. The integers modulo n are partitioned into cyclotomic cosets as

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

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

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

For non-negative integers s, let $\mathrm{w}_2(s)$ denote the number of 1's in the binary expansion of s. For positive integers r, m such that $r < m$, the *punctured Reed-Muller code* $\mathcal{R}(r,m)^*$ of *order* r over projective space $\mathrm{PG}(m-1,2)$ is the cyclic code of parameters

$$\left[2^m - 1, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r} - 1\right]$$

defined by the generator polynomial

$$g(x) = \prod_{\substack{1 \leqslant \mathrm{w}_2(s) \leqslant m-r-1 \\ s \in S_{2^m-1}}} M_s(x).$$

For a comprehensive treatment of punctured Reed-Muller codes, the interested reader is referred to [10]. We use the basic property of $\mathcal{R}(r,m)^*$ that the generator polynomial $g^\perp(x)$ of its dual $\mathcal{R}(r,m)^{*\perp}$ is

$$g^\perp(x) = (x+1) \prod_{\substack{1 \leqslant \mathrm{w}_2(s) \leqslant r \\ s \in S_{2^m-1}}} M_s(x).$$

Punctured Reed-Muller codes are cyclic codes with the desired nested property for our purpose.

Lemma 9. For any positive integers r_1, r_2, and m such that $\lceil \frac{m}{2} \rceil < r_2 < r_1 < m$, the punctured Reed-Muller codes of order r_1 and r_2 over $\mathrm{PG}(m-1,2)$ satisfy the condition that

$$\mathcal{R}(r_2,m)^{*\perp} \subseteq \mathcal{R}(r_2,m)^* \subset \mathcal{R}(r_1,m)^*.$$

Proof. Let $g_1(x)$, $g_2(x)$, and $g_2^\perp(x)$ be the generator polynomials of $\mathcal{R}(r_1,m)^*$, $\mathcal{R}(r_2,m)^*$, and $\mathcal{R}(r_1,m)^{*\perp}$, respectively.

Because these are generators of the corresponding principal ideals of $\mathbb{F}_2[x]$, we only need to show that $g_1(x)$ divides $g_2(x)$ and that $g_2(x)$ divides $g_2^{\perp}(x)$. Because $r_2 < r_1$, we have

$$g_2(x) = g_1(x) \prod_{\substack{m-r_1 \leqslant \mathrm{w}_2(s) \leqslant m-r_2-1 \\ s \in S_{2^m-1}}} M_s(x).$$

Because $\lceil \frac{m}{2} \rceil < r_2 < m$, we have

$$g_2^{\perp}(x) = g_2(x)(x+1) \prod_{\substack{m-r_2 \leqslant \mathrm{w}_2(s) \leqslant r_2 \\ s \in S_{2^m-1}}} M_s(x).$$

The proof is complete. ■

The above lemma allows us to use punctured Reed-Muller codes as the cyclic codes $\mathcal{C}$ and $\mathcal{D}$ in Theorem 4 to obtain a family of quantum synchronizable codes:

Theorem 10. Let r_1, r_2, m, and n be positive integers such that $\lceil \frac{m}{2} \rceil < r_2 < r_1 < m$ and such that $n = 2^m - 1$. For every pair a_l, a_r of non-negative integers such that $a_l + a_r < \mathrm{lcm}_s\{\mathrm{ord}[M_s(x)]\}$, where s runs through all integers in the canonical system S_n of representatives of cyclotomic cosets modulo n satisfying the condition that $m - r_1 \leqslant \mathrm{w}_2(s) \leqslant m - r_2 - 1$, there exists a quantum synchronizable (a_l,a_r)-$[[n + a_l + a_r, 2\sum_{i=0}^{r_2}\binom{m}{i} - n]]$ code that corrects at least up to $2^{m-r_2-1} - 1$ phase errors and at least up to $2^{m-r_1-1} - 1$ bit errors.

Another useful property of punctured Reed-Muller codes is that their ambient spaces contain well-known cyclic codes. Let n be an odd integer and $\alpha \in \mathbb{F}_{2^{|C_{1,n}|}}$ a primitive nth root of unity. A *Bose-Chaudhuri-Hocquenghem* (BCH) *code* of *length* n and *designed distance* d is a cyclic code of length n whose generator polynomial is

$$g(x) = \prod_{i \in \bigcup_{j=0}^{d-2} C_{b+j,n}} (x - \alpha^i),$$

where b is a nonnegative integer. The term designed distance reflects the fact that the true minimum distance of a BCH code is at least its designed distance. The proof of this fact and other basic properties of BCH codes can be found in [10]. A BCH code is *primitive* if the length is of the form $n = 2^m - 1$ for some positive integer m, and *narrow-sense* if $b = 1$.

BCH codes are one of the older classes of cyclic codes and have been extensively studied in classical coding theory. Their dual-containing property and basic parameters have also been investigated in the context of quantum error correction [15,16]. For this reason, they have a great potential as a source of excellent quantum synchronizable codes. In fact, Theorem 2 is a straightforward application of primitive, narrow-sense BCH codes of odd designed distance.

We begin with the following observation.

Lemma 11. Let $\mathcal{B}$ be the primitive, narrow-sense BCH code of length $2^m - 1$ and designed distance $2^{m-r} - 1$, where $\lceil \frac{m}{2} \rceil < r < m - 2$ and $m \geqslant 7$. Then

$$\mathcal{R}(r,m)^{*\perp} \subseteq \mathcal{R}(r,m)^* \subset \mathcal{B}.$$

Proof. Let S be the set of positive integers less than $2^{m-r} - 1$. Then the generator polynomial $g(x)$ of the primitive, narrow-sense BCH code of length $2^m - 1$ and designed distance $2^{m-r} - 1$ is

$$g(x) = \prod_{i \in \bigcup_{j \in S} C_{j,2^m-1}} (x - \alpha^i) = \prod_{s \in S \cap S_{2^m-1}} M_s(x),$$

where S_{2^m-1} is the canonical system of representatives of the cyclotomic cosets modulo $2^m - 1$. For any positive integer $a < 2^{m-r} - 1$, we have $\mathrm{w}_2(a) \leqslant m - r - 1$. Hence, we have

$$S \cap S_{2^m-1} \subseteq \{s \mid s \in S_{2^m-1}, 1 \leqslant \mathrm{w}_2(s) \leqslant m - r - 1\}.$$

Hence, $g(x)$ divides the generator polynomial of $\mathcal{R}(r,m)^*$, which implies that $\mathcal{R}(r,m)^* \subseteq \mathcal{B}$. It is known that $\mathcal{R}(r,m)^* \neq \mathcal{B}$ if $\lceil \frac{m}{2} \rceil < r < m - 2$ and $m \geqslant 7$ (see, for example, [17], Lemma 5.3]). Hence, we have $\mathcal{R}(r,m)^* \subset \mathcal{B}$. By Lemma 9, $\mathcal{R}(r,m)^{*\perp} \subseteq \mathcal{R}(r,m)^*$. The proof is complete. ■

Because BCH codes are cyclic, Lemma 11 states that we may use dual-containing punctured Reed-Muller codes together with primitive, narrow-sense BCH codes to construct quantum synchronizable codes. Note that $\mathcal{C}^{\perp} \subseteq \mathcal{C} \subset \mathcal{D}$ implies that $\mathcal{D}^{\perp} \subset \mathcal{D}$. Since a BCH code is trivially contained in another BCH code of smaller designed distance, we can also construct quantum synchronizable codes from a pair of dual-containing BCH codes without using punctured Reed-Muller codes. The following are two useful known results on primitive, narrow-sense BCH codes that are dual containing:

Theorem 12 ([16]). For $m \geqslant 2$, a primitive, narrow-sense BCH code of length $2^m - 1$ is dual containing if and only if its designed distance d satisfies the condition that $2 \leqslant d \leqslant 2^{\lceil \frac{m}{2} \rceil} - 1$.

Theorem 13 ([16]). A primitive, narrow-sense BCH code of length $2^m - 1$ and designed distance d that is dual containing is of dimension $2^m - 1 - m\lceil \frac{d-1}{2} \rceil$.

By applying Lemmas 9 and 11 and Theorems 12 and 13 to Theorem 4, we can obtain a variety of quantum synchronizable codes. For instance, the following is a special case based on punctured Reed-Muller codes and BCH codes:

Theorem 14. Let n, r, m be positive integers satisfying the conditions that $n = 2^m - 1$ is a prime, that $\lceil \frac{m}{2} \rceil < r < m - 2$, and that $m \geqslant 7$. Then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < n$ there exists a quantum synchronizable (a_l,a_r)-$[[n + a_l + a_r, \sum_{i=0}^{r}\binom{m}{i}]]$ code that corrects at least up to $2^{m-r-1} - 1$ phase errors and at least up to $2^{m-r-1} - 1$ bit errors.

The following lemmas allow us to calculate the synchronization recovery capabilities of quantum synchronizable error-correcting codes based on primitive, narrow-sense BCH codes:

Lemma 15 ([16]). Let n, m be positive integers such that $n = 2^m - 1$. For any positive integer $s \leqslant 2^{\lceil \frac{m}{2} \rceil}$, the cardinality $|C_{s,n}| = m$.

Lemma 16 ([16]). Let n, m be positive integers such that $n = 2^m - 1$. For any odd positive integer $s,s' \leqslant 2^{\lceil \frac{m}{2} \rceil}$, we have $C_{s,n} \neq C_{s',n}$.

Theorem 17. 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 $m \geqslant 5$ and $d_1 - d_2 \geqslant 4$. Then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < n$ there exists a quantum synchronizable

(a_l,a_r)-$[[n+a_l+a_r,n-m(d_2-1)]]$ code that corrects at least up to $\frac{d_1-1}{2}$ phase errors and at least up to $\frac{d_2-1}{2}$ bit errors.

Proof. Apply Theorems 12 and 13 to Theorem 4. By Lemma 16 and the fact that for every positive even integer $s \leqslant d_1$ the cyclotomic coset $C_{s,n} = C_{\frac{s}{2},n}$, the generator polynomials of the primitive, narrow-sense BCH codes of distance d_1 and d_2 are

$$g_1(x) = \prod_{\substack{1 \leqslant s \leqslant d_1 - 1 \\ s \text{ odd}}} M_s(x)$$

and

$$g_2(x) = \prod_{\substack{1 \leqslant s \leqslant d_2 - 1 \\ s \text{ odd}}} M_s(x),$$

respectively. Thus we only need to prove that

$$f(x) = \prod_{\substack{d_2 \leqslant s \leqslant d_1 - 1 \\ s \text{ odd}}} M_s(x)$$

is of order n. By Lemma 15, for $d_2 \leqslant s \leqslant d_1 - 1$ we have $\deg[M_s(x)] = m$. Hence, because $\mathrm{ord}[M_s(x)]$ is the order of α^s in the multiplicative group $\mathbb{F}_{2^m}^*$ (see [12], Theorem 3.33]), we have $\mathrm{ord}[M_s(x)] = \frac{n}{\gcd(s,n)}$. Because we have $d_1 - d_2 \geqslant 4$, the polynomial $f(x)$ has two irreducible factors $M_s(x)$ and $M_{s+2}(x)$ for some odd s. Hence, by Proposition 6, we have

$$\mathrm{ord}[f(x)] \geqslant \mathrm{lcm}\left(\frac{n}{\gcd(s,n)}, \frac{n}{\gcd(s+2,n)}\right) = n$$

as desired. The proof is complete. ∎

Since the parity of the designed distance of each BCH code in Theorem 17 does not affect whether the pair of cyclic codes satisfies the nested property required to construct a quantum synchronizable code, one may also exploit BCH codes of even designed distance to obtain similar quantum synchronizable error-correcting codes, albeit of parameters slightly cumbersome to spell out.

V. CONCLUDING REMARKS

We refined the known general framework for designing quantum synchronizable codes through an algebraic approach. With this refinement, we can compute the best attainable synchronization recovery capabilities a given pair of classical cyclic codes can offer. We also examined the structures of punctured Reed-Muller codes and BCH codes in their ambient spaces to obtain families of quantum synchronizable codes.

While we focused on the case when code lengths are of the form $n = 2^m - 1$, in principle, we can also apply similar techniques to the general case when n is a positive integer. In fact, narrow-sense BCH codes that are not primitive are also known to be dual containing if their designed distances satisfy a condition similar to the one given in Theorem 12 [16]. The exact dimensions can be obtained in the same way as well. Moreover, as we will see here, our result on the maximum tolerable magnitude of misalignment can also be extended in theory to the case of general n.

To generalize our approach through Lemma 3 to the case when n may not be of the form $2^m - 1$, we need to know the order of a given polynomial $f(x)$ which divides $x^n - 1$ but may contain irreducible factors of multiplicity more than one. The following fact is useful for computing the order.

Proposition 18. Let $f(x) \in \mathbb{F}_2[x]$ be irreducible over $\mathbb{F}_2$ with $f(0) = 1$ and $\mathrm{ord}[f(x)] = e$. Let a be a positive integer and define b to be the smallest integer such that $2^b \geqslant a$. Then $\mathrm{ord}[(f(x))^a] = 2^b e$.

The proof of the above proposition can be found in [12], Theorem 3.8.

Because the polynomial of which we need to compute the order divides $x^n - 1$, its irreducible factors $f_i(x)$ all satisfy the condition that $f_i(0) = 1$. Thus, by Propositions 6 and 18, even if n is not a Mersenne number, the maximum tolerable magnitude of misalignment can be computed from the order of each irreducible factor. A table of the orders of irreducible polynomials can be found in [12].

Our block synchronization scheme may be seen as an algebraically modernized quantum analog of the classical schemes introduced in the 1960s, where cosets of cyclic codes played the key role (see, for example, [6,18,19]). The theory of synchronization for classical bits has seen progress since its inception and gave birth to different synchronization techniques. The most recent major progress includes the proof of the existence of capacity-achieving codes in a single-shot model within a finite length regime [20] and explicit constructions for high-rate self-synchronizing codes [21].

A notable property of many newer classical codes for synchronization is that they allow for locating boundaries regardless of the magnitude of misalignment while achieving high information rates. This means that the sender and receiver can establish and maintain efficient communications over noisy channels even if no prior block synchronization is assumed. While such high-level control over quantum information would be extremely challenging both theoretically and experimentally, very recently an initial step from the theoretical side has been made in this direction as well [22]. It would be of interest to look for a way to realize quantum analogs of recent software solutions for synchronization in classical communications.

Another interesting related topic would be the type of synchronization error due not to misalignment but to undetected loss of bits. Such synchronization errors are called *deletions* in classical coding theory (see [23,24] for surveys of results on this and closely related types of synchronization errors). As far as the authors are aware, no result is available on the quantum analog of this channel at the time of writing. While a deletion can be recovered by our method in some cases such as qubit loss at the start of quantum communication, quantum synchronizable codes are not able to treat all types of deletion.

In general, loss of qubits may be treated as *erasures* or *located errors* if there is a hardware solution for detecting such anomalies (see, for example, [25–32]). Hence, errors such as photon loss can be handled by tracing out the lost qubits and then recovering them through quantum error-correcting codes for erasures such as those found in [33]. While this assumption is reasonable in many contexts such as linear optical quantum memories, it may be more reasonable to also consider undetected loss of qubits in other

contexts such as asynchronous free-space optical quantum communication at high rates. We hope that the present work will stimulate research on asynchronous quantum information transmission.

ACKNOWLEDGMENTS

Y.F. acknowledges support from JSPS. Vladimir Tonchev is supported by an NSA grant.

[1] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).

[2] Y. Fujiwara, Phys. Rev. A **87**, 022344 (2013).

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

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

[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[6] R. C. Bose and J. G. Caldwell, Inf. Contr. **10**, 616 (1967).

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

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

[9] Assume that we have a pair $\mathcal{C}$, $\mathcal{D}$ of linear codes such that $\mathcal{C}^{\perp} \subseteq \mathcal{C} \subset \mathcal{D}$. Then, because $\mathcal{C} \subset \mathcal{D}$ if and only if $\mathcal{D}^{\perp} \subset \mathcal{C}^{\perp}$, we have $\mathcal{D}^{\perp} \subset \mathcal{C}^{\perp} \subseteq \mathcal{C} \subset \mathcal{D}$. Hence, we have $\mathcal{D}^{\perp} \subset \mathcal{D}$.

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Publishing Company, Amsterdam, 1977).

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

[12] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed. (Cambridge University Press, Cambridge, 1997).

[13] E. F. Assmus, Jr. and J. D. Key, in *Handbook of Coding Theory*, Vol. II, edited by V. S. Pless and W. C. Huffman (North-Holland, Amsterdam, 1998), Chap. 16, pp. 1269–1344.

[14] P. Charpin, in *Handbook of Coding Theory*, Vol. I, edited by V. S. Pless and W. C. Huffman (North-Holland, Amsterdam, 1998), Chap. 11, pp. 963–1064.

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

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

[17] W. C. Huffman, in *Handbook of Coding Theory*, Vol. II, edited by V. S. Pless and W. C. Huffman (North-Holland, Amsterdam, 1998), Chap. 17, pp. 1345–1440.

[18] J. E. Levy, IEEE Trans. Inf. Theory **12**, 286 (1966).

[19] S. E. Tavares and M. Fukada, IEEE Trans. Inf. Theory **15**, 93 (1969).

[20] Y. Polyanskiy, IEEE Trans. Inf. Theory **59**, 1256 (2013).

[21] Y. Fujiwara and V. D. Tonchev, IEEE Trans. Inf. Theory **59**, 2328 (2013).

[22] Y. Fujiwara, arXiv:1207.1138 [IEEE Trans. Information Theory (to be published)].

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

[24] M. Mitzenmacher, Probability Surveys **6**, 1 (2009).

[25] P. Migdał and K. Banaszek, Phys. Rev. A **84**, 052318 (2011).

[26] M. Lassen, M. Sabuncu, A. Huck, J. Niset, G. Leuchs, N. J. Cerf, and U. L. Andersen, Nat. Photonics **4**, 700 (2010).

[27] J. Niset, U. L. Andersen, and N. J. Cerf, Phys. Rev. Lett. **101**, 130503 (2008).

[28] C.-Y. Lu, W.-B. Gao, J. Zhang, X.-Q. Zhou, T. Yang, and J.-W. Pan, Proc. Natl. Acad. Sci. U.S.A. **105**, 11050 (2008).

[29] W. Wasilewski and K. Banaszek, Phys. Rev. A **75**, 042316 (2007).

[30] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).

[31] J. Vala, K. B. Whaley, and D. S. Weiss, Phys. Rev. A **72**, 052318 (2005).

[32] R. M. Gingrich, P. Kok, H. Lee, F. Vatan, and J. P. Dowling, Phys. Rev. Lett. **91**, 217901 (2003).

[33] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).