On a Family of Quantum Synchronizable Codes Based on the \((\lambda(u + v)|u - v)\) Construction

CHAO DU, ZHI MA, LAN LUO, DAKANG HUANG, AND HONG WANG

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China

Corresponding author: Zhi Ma (ma_zhi@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61972413, Grant 61701539, and Grant 61901525, and in part by the National Cryptography Development Fund under Grant mmjj20180107 and Grant mmjj20180212.

ABSTRACT In this paper, we propose a family of quantum synchronizable codes from repeated-root cyclic codes and constacyclic codes. This family of quantum synchronizable codes are based on \((\lambda(u + v)|u - v)\) construction which is constructed from constacyclic codes. Under this construction, we enrich the varieties of valid quantum synchronizable codes. We also prove that the obtained quantum synchronizable codes can achieve maximum synchronization error tolerance. Furthermore, quantum synchronizable codes based on \((\lambda(u + v)|u - v)\) construction are shown to have a better capability in correcting bit errors than those from projective geometry codes.

INDEX TERMS Repeated-root constacyclic codes, quantum synchronizable codes, \((\lambda(u + v)|u - v)\) construction.

I. INTRODUCTION

In recent years, quantum computation and quantum communication have become a hot topic in communication, physics, and mathematics. Quantum information theory has achieved unprecedented development. Among them, quantum error correction, which focuses on dealing with quantum noise, is a necessary guarantee for the realization of quantum information processing in a noisy environment. Typically, quantum noise is characterized by operators acting on qubits. The most common error model is a linear combination of the Pauli operators \(I, X, Y,\) and \(Z\) operating on each qubit [1]. This typical error model can be regarded as the quantum version of additive noise, which is one of the most important and deeply-studied error models in information theory. Also, misalignment [2] concerning the block structure of a qubit stream is another type of error in quantum information processing. Misalignment is the simplest type of synchronization error, which is different from the additive noise but also crucial.

In classical digital computing and communication, block synchronization (or frame synchronization) is a challenging problem to make sure that the receiver can correctly decode the transmitted information. Classical block synchronization is commonly accomplished by information receiver or processing equipment continuously monitoring data to accurately identify the inserted boundary signals of information blocks [3], [4], or by using synchronized error-correcting codes [5] that can correct both additive noise and misalignment in block synchronization. However, the former way does not apply in the quantum domain because the measurement of qubits usually destroys their contained quantum information. Many scientists have been working on a quantum analog of the latter technique.

Fortunately, Fujiwara [2] proposed a coding system, quantum synchronizable error-correcting codes, which can simultaneously realize synchronization recovery and Pauli error correction. In his scheme, a pair of nested dual-containing cyclic codes are required, both of which promise large minimum distances. After that, Fujiwara et al. [6] improved the known general framework for designing quantum synchronizable codes through a more careful analysis of the algebraic machinery behind synchronization recovery, and gave several families of quantum synchronizable codes based on punctured Reed-Muller codes and their ambient spaces. Subsequently, quantum synchronizable codes were presented from finite geometric codes [5], quadratic residue codes [7] and repeated-root cyclic codes [8]. Furthermore, Luo et al. [9] provided two new ways of constructing quantum synchronizable codes. One is based on the \((u + v)|u - v\) construction from cyclic codes and negacyclic codes, and the other is to exploit
the product construction to produce new cyclic codes from two cyclic codes with coprime lengths. In the former case, the obtained quantum synchronizable codes were shown to be able to provide better performance in correcting Pauli errors than non-primitive, narrow-sense BCH codes [8], [9], and achieve the maximum tolerance against misalignment under certain condition.

In this paper, we expand the results of Luo et al. [9] and propose a family of quantum synchronizable codes based on the \((\lambda(u + v)|u - v)\) construction. This type of quantum synchronizable codes are generated in two steps. First, we exploit constacyclic codes to generate negacyclic codes with twice the lengths. And then, we use the obtained negacyclic codes and cyclic codes satisfying the property of nested dual-containing to generate new cyclic codes. Our quantum synchronizable codes are derived from the final obtained cyclic codes. The \((\lambda(u + v)|u - v)\) construction is deduced from the \((u + v)|u - v)\) construction and appears in negacyclic codes which are generated by constacyclic codes. We also present the circumstance where the obtained synchronizable quantum codes can achieve maximum tolerance against misalignment. In particular, we show that quantum synchronizable codes derived from cyclic codes and constacyclic codes may have a better Pauli performance in correcting bit errors than those from projective geometry codes.

In the next section, we first introduce classical error-correcting codes and the quantum synchronizable coding framework. In Section 3, we propose the general formalism of quantum synchronization codes based on the \((\lambda(u + v)|u - v)\) construction. In Section 4, we use repeated-root cyclic codes and constacyclic codes to construct quantum synchronizable codes presented in Section 3 and prove that the obtained quantum codes can reach the maximum tolerance against misalignment. In Section 5, we discuss the minimum distances of above repeated-root constacyclic codes and give an example of quantum synchronizable codes. Finally, we present a summary of our work in the last section.

II. PRELIMINARIES

Let \(\mathbb{F}_q\) be a finite field with \(q = p^m\) a prime power, where \(p\) is the odd prime characteristic of \(\mathbb{F}_q\) and \(m\) is a positive integer. Denote by \(\mathbb{F}_q^* = \mathbb{F}_q\setminus\{0\}\) the multiplicative group. It is well known that \(\mathbb{F}_q^*\) is a cyclic group of order \(q - 1\). Let \(\xi\) be a primitive \((q - 1)\)-th root of unity in \(\mathbb{F}_q^*\), then

\[\mathbb{F}_q^{pm} = \{0, \xi, \ldots, \xi^{pm-2}, \xi^{pm-1} = 1\}.\]

For any element \(\alpha \in \mathbb{F}_q^*\), we define \(\text{ord}_q(\alpha)\) as order in the multiplicative group \(\mathbb{F}_q^*\).

A classical linear \([n, k, d]\) code \(C\) over \(\mathbb{F}_q\) of length \(n\) and minimum Hamming distance \(d\) is a \(k\)-dimensional vector subspace of \(\mathbb{F}_q^n\), where \(d = \min\{\text{wt}(c) | c \neq 0, c \in C\}\) and \(\text{wt}(c)\) is the number of nonzero coordinates of a codeword \(c\). The code \(C\) can be determined by an \((n - k) \times n\) parity-check matrix \(H\), i.e., \(C = \{c \in \mathbb{F}_q^n | Hc^T = 0\}\). Accordingly, there exists a \(k \times n\) generator matrix \(G\) satisfying \(HG^T = 0\). The dual code \(C^\perp = \{c' \in \mathbb{F}_q^n | c' \cdot c^T = 0, \forall c \in C\}\) of \(C\) is an \([n, n - k]\) linear code with a parity-check matrix \(G\) and a generator matrix \(H\). We call that \(C\) is a self-dual code if and only if \(C = C^\perp\). Besides, \(C\) is said to be a self-orthogonal code if \(C \subset C^\perp\) and a dual-containing code if \(C^\perp \subset C\).

Let \(\lambda\) be a nonzero element of \(\mathbb{F}_q\). Given an \(n\)-tuple \(c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n\), define a \(\lambda\)-constacyclic shift \(\tau_{\lambda}(c_0, c_1, \ldots, c_{n-1}) = (\xi^\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2})\).

A code \(C\) is \(\lambda\)-constacyclic if \(\tau_{\lambda}(C) = C\). And a \(\lambda\)-constacyclic code \(C\) is said to be a cyclic code if \(\lambda = 1\) and a negacyclic code if \(\lambda = -1\). Any \(\lambda\)-constacyclic code \(C\) of length \(n\) over \(\mathbb{F}_q\) can be identified as exactly one ideal in the quotient ring \(\mathbb{F}_q[x]/(x^n - \lambda)\), which is generated by a monic polynomial \(g(x)\) of \(x^n - \lambda\). We call the monic polynomial \(g(x)\) of degree \(n - k\) as the generator polynomial of \(C\) and denote by \(C = \langle g(x) \rangle\). Let \(h(x) = \frac{x^n - \lambda}{g(x)}\). Then the dual code \(C^\perp\) of \(C\) is a \(\lambda\)-negacyclic code and has a generator polynomial \(h^*(x)\), where \(h^*(x) = h(0)^{-1}x^{\deg h}(x)h(x^{-1})\) is the reciprocal polynomial of \(h(x)\).

An \([n, k, d]\) quantum error-correcting code \(Q\) is a \(d^2\)-dimensional subspace of a \(d^2\)-dimensional Hilbert space \((\mathbb{C}^d)^\otimes n\), and can correct bit errors and phase errors caused by Pauli operators of weight less than \(\left\lfloor \frac{d - 1}{2} \right\rfloor\). For an \((a_1, a_2) = [n, k]\) quantum synchronizable code, it can correct not only Pauli errors, but block misalignment to the left by at most \(a_1\) qubits and to the right by at most \(a_2\) qubits for a pair of nonnegative integers \((a_1, a_2)\). Luo et al. [9] exploited the well-known \((u + v)|u - v)\) construction on cyclic codes and negacyclic codes to get new cyclic codes with twice the lengths. Then they provided a new way in regard to generating quantum synchronizable code. Let \(f(x)\) be a polynomial over \(\mathbb{F}_q\) with \(f(0) \neq 0\). Denote by \(\text{ord}(f(x)) = |\{x^d \mod f(x) | a \in \mathbb{N}\}|\) the order of the polynomial \(f(x)\). The main result is given as following.

Theorem 1 [9]: \(C_1 = \langle g(x) \rangle\) be an \([n, k, d]\) dual-containing code for \(i \in \{1, 2, 3, 4\}\). Suppose that \(C_1, C_2\) are cyclic codes with \(C_1 \subset C_2\) and \(C_3, C_4\) are negacyclic codes with \(C_3 \subset C_4\). Define the polynomial \(f(x)\) to be the quotient of \(g(x)g_3(x)\) divided by \(g_2(x)g_4(x)\). Then for any pair of nonnegative integers \(a_1, a_2\), such that \(a_1 + a_2 < \text{ord}(f(x))\), there exists an \((a_1, a_2) = [2n + a_1 + a_2, 2(k_1 + k_3) - n]\) quantum synchronizable code that can correct up to \(\min\{2d_2, 2d_4, \max\{d_2, d_4\} - 1\}\) bit errors and \(\min\{2d_2, 2d_4, \max\{d_2, d_4\} - 1\}\) phase errors.

Theorem 1 needs a pair of dual-containing cyclic codes \(C_1, C_2\) and a pair of dual-containing negacyclic codes \(C_3, C_4\) to generate a family of quantum synchronizable code. The obtained quantum synchronizable code can achieve the maximum tolerance against misalignment when \(\text{ord}(f(x)) = 2n\). Besides, these quantum codes have a better capability in correcting Pauli errors because cyclic codes on \((u + v)|u - v)\) construction have minimum distances no worse
III. THE $(\lambda(u+v)|u-v)$ CONSTRUCTION

In this section, we discuss the quantum synchronizable codes based on the $(\lambda(u+v)|u-v)$ construction. Under this construction, we are able to obtain new negacyclic codes with twice the lengths from the component constacyclic codes. It is required that $x^{2n}+1=(x^\lambda-\lambda_1)(x^\lambda-\lambda_2)$ since we use an $n$-length $\lambda_1$-constacyclic code and an $n$-length $\lambda_2$ constacyclic code to generate a $2n$-length negacyclic code. Therefore, the conditions that $\lambda_1^2+1=0$ and $\lambda_2=-\lambda_1$ need to be met. Some important results about the $(\lambda(u+v)|u-v)$ construction are given in the following theorem.

Theorem 2: Let $C_1$ and $C_2$ be $[n, k_1]$ and $[n, k_2]$ constacyclic code over $\mathbb{F}_q$. Denote by $G_1$, $G_2$ and $H_1$, $H_2$ the generator matrices and parity-check matrices of $C_1$ and $C_2$ respectively. And $g_1(x)$, $g_2(x)$ are the generator polynomials of $C_1$ and $C_2$ respectively, where $g_1(x)|x^n-\lambda_1$, $g_2(x)|x^n-\lambda_2$ and $\lambda_2=-\lambda_1$, $\lambda_1^2+1=0$. Let $\lambda=\lambda_1$. Then the $(\lambda(u+v)|u-v)$ construction $C=C_1 \cap C_2=\{(u+v)|u-v)|u \in C_1, v \in C_2\}$ is a $[2n, k_1+k_2, \min\{2d_1, 2d_2, \max\{d_1, d_2\}\}]$ negacyclic code with a generator matrix

$$G=\begin{pmatrix} -\lambda_2G_1 & G_1 \\ \lambda_1G_2 & -G_2 \end{pmatrix}, \tag{1}$$

and a generator polynomial $g(x)=g_1(x)g_2(x)$. The dual code $C^\perp$ is a $(\lambda(u+v)|u-v)$ construction of $C_1^\perp$ and $C_2^\perp$, i.e., $C^\perp=(C_1 \cap C_2)^\perp=C_1^\perp \cap C_2^\perp$ with the generator matrix

$$H=\begin{pmatrix} -\lambda_2^{-1}H_1 & H_1 \\ \lambda_1^{-1}H_2 & -H_2 \end{pmatrix}. \tag{2}$$

Proof: It is easily known that $C_1 \cap C_2$ is the row space of $G$, and $G$ has rank $k_1+k_2$. So $C_1 \cap C_2$ is a negacyclic code. Assume that $C_1 \cap C_2$ has a generator polynomial $g(x)|x^n+1$. Since $g$ is a codeword, $g$ can be written as

$$g(x)=-\lambda_2ag_1+\lambda_1bg_2+x^\lambda(a_1g_1-bg_2) =\lambda_2g_1+bg_2+x^\lambda(a_1-bg_2) \tag{3}$$

for some polynomials $a,b$. The equality (3) can be rewritten as $g(x)=ag_1(x^\lambda-\lambda_2)-bg_2(x^\lambda-\lambda_1)$. Due to $g_1(x)|x^\lambda-\lambda_1$ and $g_2(x)|x^\lambda-\lambda_2$, we get $g_1(x)g_2(x)|g(x)$. Finally, we have

$$\deg(g(x))=2n-k_1-k_2=\deg(g_1(x))g_2(x).$$

So $g(x)=g_1(x)g_2(x)$. Suppose that $u \in C_1, v \in C_2$ are different codewords. If $u \neq 0$, then $wt(\lambda(u+v), u-v) \geq wt(u) \geq d_1$. And if $u=0$, then $wt(\lambda(v), v)=0$. As a result, the code $C=C_1 \cap C_2$ based on the $(\lambda(u+v)|u-v)$ construction has the minimum distance $d=\min\{2d_1, 2d_2, \max(d_1, d_2)\}$. The properties of the dual code $C^\perp$ can be obtained by using the same method.

Remark: Consider the cyclic group $\mathbb{F}_q^\times=\langle \xi \rangle$ of order $q-1$, where $\xi$ is a primitive $(q-1)$-th root of unity in $\mathbb{F}_q$, we can easily know that $x^{2n}+1=(x^n-\xi^{\frac{q-1}{2}})(x^n+\xi^{\frac{q-1}{2}})$. That is to say, two constacyclic codes which can generate a negacyclic code are $\xi^{\frac{q-1}{2}}$-constacyclic code and $-\xi^{\frac{q-1}{2}}$-constacyclic code respectively. Note that there exists an element $\lambda \in \mathbb{F}_q^\times$ such that $\lambda=\xi^{\frac{q-1}{2}}$ if and only if $p \equiv 1 \mod 4$ (any $m$) or $p \equiv 3 \mod 4$ (any $m$ is even).

Throughout this paper, we assume that $p \equiv 1 \mod 4$ (any $m$) or $p \equiv 3 \mod 4$ (any $m$) is even. Following Theorem 2, we can now give the construction method of quantum synchronizable code based on $(\lambda(u+v)|u-v)$ construction as follows.

Theorem 3: Let $C_i=\langle g_i(x) \rangle$ be a $[2n, k_i, d_i]$ dual-containing cyclic code for $i \in \{1, 2\}$. Let $C_0=\langle g(x) \rangle$ be an $[n, k_i, d_i]$ constacyclic code for $j \in \{5, 6, 7, 8\}$. $C_5=\langle g(x) \rangle$ and $C_7=\langle g(x) \rangle$ are $\lambda$-constacyclic codes of length $n$. $C_6=\langle g_6(x) \rangle$ and $C_8=\langle g_8(x) \rangle$ are $-\lambda$-constacyclic codes of length $n$. Suppose that $C_1 \subset C_2 \subset C_3 \subset C_7 \subset C_8$. Then $C_3=C_5 \cap C_6 \subset C_7 \cap C_8$ are negacyclic codes satisfying $C_3 \subset C_4$. Denote by $d_3$, $d_4$ the minimum distances of $C_3$, $C_4$ and $k_2$, $k_4$ the dimensions of $C_3$, $C_4$ respectively. Define the polynomial $f(x)=\frac{g_1(x)g_6(x)}{g_2(x)g_7(x)}$. Then for any pair of nonnegative integers $a_1, a_2$ such that $a_1+a_2<\text{ord}(f(x))$, there exists an $(a_1, a_2)-[(4n+a_1+a_2, 2(k_1+k_2+k_6-2n)\] quantum synchronizable code that can correct up to $\min\{2d_2, 2d_3, \max\{d_2, d_3\}\}$ bit errors and $\min\{2d_1, 2d_3, \max\{d_1, d_3\}\}$ phase errors, where $d_3=\min\{2d_2, 2d_6, \max\{d_5, d_6\}\}$ and $d_4=\min\{2d_7, 2d_8, \max\{d_7, d_8\}\}$.

Proof: From Theorem 2 we can get the result that $C_3=C_5 \cap C_6=\langle g_6(x)g_6(x) \rangle$ is a $[2n, k_5+k_6, d_5]$ negacyclic code with $d_3=\min\{2d_2, 2d_6, \max\{d_5, d_6\}\}$ and $C_4=C_7 \cap C_8=\langle g_7(x)g_8(x) \rangle$ is a $[2n, k_7+k_8, d_4]$ with $d_4=\min\{2d_7, 2d_8, \max\{d_7, d_8\}\}$. It is clear that $C_3 \subset C_4$ because of $C_3 \subset C_7$ and $C_4 \subset C_8$. Then we can get the desired quantum synchronizable codes by applying $C_1, C_2, C_3, C_4$ to Theorem 1.

IV. THE USE OF REPEATED-ROOT CONSTACYCLIC CODE OVER $\mathbb{F}_q$

In this section, we exploit repeated-root constacyclic codes and cyclic codes over $\mathbb{F}_q$ to construct quantum synchronizable codes. In particular, the maximum tolerance against misalignment of the obtained quantum synchronizable code is $4n$ because the maximum value of $\text{ord}(f(x))$ is $4n$. Let $f(x)=\frac{g_1(x)g_6(x)}{g_2(x)g_7(x)}$ in Theorem 3. The way of achieving the maximum tolerance against misalignment is to make $\text{ord}(\frac{g_1(x)}{g_2(x)})=4n$ or $\text{ord}(\frac{g_6(x)}{g_7(x)})=4n$ whatever the value of $\text{ord}(\frac{g_1(x)}{g_2(x)})$ is.

A. THE USE OF REPEATED-ROOT CONSTACYCLIC CODES OF LENGTH $p^s$ OVER $\mathbb{F}_q$

We first consider the easy case of constacyclic codes of length $p^s$. Firstly we have $x^{2p^n}+1=(x^{p^n}-\lambda)(x^{p^n}+\lambda)$ with $\lambda=\xi^{p^n-1} \in \mathbb{F}_{p^n}$. $\lambda$ is a nonzero element of the field $\mathbb{F}_{p^n}$, so $\lambda^{-p^n}=\lambda^{-1}$. By the division algorithm, there exist nonnegative integers $r_1, r_2$ such that $s=r_1m+r_2$ and $0 \leq r_2 < m-1$. Then $\lambda_0=-\lambda^{-p^{r_1+1}m-r_2}=-\lambda^{-p^{r_2}}$. Then
\[ \lambda_0 p^r = -\lambda^{-1} p^{r+1} \lambda_0 = -\lambda^{-1} \text{.} \] The following lemma gives the generator polynomial of \( \lambda \)-constacyclic code of length \( p^r \).

**Lemma 1** [11]: Suppose that \( C = \langle \lambda(x) \rangle \subset \mathbb{F}_p[x] \) is a \( \lambda \)-constacyclic code of length \( p^r \). There exists a nonzero element \( \lambda_0 \in \mathbb{F}_p^* \) such that \( \lambda_0 p^r = -\lambda^{-1} \). Then the code \( C \) is precisely the ideal \( \langle (\lambda_0 x + 1)^{\lambda} \rangle \subset \mathbb{F}_p[x] \) where \( 0 \leq i \leq p^r \).

Applying Lemma 1 to Theorem 3, we can construct quantum synchronized codes from constacyclic codes of length \( p^r \).

**Theorem 4:** Let \( C_r = \langle (x - 1)^{p^r-1}(x + 1)^{p^r-1} \rangle \) be a cyclic code of length \( 2p^r \) with \( e_1, 1 \leq e_2, 1, e_2, 2 \leq e_2, 2, \) \( 0 \leq e, 1, e, 2 \leq p^r, \) and \( r \in \{1, 2\} \). Furthermore, \( \mathbb{C}_r = \langle (\lambda_0 x + 1)^{p^r-i} \rangle \) and \( \mathbb{C}_r = \langle (\lambda_0 x + 1)^{p^r-i} \rangle \) are \( \lambda \)-constacyclic code and \( \lambda \)-constacyclic code of length \( p^r \) respectively with \( 0 \leq e, 1, e, 2 \leq p^r \) for \( i \in \{5, 7\} \) and \( j \in \{6, 8\} \), where \( \lambda = \lambda^{\pm 1} \) and \( \lambda_0 p^r = -\lambda^{-1} \). Assume that \( e_5 \leq e_7 \) and \( e_6 \leq e_8 \). If \( e_7 - e_5 \geq p^r-1 \) or \( e_8 - e_6 \geq p^r-1 \), then for any pair of nonnegative integers \( a, d \) such that \( a + d < 4p^r \), we can construct an \( (a, d, d - 1)^p \lambda^{-1} \) quantum synchronized code where \( k = 2(e_1, 1 + e_1, 2 + e_5 + e_6 - 2p^r) \).

**Proof:** \( C_r \) is a dual containing code since the condition \( 0 \leq e, 1, e, 2 \leq p^r \) for \( r \in \{1, 2\} \). By Lemma 1, \( \lambda \)-constacyclic code \( C_r \) has a generator polynomial as follows:

\[ g_{1}(x) = (\lambda_0 x + 1)^{p^r-i}, \quad i \in \{5, 7\} \]

with \( \lambda_0 p^r = -\lambda^{-1} \). Due to \( \lambda^{-1} = -\lambda \), we can get \( -\lambda -1 \)-constacyclic code \( C_r \) has a generator polynomial as follows:

\[ g_{2}(x) = (-\lambda_0 x + 1)^{p^r-1}, \quad j \in \{6, 8\} \]

It is clear that \( C_3 = C_5 \subset C_6 \) and \( C_4 = C_7 \subset C_8 \) are negacyclic codes. Furthermore, the fact that \( C_1 \subset C_2 \) and \( C_3 \subset C_4 \) is obvious due to the assumption that \( e_1, 1 \leq e_2, 1, e_1, 2 \leq e_2, 2, \) and \( e_5 \leq e_7, e_6 \leq e_8 \). If \( e_7 - e_5 \geq p^r-1 \) or \( e_8 - e_6 \geq p^r-1 \), then the order of the polynomial

\[ f(x) = g_{1}(x)g_{2}(x)g_{3}(x)g_{4}(x) = (x - 1)^{p^r-\lambda\xi-1}(x + 1)^{p^r-\lambda\xi-1} \]

is \( 4p^r \). By applying above properties to Theorem 3, we can naturally complete the proof of Theorem 4.

**B. The Use of Repeated-Root Constacyclic Codes of Length \( lp^s \) Over \( \mathbb{F}_q \)**

Now we investigate constacyclic codes of length \( lp^s \) as the component codes in Theorem 4, where \( l, p \) are distinct primes (the case \( l = 2 \) will be discussed later), \( q = p^n \) and \( m, s \geq 1 \) are positive integers.

For any integer \( t \), denote by \( C_t \) the \( q \)-cyclic coset of \( t \) modulo \( l \) over \( \mathbb{F}_q^* \) by \( C_t = \{ t \cdot q^j (\mod l) \} | j = 0, 1, \ldots \) \]. Let \( y \) be a primitive \( l \)-th root of unity in the extension field \( \mathbb{F}_q^* \), where \( w = \text{ord}(q) \) indicates the order of \( q \) in \( \mathbb{Z}_q^* \).

Let \( e = \frac{l-1}{w} \). Then the following equality gives the irreducible factorization of \( x^{p^r} - 1 \) in \( \mathbb{F}_q \):

\[ x^{p^r} - 1 = (x^j - 1)^{p^r} = \prod_{i=0}^{e} M_i(x)^{p^r} \quad (5) \]

where \( M_i(x) = \prod_{i} (x - j^t) \) is the minimal polynomial of \( y^t \) over \( \mathbb{F}_q \) for \( 0 \leq t \leq e \). Denote by \( M_i(x) \) the monic polynomial of \( M_i(x) \) dividing its leading coefficient. The following lemma gives the generator polynomials of \( \lambda \)-constacyclic codes of length \( lp^s \).

**Lemma 2** [12]: Suppose that \( C = \langle \lambda(x) \rangle \subset \mathbb{F}_p[x] \) is a \( \lambda \)-constacyclic code of length \( lp^s \). Let \( w = \text{ord}(q) \).

(I): If \( \gcd(l, q - 1) = 1 \), then there exists a unique element \( a \in \mathbb{F}_q^* \) such that \( d^{\lambda} \lambda = 1 \). And we have the generator polynomial of \( C \) as follows:

\[ g(x) = \prod_{i=0}^{e} M_i(ax)^{p^r} \quad (6) \]

Especially, if \( w \) is odd, the generator polynomial of \( C \) can be written as

\[ g(x) = (x - a^{-1}(p^r - 1))^{e_1} \prod_{i=0}^{e} M_i(ax)^{p^r} \quad (7) \]

where \( 0 \leq e_1, e_r \leq p^r \) for \( 0 \leq t \leq \frac{e_1}{e} \).

(II): If \( \gcd(l, q - 1) = l \), let \( \xi \in \mathbb{F}_q \) be a primitive \( l \)-th root of unity in \( \mathbb{F}_q^* \). One of the following two cases holds:

(i): \( \lambda \notin (\xi^{1})^l \). Then there exists a unique element \( b \in \mathbb{F}_q^* \) such that \( b^{\lambda} \lambda = 1 \), and the generator polynomial of \( C \) is

\[ g(x) = (x - b^{-1} \xi^{1} \xi^{p^r - e}) \prod_{i=1}^{e} (x - b^{-1} \xi^{1} \xi^{p^r - e}) \quad (8) \]

where \( 0 \leq e_1, e_r \leq p^r \) for \( 0 \leq t \leq \frac{e_1}{e} \).

(ii): \( \lambda \notin (\xi^{1})^l \). A unique integer \( j \) with \( 1 \leq j \leq l - 1 \) and an element \( d \in \mathbb{F}_q^* \) can be found such that \( d^{\lambda} \lambda = \xi^{j} \). Then the generator polynomial of \( C \) is

\[ g(x) = (x - d^{-1} \xi^{1} \xi^{p^r - e}) \quad 0 \leq e \leq p^r \quad (9) \]

Applying Lemma 2 to Theorem 4, we can easily obtain a family of quantum synchronized codes that possess the maximum tolerance against misalignment.

**Theorem 5:** Let \( l \) be an odd prime satisfying \( \gcd(l, q - 1) = 1 \). Assume that \( C_1 = \langle g_1(x) \rangle, C_2 = \langle g_2(x) \rangle \) are cyclic codes of length \( 2lp^s \). \( C_3 = \langle g_3(x) \rangle, C_4 = \langle g_4(x) \rangle \) are \( \lambda \)-constacyclic codes of length \( lp^s \). \( C_5 = \langle g_5(x) \rangle \) are \( \lambda \)-constacyclic codes of length \( lp^s \). There exists a unique element \( a \in \mathbb{F}_q^* \) such that \( d^{\lambda} \lambda = 1 \), where \( \lambda = \xi^{\frac{p^r - 1}{l}} \). Let \( w = \text{ord}(q) \).

(I): If \( w \) is even, then the generator polynomial of cyclic code \( C_r \) for \( r \in \{1, 2\} \) is

\[ g_r(x) = \prod_{i=0}^{e} M_i(x)^{p^{r-1}} \quad \text{for} \quad r \in \{1, 2\} \quad (10) \]
with $\ell^e \leq e_{x,t} \leq p^t$ for $0 \leq t \leq e$. Furthermore, constacyclic codes $C_i, C_j$ for $i \in \{5, 7\}$ and $j \in \{6, 8\}$ have generator polynomials
\[
g_i(x) = \prod_{t=0}^{e} \hat{M}_i(ax)^{p^t-e_{x,t}}, \quad i \in \{5, 7\},
\]
\[
g_j(x) = \prod_{t=0}^{e} \hat{M}_j(-ax)^{p^t-e_{j,t}}, \quad j \in \{6, 8\},
\]
respectively with $\ell^e \leq e_{x,t} \leq e_{j,t} \leq p^t$ for $0 \leq t \leq e$. Assume that
\[
e_{x,t} \leq e_{2,t}, \quad \delta_{1,t} \leq \delta_{2,t},
\]
\[
e_{5,t} \leq e_{7,t}, \quad e_{6,t} \leq e_{8,t},
\]
for $0 \leq t \leq e$. If there exists an integer $v$ in the range $0 \leq v \leq e$ such that $e_{7,v} - e_{5,v} > p^t - 1$ or $e_{8,v} - e_{6,v} > p^t - 1$, then for any pair of nonnegative integers $a_1, a_2$ such that $a_1 + a_2 < 4lp^t$, we can construct an $(a_1, a_2) - [[4lp^t + a_1 + a_2, k]]$ quantum synchronizable code where
\[
k = 2(\sum_{\ell^e \leq t \leq e} (e_{1,t} + \delta_{1,t} + \delta_{1,-t} + \delta_{1,t} + e_{5,t})
\]
\[+ (e_{1,0} + \delta_{1,0} + e_{5,0} + e_{6,0})] - 2lp^t). \quad (16)
\]
Proof: Assume $w$ is even. We have the factorization
\[
\chi^{2lp^t} - 1 = (x^{2l} - 1)^{p^t} = \prod_{t=0}^{e} \hat{M}_i(ax)^{p^t-e_{x,t}+1}, \quad i \in \{5, 6\},
\]
with a unique element $a \in F_q^*$ such that $a^{lp^t} \cdot (\lambda) = 1$, where $\ell^e \leq e_{x,t} \leq p^t$ for $0 \leq t \leq e$. In a similar way, we can know that $-\lambda$-constacyclic code $C_i$ has a generator polynomial as follows
\[
g_j(x) = \prod_{t=0}^{e} \hat{M}_j(-ax)^{p^t-e_{j,t}}, \quad j \in \{6, 8\},
\]
with a unique element $-a \in F_q^*$ such that $(-a)^{lp^t} \cdot (\lambda) = 1$, where $\ell^e \leq e_{j,t} \leq p^t$ for $0 \leq t \leq e$. According to the assumption (12), we get $C_1 \subset C_2$ and $C \subset D$. Next we prove the order of $f(x)$ in Theorem 3 is $4n$. Under the assumptions, the polynomial $f(x)$ is
\[
f(x) = g_1(x)g_5(x)g_3(x)
\]
\[g_2(x)g_7(x)g_8(x)
\]
\[= \prod_{t=0}^{e} \hat{M}_i(ax)^{p^t-e_{x,t}}\hat{M}_i(-ax)^{p^t-e_{x,t}}, \quad i \in \{5, 7\},
\]
\[\prod_{t=0}^{e} \hat{M}_j(-ax)^{p^t-e_{j,t}}, \quad j \in \{6, 8\},
\]
respectively with $\ell^e \leq e_{x,t} \leq e_{j,t} \leq p^t$, $p^t \leq e_{1,t} + e_{1,-t} + e_{1,t} + e_{1,-t} \leq 2p^t$ for $1 \leq t \leq \ell^e$, where $d^{lp^t} \lambda = 1$. Assume that
\[
e_{1,0} \leq e_{2,0}, \quad e_{1,0} \leq e_{2,0}, \quad e_{1,-t} \leq e_{2,-t}, \quad e_{5,0} \leq e_{7,0},
\]
\[e_{5,t} \leq e_{7,t}, \quad e_{6,t} \leq e_{8,t}, \quad \delta_{1,0} \leq \delta_{2,0}, \quad \delta_{1,-t} \leq \delta_{2,t},
\]
\[\delta_{1,-t} \leq \delta_{2,-t}, \quad e_{5,t} \leq e_{6,t} \leq e_{8,t}, \quad e_{5,-t} \leq e_{7,-t} \leq e_{8,-t},
\]
for $1 \leq t \leq \ell^e$. If there exists an integer $v$ in the range $-\ell^e \leq v \leq \ell^e$ such that $e_{7,v} - e_{5,v} > p^{t-1}$ or $e_{8,v} - e_{6,v} > p^{t-1}$, then for any pair of nonnegative integers $a_1, a_2$ such that $a_1 + a_2 < 4lp^t$, we can construct an $(a_1, a_2) - [[4lp^t + a_1 + a_2, k]]$ quantum synchronizable code where
\[
k = 2(\sum_{\ell^e \leq t \leq e} (e_{1,t} + \delta_{1,t} + \delta_{1,-t} + \delta_{1,t} + e_{5,t})
\]
\[+ (e_{1,0} + \delta_{1,0} + e_{5,0} + e_{6,0})] - 2lp^t). \quad (16)
\]
Pick an integer \( v \) in the range \( 0 \leq v \leq e \) satisfying \( \varepsilon_7, v > \varepsilon_5, v > p^{i-1} \) or \( \varepsilon_8, v = \varepsilon_6, v > p^{i-1} \), then \( \text{ord}(f(x)) \) has a factor \( p^i \cdot \text{ord}(\tilde{M}_e(ax)) \). It is easily known that \( \text{ord}(\tilde{M}_e(ax)) = 4l \). We have \( \text{ord}(f(x)) \geq 4lp^t \). There is also \( \text{ord}(f(x)) \leq 4lp^t \), so we get \( \text{ord}(f(x)) = 4lp^t \). Finally, \( C \) has dimension

\[
k_r = 2lp^t - \left( \sum_{i=1}^{e} (p^s - \varepsilon_{i,r} + p^s - \delta_{r,t})w \right) + (p^s - \varepsilon_{i,r,0} + p^s - \delta_{r,t,0}) = \sum_{i=1}^{e} (\varepsilon_{i,r} + \delta_{r,t})w + (\varepsilon_{i,r,0} + \delta_{r,t,0}).
\]

Similarly, \( C \) and \( D \) have dimensions

\[
k_C = \sum_{i=1}^{e} (\varepsilon_{5,i} + \varepsilon_{6,i})w + (\varepsilon_{5,0} + \varepsilon_{6,0}),
\]

\[
k_D = \sum_{i=1}^{e} (\varepsilon_{7,i} + \varepsilon_{8,i})w + (\varepsilon_{7,0} + \varepsilon_{8,0}),
\]

respectively. Applying the above discussion to Theorem 3, we can build the quantum synchronizable code with the desired parameters. For the case that \( w \) is odd, we can get the statement in (II) by taking similar argument of the case that \( w \) is even.

Theorem 6: Let \( l \) be an odd prime satisfying \( \text{gcd}(l, q - 1) = l \). Assume that \( g_1(x), g_2(x) \) are cyclic codes of length \( 2lp^t \). \( C \) is a cyclic code of length \( l \). Let \( \lambda \) be a \( \lambda \)-constacyclic codes of length \( lp^t \) with \( \lambda = \xi^{\frac{p-1}{2}} \). \( C_6, C_8 \) are \( -\lambda \)-constacyclic codes of length \( lp^t \). Then cyclic code \( C \) has a generator polynomial

\[
g_{r_1}(x) = (x - 1)^{p^s - \varepsilon_{1,0}} \prod_{i=1}^{l-1} (x - \xi^i)^{p^s - \varepsilon_{2,i}},
\]

\[
g_{r_2}(x) = (x + 1)^{p^s - \delta_{0,0}} \prod_{i=1}^{l-1} (x + \xi^i)^{p^s - \delta_{1,i}},
\]

respectively with \( \frac{\ell}{r} \leq \varepsilon_{1,0}, \varepsilon_{2,0} \leq p^t, \frac{\ell}{r} \leq \delta_{0,0}, \delta_{1,0} \leq p^t, p^t \leq \varepsilon_{1,0,1} + \varepsilon_{2,0,1} + \varepsilon_{2,1,1} + \delta_{0,0,1} = 2p^t \). Furthermore, \( \lambda \)-constacyclic codes \( C_i, C_j \) for \( i \in \{5, 7\} \) and \( j \in \{6, 8\} \) have generator polynomials

\[
g_i(x) = (x - b^{-1} \xi^i)^{p^s - \varepsilon_{i,0}} \prod_{i=1}^{l-1} (x - b^{-1} \xi^i)^{p^s - \varepsilon_{i,1}},
\]

\[
\times (x - b^{-1} \xi^i)^{p^s - \varepsilon_{i,1}}, \quad i \in \{5, 7\},
\]

\[
g_j(x) = (x + b^{-1} \xi^i)^{p^s - \varepsilon_{j,0}} \prod_{i=1}^{l-1} (x + b^{-1} \xi^i)^{p^s - \varepsilon_{j,1}},
\]

\[
\times (x + b^{-1} \xi^i)^{p^s - \varepsilon_{j,1}}, \quad j \in \{6, 8\},
\]

with \( \frac{\ell}{r} \leq \varepsilon_{1,0}, \varepsilon_{2,0} \leq p^t, \frac{\ell}{r} \leq \delta_{0,0}, \delta_{1,0} \leq p^t, p^t \leq \varepsilon_{1,0,1} + \varepsilon_{2,0,1} + \varepsilon_{2,1,1} + \delta_{0,0,1} = 2p^t \). Furthermore, \( \lambda \)-constacyclic codes \( C_i, C_j \) for \( i \in \{5, 7\} \) and \( j \in \{6, 8\} \) have generator polynomials

\[
g_i(x) = (x - 1)^{p^s - \varepsilon_{1,0}} (x + 1)^{p^s - \varepsilon_{2,0}} (x - \lambda)^{p^s - \varepsilon_{2,1}}
\]

\[
\times (x + \lambda)^{p^s - \varepsilon_{2,1}}, \quad i \in \{5, 7\},
\]

\[
g_j(x) = (x - 1)^{p^s - \varepsilon_{1,0}} (x + 1)^{p^s - \varepsilon_{2,0}} (x - \lambda)^{p^s - \varepsilon_{2,1}}
\]

\[
\times (x + \lambda)^{p^s - \varepsilon_{2,1}}, \quad j \in \{6, 8\}.
\]

Proof: Note that \( \frac{\ell}{r} \) is even, so \( \lambda = \xi^{\frac{p-1}{2}} \). Then taking arguments similar to the proof of Theorem 5, we can get the results in Theorem 6.

Now we consider the case of \( l = 2 \). Similarly, there exists a polynomial reduction \( x^{p^t} + 1 = (x^{p^t} - \lambda)(x^{p^t} + \lambda) \) with \( \lambda = \xi^{\frac{p-1}{2}} \). Dinh [13] has discussed the generator polynomial of constacyclic codes of length \( 2lp^t \). Divide the elements of \( \mathbb{F}_q \) into two disjoint subsets \( A_{odd} \cup A_{even} \), where

\[
A_{odd} = \{ \xi^n | 1 \leq i \leq p^t - 1, \ i \text{ is odd} \},
\]

and

\[
A_{even} = \{ \xi^n | 1 \leq i \leq p^t - 1, \ i \text{ is even} \}.
\]

Obviously, \( \{0\}, A_{odd} \) and \( A_{even} \) are disjoint sets. \( 2p^t \)-length \( \lambda \)-constacyclic codes can be described clearly as following lemmas.

Lemma 3 [13]: Suppose that \( C = \langle g(x) \rangle \subset \mathbb{F}_q[x] \) is a \( \lambda \)-constacyclic code of length \( 2p^t \). Then one of the following two cases holds:

(I). If \( \lambda \in A_{even} \), then there exists a nonzero element \( \theta_0 \in \mathbb{F}_q^\times \) such that \( \theta_0^{2p^t} = \lambda^{-1} \). Then \( \lambda \) is the ideal \( \langle \theta_0 x - 1 \rangle \langle \theta_0 x + 1 \rangle \subset \mathbb{F}_q \), where \( 0 \leq i, j \leq p^t \).

(II). If \( \lambda \in A_{odd} \), then there exists a nonzero element \( \theta_1 \in \mathbb{F}_q^\times \) such that \( \theta_1^{2p^t} = -\lambda \). Then \( \lambda \) is the ideal \( \langle (x^2 + \theta_1) x \rangle \subset \mathbb{F}_q \), where \( 0 \leq i \leq p^t \).

Now we give Theorem 7 on constructing quantum synchronizable codes from constacyclic codes of length \( 2p^t \).

Theorem 7: Assume that \( C_1 = \langle g_1(x) \rangle, C_2 = \langle g_2(x) \rangle \) are cyclic codes of length \( 4p^t \). \( C_6 = \langle g_6(x) \rangle, C_8 = \langle g_8(x) \rangle \) are \( \lambda \)-constacyclic codes of length \( 2p^t \) with \( \lambda = \xi^{\frac{p-1}{2}} \). \( C_6 = \langle g_6(x) \rangle, C_8 = \langle g_8(x) \rangle \) are \( -\lambda \)-constacyclic codes of length \( 2p^t \). Then the generator polynomial of cyclic code \( C_r \) for \( r \in \{1, 2\} \) is

\[
g_r(x) = (x - 1)^{p^s - \varepsilon_{r,1}} (x + 1)^{p^s - \varepsilon_{r,2}} (x - \lambda)^{p^s - \varepsilon_{r,1}}
\]

\[
\times (x + \lambda)^{p^s - \varepsilon_{r,2}}, \quad r \in \{1, 2\}.
\]
The generator polynomials of $C_i$, $C_j$, $i \in \{5, 7\}$ and $j \in \{6, 8\}$ are one of the following two cases:

(I). If $p \equiv 1 \bmod 8$ (any $m$) or $p \equiv 3, 5, 7 \bmod 8$ ($m$ is even), then $C_i$, $C_j$ have generator polynomials

$$g_i(x) = (\theta_0 x - 1)^{p^i - s_{i,1}}(\theta_0 x + 1)^{p^i - s_{i,2}}, \quad i \in \{5, 7\},$$
$$g_j(x) = (\theta_0 - 1) x - 1)^{p^j - s_{j,1}}(\theta_0 - 1) x + 1)^{p^j - s_{j,2}}, \quad j \in \{6, 8\}.$$  

(23)

respectively with $\theta_0 p^t = \lambda - 1$, where $\sigma_t^p \geq e_{i,1}, e_{j,1} \leq p^t$ for $t \in \{1, 2\}$. Assume that $e_{5,1} \leq e_{7,1}$. If there exists an integer $\mu \in \{1, 2\}$ such that $e_{7,1} > e_{5,1} + 1$ or $e_{8,1} > e_{6,1} + 1$, then quantum synchronizable code $(a_1, a_2) - \left[ [8^p a_1 + a_2, a_2, k] \right]$ quantum synchronizable code where $k = 2 \left( e_{5,1} + e_{6,1} + e_{7,1} - 4 p^t \right)$.

(II). If $p \equiv 5 \bmod 8$ ($m$ is odd), then $C_i$, $C_j$ have generator polynomials

$$g_i(x) = (x^2 + \theta_1)^{p^i - e_{i,1}}, \quad i \in \{5, 7\},$$
$$g_j(x) = (x^2 + \theta_1 - 1)^{p^j - e_{j,1}}, \quad j \in \{6, 8\}.$$  

(24)

respectively with $\theta_1 p^t = -\lambda$, where $\sigma_t^p \leq e_{i,1}, e_{j,1} \leq p^t$. Assume that $e_{5} \leq e_{7}$, $e_{6} \leq e_{8}$. If there exists an integer $\nu \in \{1, 2\}$ such that $e_{7} > e_{5} + 1$ or $e_{6} > e_{5} + 1$, then for any pair of non-negative integers $a_1, a_2$ such that $a_1 + a_2 < 8^p$, we can construct an $(a_1, a_2) - \left[ [8^p a_1 + a_2, a_2, k] \right]$ quantum synchronizable code where $k = 2 \sum_{t=1}^{2} (e_{5,1} + e_{6,1} + e_{7,1}) - 4 p^t$.

Proof: Note that $\lambda \in A_{even}$ if $p \equiv 1 \bmod 8$ (any $m$) or $p \equiv 3, 5, 7 \bmod 8$ ($m$ is odd), and $\lambda \in A_{odd}$ if $p \equiv 5 \bmod 8$ ($m$ is odd). We can get the generator polynomials of $\lambda$-constacyclic codes by Lemma 3. There does not exist $\lambda$-constacyclic codes of length $2p^t$ in other cases of $p$ modulo 8. Then taking arguments similar to the proof of Theorem 5, we can obtain the results of Theorem 7.

From Theorem 4, 5, 6, and 7, we can tell that the quantum synchronizable codes can be derived from cyclic codes and constacyclic codes. And the conditions that quantum synchronizable codes reach maximum tolerance against misalignment are proved.

V. THE ERROR-CORRECTING CAPABILITY OF QUANTUM SYNCHRONIZABLE CODES

In this section, we discuss the error-correcting capability of quantum synchronizable codes in Section 4. If the constacyclic codes and cyclic codes meet the conditions of theorems mentioned in Section 4, the obtained quantum synchronizable codes can achieve maximum tolerance against misalignment. Besides, the component classical codes with large minimum distances guarantee that quantum synchronizable codes have great ability in correcting Pauli errors. For simplicity, we only discuss the error-correcting capability against bit errors. Phase errors can be discussed through the same method.

Firstly, there is an $\mathbb{F}_q$-algebra isomorphism [12]

$$\phi_0 : \mathbb{F}_q[x] / (x^{p^m} - 1) \rightarrow \mathbb{F}_q[x] / (x^{p^m} - \lambda),$$
$$f(x) \mapsto f(ax),$$  

(25)

where $a$ is a nonzero element of $\mathbb{F}^+_{q^m}$. Therefore, the minimum distances of $lp^t$-length constacyclic codes can be determined by following the same strategies of cyclic codes. And Luo et al. [8] have discussed the computation of the minimum distances of $lp^t$-length cyclic codes. Define a set of corresponding simple-root $l$-length $\lambda$-constacyclic codes $\{\overline{C}_{i,\nu}\}_{0 \leq \nu \leq p^t - 1}$ with the generator polynomial

$$\tilde{g}_{i,\nu}(x) = \prod_{t=0}^{e} \tilde{M}_t(ax)^{\lambda - s_{i,t}},$$  

(26)

where $f_{r,\nu,t}(x) = \begin{cases} 1, & \text{if } p^t - e_{i,t} > \nu, \\ 0, & \text{otherwise}. \end{cases}$ Denote by $P_{\nu}$ the Hamming weight of the polynomial $(x - 1)^\nu$ and $P_{\nu} = \prod_{\mu=0}^{e-1} (\nu_\mu + 1)$, where $v = \sum_{\mu=0}^{e-1} \nu_\mu p^\mu$ for $0 \leq \nu_\mu \leq p - 1$ and $0 \leq \nu \leq s - 1$. Define the set [14]

$$V = \sum_{\nu=0}^{p^t - 1} (p^t - \nu)^{s_{i,t}} + \nu^{s_{i,t} - 1} | 1 \leq \nu \leq s,$$

$$1 \leq \tau \leq p - 1 \} \cup \{0\}.$$  

(27)

Then the minimum distance $d(C_i)$ of $\lambda$-constacyclic code $C_i$ can be computed by

$$d(C_i) = \min\{P_{\nu} \cdot d(\overline{C}_{i,\nu}) | v \in V\},$$  

(28)

where $d(\overline{\mathcal{C}}_{i,\nu})$ is the minimum distance of $\overline{C}_{i,\nu}$. Therefore, we are able to convert the computation of $d(C_i)$ into computing $\min\{P_{\nu} | v \in V\}$ and $d(\overline{\mathcal{C}}_{i,\nu})$. The minimum distance of $-\lambda$-constacyclic code $C_j$ can be discussed similarly.

Let $\epsilon_{\min}$ and $\epsilon_{\max}$ be the minimum and maximum elements in the set $[p^t - e_{i,t}]_{0 \leq t \leq e}$ respectively. Parameter $d'$ denotes the minimum distance of $\overline{\mathcal{C}}_{i,\nu}$, where $P_{\nu} = \min\{P_{\nu} | v \in V, \epsilon_{\min} \leq v < \epsilon_{\max}\}$. Parameters $1 \leq \beta, \beta_1, \beta_2 \leq p - 2, 1 \leq \mu, \mu_1, \mu_2 \leq s - 1$ and $1 \leq \tau, \tau_1, \tau_2 \leq p - 1$ are integers. Then the minimum distance of $lp^t$-length constacyclic code are listed in Table 1.

From the above, we take $3p^t$-length constacyclic codes as an example. Let $l = 3$ be a prime distinct from $p$ and $\gcd(l, q - 1) = 1$. Then we have $p^m \equiv 2 \bmod 3$. Due to (25) we can construct a $\mathbb{F}_q$-algebra isomorphism $\phi_0 : \mathbb{F}_q[x] / (x^{p^m} - 1) \rightarrow \mathbb{F}_q[x] / (x^{p^m} - \lambda)$ that maps $f(x)$ to $f(ax)$, where $\theta \in \mathbb{F}_q^+$ such that $\theta^3 p^t = \lambda$ [15]. When $l = 3$ and $p^m \equiv 2 \bmod 3$, $3p^t$-length cyclic code has a generator polynomial $g(x) = (x - 1)^{p^t - 1}(x^2 + x + 1)^{p^t - 2}$ for $0 \leq i_1, i_2 \leq p^t$. According to the map $\phi_0, \lambda = \left[ [8^p a_1 + a_2, a_2, k] \right]$ quantum synchronizable code where $k = 2 \sum_{t=1}^{2} (e_{5,1} + e_{6,1} + e_{7,1}) - 4 p^t$.

$$g_i(x) = (x + a)^{p^i - s_{i,1}}(x^2 - ax + a^2)^{p^i - s_{i,1}}, \quad i \in \{5, 7\},$$
$$g_j(x) = (x - a)^{p^j - s_{j,1}}(x^2 + ax + a^2)^{p^j - s_{j,2}}, \quad j \in \{6, 8\}.$$  

(29)
then there exists an element \( v \). Assume that \( p \) and \( \beta \) are known. We also can find an element \( v \).

The minimum distance of an \( p \)-length cyclic code with a generator polynomial

\[
g_r(x) = (x - 1)^{p^s - r_{i,1}}(x + 1)^{p^s - r_{i,2}}(x^2 + x + 1)^{p^s - r_{i,3}}
\]

respectively with \( p^s \leq e_{j,1} \leq e_{j,2}, e_{j,1} \leq e_{j,2} \leq p^s \). The minimum distances of \( \bar{C}_{i,v} \) and \( \bar{C}_{j,v} \) are given as follows

\[
d(\bar{C}_{i,v}) = \begin{cases} 
1, & \text{if } p^s - e_{i,1} \leq v, p^s - e_{i,2} \leq v \\
2, & \text{if } p^s - e_{i,1} > v, p^s - e_{i,2} \leq v \\
3, & \text{if } p^s - e_{i,1} \leq v, p^s - e_{i,2} > v \\
\infty, & \text{if } p^s - e_{i,1} > v, p^s - e_{i,2} > v,
\end{cases}
\]

\[
d(\bar{C}_{j,v}) = \begin{cases} 
1, & \text{if } p^s - e_{j,1} \leq v, p^s - e_{j,2} \leq v \\
2, & \text{if } p^s - e_{j,1} > v, p^s - e_{j,2} \leq v \\
3, & \text{if } p^s - e_{j,1} \leq v, p^s - e_{j,2} > v \\
\infty, & \text{if } p^s - e_{j,1} > v, p^s - e_{j,2} > v.
\end{cases}
\]

Assume that \( p^s - e_{i,1} < p^s - e_{i,2} \) and \( p^s - e_{j,1} < p^s - e_{j,2} \), then there exists an element \( v' \) in \( V \) such that \( d(\bar{C}_{i,v'}) = 3 \) and \( P_{i,v'} = \min(P_{i,v} \mid v' \in V, v' < p^s - e_{i,2}) \). We also can find an element \( v_i' \) in \( V \) such that \( d(C_i) = 3 \). Table 2 lists sample parameters for constacyclic codes \( C_i, C_j \) and negacyclic code \( C_j \) based on the \((u + v)(u - v)\) construction.

Suppose that \( C_r \) is a \( 6p^s \)-length cyclic code with a generator polynomial

\[
g_r(x) = (x - 1)^{p^s - e_{r,1}}(x + 1)^{p^s - e_{r,2}}(x^2 + x + 1)^{p^s - e_{r,3}}
\]

The minimum distance of a \( 6p^s \)-length cyclic code can be computed using the strategies in [8]. Then the \( 12p^s \)-length cyclic code \( C_r \) can be determined. We list some parameters in Table 3.
tell that it is easy to construct dual-containing constacyclic codes for a set of parameters. This is because repeated-root constacyclic codes have their advantageous dual-containing properties. And due to the strong relation between their minimum distances and those of a corresponding set of simple-root cyclic codes, we can exactly compute the minimum distance of constacyclic codes.

Table 4 lists some sample parameters of projective geometry codes. By the comparison between Table 3 and 4, we can tell that if the parameters of repeated-root cyclic codes and constacyclic codes are chosen properly, then $C_r \∩ (C_1 \∩ C_2)$ has a larger minimum distance than a projective geometry code of close length.

Example 1: Taking case 3 in Table 3 for example, we can use the constacyclic codes and cyclic codes with the parameters of case 3 to construct an $(a_1, a_r) - [[1452 + a_1 + a_r, 466]]$ quantum synchronizable code $Q_1$. $Q_1$ can correct at least up to 3 bit errors. Besides, we can construct an $(a_1, a_r) - [[1464 + a_1 + a_r, 890]]$ quantum synchronizable code $Q_2$ from a projective geometry code $[5, 16]$ with the parameters of case 3 in Table 4. $Q_2$ also reach maximum tolerance against misalignment. And $Q_2$ can corrects at least up to 1 bit errors.

Comparing $Q_1$ with $Q_2$, we can see that $Q_1$ from cyclic codes and constacyclic codes can correct more bit errors than $Q_2$ from a projective geometry code over the same base fields of close lengths. In other words, although both of $Q_1$ and $Q_2$ achieve maximum tolerance against misalignment, the quantum synchronizable codes from cyclic codes and constacyclic codes may have a better capability in correcting bit errors than those from projective geometry codes in some cases.

Example 2: We can use the constacyclic codes and cyclic codes with the parameters of case 4 in Table 3 to construct an $(a_1, a_r) - [[3468 + a_1 + a_r, 436]]$ quantum synchronizable code $Q_3$. $Q_3$ can correct at least up to 5 bit errors and 5 phase errors. However, an $(a_1, a_r) - [[5220 + a_1 + a_r, 4609]]$ quantum synchronizable code $Q_4$ from a projective geometry code with the parameters of case 4 in Table 4 can corrects at least up to 1 bit errors and 8 phase errors.

According to the above examples, the quantum synchronizable codes from projective geometry codes reduce bit error-correcting capabilities because the cyclic codes responsible for bit error detection will have smaller minimum distances [5]. We use the parameters in Table 3 and construct quantum synchronizable codes which are listed in Table 5. We can tell that quantum synchronizable codes from cyclic codes and constacyclic codes can correct bit errors and phase errors with a close number. So our quantum synchronizable codes ensure good performance in both bit errors and phase errors.

VI. CONCLUSION

In this paper, we expand the work of [9] and present a family of quantum synchronizable codes based on the $(\lambda(u + v)u - v)$ construction. This family of quantum synchronizable codes are derived from cyclic codes and constacyclic codes. The obtained quantum synchronizable codes can reach maximum tolerance against misalignment under some conditions. Besides, we precisely compute minimum distance of the component cyclic codes and constacyclic codes. Some sample parameters are listed in Table 2 and 3. We also give the sample parameters of projective geometry codes. By the comparison between two types of quantum synchronizable codes, we illustrate that quantum synchronizable codes from repeated-root codes of length $lp^r$ are able to have a better performance in correcting bit errors than those from projective geometry codes in some cases.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, Quantum Computing Quantum Information, 10th ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[2] Y. Fujiwara, “Block synchronization for quantum information,” Phys. Rev. A, Gen. Phys., vol. 87, no. 2, Feb. 2013.
[3] S. Bregni, Synchronization of Digital Telecommunications Networks. New York, NY, USA: Wiley, 2002.
[4] B. Sklar, Digital Communications: Fundamentals and Applications, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2006.
[5] Y. Fujiwara and P. Vandendriessche, “Quantum synchronizable codes from finite geometries,” IEEE Trans. Inf. Theory, vol. 60, no. 11, pp. 7345–7354, Nov. 2014.
[6] Y. Fujiwara, V. D. Tonchev, and T. W. H. Wong, “Algebraic techniques in designing quantum synchronizable codes,” Phys. Rev. A, Gen. Phys., vol. 88, no. 1, pp. 162–166, Jul. 2013.
[7] Y. Xie, J. Yuan, and Y. Fujiwara, “Quantum synchronizable codes from quadratic residue codes and their superscripts,” PLoS ONE, vol. 6, no. 2, 2014, Art. no. e14641.
[8] L. Luo and Z. Ma, “Non-binary quantum synchronizable codes from repeated-root cyclic codes,” IEEE Trans. Inf. Theory, vol. 64, no. 3, pp. 1461–1470, Mar. 2018.
[9] L. Luo, Z. Ma, and D. Lin, “Two new families of quantum synchronizable codes,” Quantum Inf. Proces., vol. 18, no. 9, p. 277, Sep. 2019.
[10] G. Hughes, “Constacyclic codes, cocycles and a u-vu-v construction,” IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 674–680, Mar. 2000.
[11] H. Q. Dinh, “Constacyclic codes of length $p^s$ over $\mathbb{F}_{p^m} + u \mathbb{F}_{p^m}$,” J. Algebra, vol. 324, no. 5, pp. 940–950, Mar. 2010.
[12] B. Chen, Q. D. Hai, and H. Liu, “Repeated-root constacyclic codes of length $p^s$ and their duals,” Discrete Appl. Math., vol. 177, pp. 60–70, Nov. 2014.
[13] H. Q. Dinh, “Repeated-root constacyclic codes of length $2p^s$,” Finite Fields Their Appl., vol. 18, no. 1, pp. 133–143, 2012.
C. Du et al.: On a Family of Quantum Synchronizable Codes Based on the $(\lambda (u + v)|u - v)$ Construction

[14] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, “On repeated-root cyclic codes,” IEEE Trans. Inf. Theory, vol. 37, no. 2, pp. 337–342, Mar. 1991.

[15] H. Q. Dinh, “Structure of repeated-root constacyclic codes of length $3p^s$ and their duals,” Discrete Math., vol. 313, no. 9, pp. 983–991, 2013.

[16] J. W. P. Hirschfeld and R. Shaw, “Projective geometry codes over prime fields,” in Proc. Finite Fields, Theory, Appl. Algorithms 2nd Int. Conf. Providence, RI, USA: American Mathematical Society, 1994, pp. 151–163.

CHAO DU received the B.E. degree in mathematics, in 2018. He is currently pursuing the master’s degree with the State Key Laboratory of Mathematical Engineering and Advanced Computing, and the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China. His research field is quantum error correction.

ZHI MA received the Ph.D. degree in mathematics from the University of Science and Technology of China, in 2002. She is currently a Professor with the State Key Laboratory of Mathematical Engineering and Advanced Computing, the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China, and the CAS Excellence Innovation Center of Quantum Information and Quantum Physics, Hefei, China. Her research interests include quantum information and quantum computation.

LAN LUO received the M.S. degree in mathematics, in 2017. She is currently pursuing the Ph.D. degree in mathematics with the State Key Laboratory of Mathematical Engineering and Advanced Computing, and the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China. Her research fields are quantum error correction and quantum fault-tolerant computing.

DAKANG HUANG received the M.S. degree in mathematics from the State Key Laboratory of Mathematical Engineering and Advanced Computing, and the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China, in 2019. His research fields are quantum error correction and quantum information.

LAN LUO received the M.S. degree in mathematics, in 2017. She is currently pursuing the Ph.D. degree in mathematics with the State Key Laboratory of Mathematical Engineering and Advanced Computing, and the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China. Her research fields are quantum error correction and quantum fault-tolerant computing.

HONG WANG received the Ph.D. degree in mathematics from the University of Information Engineer, in 2015. He is currently a Researcher with the State Key Laboratory of Mathematical Engineering and Advanced Computing, and the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, China. His research interests include quantum information and quantum computation.

**CHAO DU**

**LAN LUO**

**ZHI MA**

**DAKANG HUANG**

**HONG WANG**