IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 8, 2019, accepted December 22, 2019, date of publication December 31, 2019,
date of current version January 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2963289

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 be able 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 *synchronizable 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 associate editor coordinating the review of this manuscript and approving it for publication was Daniel Benevides Da Costa.

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 $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ the multiplicative group. It is well known that $\mathbb{F}_q^*$ is a cyclic group of order $q-1$. Let ξ be a primitive $(q-1)$-th root of unity in $\mathbb{F}_q$, then

$$\mathbb{F}_{p^m} = \{0, \xi, \ldots, \xi^{p^m-2}, \xi^{p^m-1} = 1\}.$$

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

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

Let λ 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 λ-constacyclic shift τ_λ on $\mathbb{F}_q^n$ as

$$\tau_\lambda(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, c_1, \ldots, c_{n-2}).$$

A code $\mathcal{C}$ is λ-constacyclic if $\tau_\lambda(\mathcal{C}) = \mathcal{C}$. And a λ-constacyclic code $\mathcal{C}$ is said to be a cyclic code if $\lambda = 1$ and a negacyclic code if $\lambda = -1$. Any λ-constacyclic code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be identified as exactly one ideal in the quotient ring $\frac{\mathbb{F}_q[x]}{\langle x^n-\lambda\rangle}$, 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 $\mathcal{C}$ and denote by $\mathcal{C} = \langle g(x)\rangle$. Let $h(x) = \frac{x^n-\lambda}{g(x)}$. Then the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is a λ^{-1}-constacyclic 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 $\mathcal{Q}$ is a q^k-dimensional subspace of a q^n-dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$, 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 $(a_l, a_r) - [[n, k]]$ quantum synchronizable code, it can correct not only Pauli errors, but block misalignment to the left by at most a_l qudits and to the right by at most a_r qudits for a pair of nonnegative integers (a_l, a_r). 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 $\mathrm{ord}(f(x)) = |\{x^a \bmod f(x) | a \in \mathbb{N}\}|$ the order of the polynomial $f(x)$. The main result is given as following.

Theorem 1 [9]: $\mathcal{C}_i = \langle g_i(x)\rangle$ be an $[n, k_i, d_i]$ dual-containing code for $i \in \{1, 2, 3, 4\}$. Suppose that $\mathcal{C}_1$, $\mathcal{C}_2$ are cyclic codes with $\mathcal{C}_1 \subset \mathcal{C}_2$ and $\mathcal{C}_3$, $\mathcal{C}_4$ are negacyclic codes with $\mathcal{C}_3 \subset \mathcal{C}_4$. Define the polynomial $f(x)$ to be the quotient of $g_1(x)g_3(x)$ divided by $g_2(x)g_4(x)$. Then for any pair of nonnegative integers a_l, a_r such that $a_l + a_r < ord(f(x))$, there exists an $(a_l, a_r) - [[2n + a_l + a_r, 2(k_1 + k_3) - n]]$ quantum synchronizable code that can correct up to $\left\lfloor \frac{\min\{2d_2, 2d_4, \max\{d_2, d_4\}\}-1}{2} \right\rfloor$ bit errors and $\left\lfloor \frac{\min\{2d_1, 2d_3, \max\{d_1, d_3\}\}-1}{2} \right\rfloor$ phase errors.

Theorem 1 needs a pair of dual-containing cyclic codes $\mathcal{C}_1, \mathcal{C}_2$ and a pair of dual-containing negacyclic codes $\mathcal{C}_3$, $\mathcal{C}_4$ to generate a family of quantum synchronizable code. The obtained quantum synchronizable code can achieve the maximum tolerance against misalignment when $\mathrm{ord}(f(x)) = 2n$. 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

than or up to twice larger than the component cyclic codes $\mathcal{C}_1$ and $\mathcal{C}_3$.

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 $x^{2n}+1=(x^n-\lambda_1)(x^n-\lambda_2)$ since we use an n-length λ_1-constacyclic code and an n-length λ_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 $\mathcal{C}_1$ and $\mathcal{C}_2$ 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 $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. And $g_1(x)$, $g_2(x)$ are the generator polynomials of $\mathcal{C}_1$ and $\mathcal{C}_2$ 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 $\mathcal{C}=\mathcal{C}_1\curlyvee\mathcal{C}_2=\{(\lambda(u+v)|u-v)|u\in\mathcal{C}_1, v\in\mathcal{C}_2\}$ is a $[2n,k_1+k_2,\min\{2d_1,2d_2,\max\{d_1,d_2\}\}]$ negacyclic code with a generator matrix

$$G=\begin{pmatrix}-\lambda_2 G_1 & G_1\\ \lambda_1 G_2 & -G_2\end{pmatrix}, \tag{1}$$

and a generator polynomial $g(x)=g_1(x)g_2(x)$. The dual code ${\mathcal{C}}^{\perp}$ is a $(-\lambda(u+v)|u-v)$ construction of ${\mathcal{C}_1}^{\perp}$ and ${\mathcal{C}_2}^{\perp}$, i.e., ${\mathcal{C}}^{\perp}=(\mathcal{C}_1\curlyvee\mathcal{C}_2)^{\perp}={\mathcal{C}_1}^{\perp}\curlyvee{\mathcal{C}_2}^{\perp}$ 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 $\mathcal{C}_1\curlyvee\mathcal{C}_2$ is the row space of G, and G has rank k_1+k_2. So $\mathcal{C}_1\curlyvee\mathcal{C}_2$ is a negacyclic code [10]. Assume that $\mathcal{C}_1\curlyvee\mathcal{C}_2$ has a generator polynomial $g(x)|x^{2n}+1$. Since g is a codeword, g can be written as

$$\begin{aligned}g(x)&=-\lambda_2 a g_1+\lambda_1 b g_2+x^n(a g_1-b g_2)\\&=\lambda(a g_1+b g_2)+x^n(a g_1-b g_2)\end{aligned} \tag{3}$$

for some polynomials a,b. The equality (3) can be rewritten as $g(x)=a g_1(x^n-\lambda_2)-b g_2(x^n-\lambda_1)$. Due to $g_1(x)|x^n-\lambda_1$ and $g_2(x)|x^n-\lambda_2$, 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 $u\in\mathcal{C}_1$, $v\in\mathcal{C}_2$ are different codewords. If $u\neq 0$, then $\mathrm{wt}(\lambda(u+v),u-v)\geqslant\mathrm{wt}(u)\geqslant d_1$. And if $u=0$, then $\mathrm{wt}(\lambda v,-v)=2d_1$. As a result, the code $\mathcal{C}=\mathcal{C}_1\curlyvee\mathcal{C}_2$ 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 ${\mathcal{C}}^{\perp}$ can be obtained by using the same method. □

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

Throughout this paper, we assume that $p\equiv 1 \bmod 4$ (any m) or $p\equiv 3 \bmod 4$ (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 $\mathcal{C}_i=\langle g_i(x)\rangle$ be a $[2n,k_i,d_i]$ dual-containing cyclic code for $i\in\{1,2\}$. Let $\mathcal{C}_j=\langle g_j(x)\rangle$ be an $[n,k_j,d_j]$ constacyclic code for $j\in\{5,6,7,8\}$. $\mathcal{C}_5=\langle g_5(x)\rangle$ and $\mathcal{C}_7=\langle g_7(x)\rangle$ are λ-constacyclic codes of length n. $\mathcal{C}_6=\langle g_6(x)\rangle$ and $\mathcal{C}_8=\langle g_8(x)\rangle$ are $-\lambda$-constacyclic codes of length n. Suppose that $\mathcal{C}_1\subset\mathcal{C}_2$, $\mathcal{C}_5\subset\mathcal{C}_7$ and $\mathcal{C}_6\subset\mathcal{C}_8$. Then $\mathcal{C}_3=\mathcal{C}_5\curlyvee\mathcal{C}_6$, $\mathcal{C}_4=\mathcal{C}_7\curlyvee\mathcal{C}_8$ are negacyclic codes satisfying $\mathcal{C}_3\subset\mathcal{C}_4$. Denote by d_3, d_4 the minimum distances of $\mathcal{C}_3$, $\mathcal{C}_4$ and k_3, k_4 the dimensions of $\mathcal{C}_3$, $\mathcal{C}_4$ respectively. Define the polynomial $f(x)=\frac{g_1(x)g_5(x)g_6(x)}{g_2(x)g_7(x)g_8(x)}$. Then for any pair of nonnegative integers a_l, a_r such that $a_l+a_r<ord(f(x))$, there exists an $(a_l,a_r)-[[4n+a_l+a_r,2(k_1+k_5+k_6-2n)]]$ quantum synchronizable code that can correct up to $\left\lfloor\frac{\min\{2d_2,2d_4,\max\{d_2,d_4\}\}-1}{2}\right\rfloor$ bit errors and $\left\lfloor\frac{\min\{2d_1,2d_3,\max\{d_1,d_3\}\}-1}{2}\right\rfloor$ phase errors, where $d_3=\min\{2d_5,2d_6,\max\{d_5,d_6\}\}$ and $d_4=\min\{2d_7,2d_8,\max\{d_7,d_8\}\}$.

Proof: From Theorem 2 we can get the result that $\mathcal{C}_3=\mathcal{C}_5\curlyvee\mathcal{C}_6=\langle g_5(x)g_6(x)\rangle$ is a $[2n,k_5+k_6,d_3]$ negacyclic code with $d_3=\min\{2d_5,2d_6,\max\{d_5,d_6\}\}$ and $\mathcal{C}_4=\mathcal{C}_7\curlyvee\mathcal{C}_8=\langle g_7(x)g_8(x)\rangle$ 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 $\mathcal{C}_3\subset\mathcal{C}_4$ because of $\mathcal{C}_5\subset\mathcal{C}_7$ and $\mathcal{C}_6\subset\mathcal{C}_8$. Then we can get the desired quantum synchronizable codes by applying $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_4$ 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 $\mathrm{ord}(f(x))$ is $4n$. Let $f(x)=\frac{g_1(x)g_5(x)g_6(x)}{g_2(x)g_7(x)g_8(x)}$ in Theorem 3. The way of achieving the maximum tolerance against misalignment is to make $\mathrm{ord}(\frac{g_5(x)}{g_7(x)})=4n$ or $\mathrm{ord}(\frac{g_6(x)}{g_8(x)})=4n$ whatever the value of $\mathrm{ord}(\frac{g_1(x)}{g_2(x)})$ 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 $x^{2p^s}+1=(x^{p^s}-\lambda)(x^{p^s}+\lambda)$ with $\lambda=\xi^{\frac{p^m-1}{4}}\in\mathbb{F}_{p^m}$. λ is a nonzero element of the field $\mathbb{F}_{p^m}$, so $\lambda^{-p^m}=\lambda^{-1}$. By the division algorithm, there exist nonnegative integers r_1, r_2 such that $s=r_1m+r_2$ and $0\leqslant r_2\leqslant m-1$. Let $\lambda_0=-\lambda^{-p^{(r_1+1)m-s}}=-\lambda^{-p^{m-r_2}}$. Then

$\lambda_0^{p^s} = -\lambda^{-p^{(r_1+1)m}} = -\lambda^{-1}$. The following lemma gives the generator polynomial of λ-constacyclic code of length p^s.

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

Applying Lemma 1 to Theorem 3, we can construct quantum synchronizable codes from constacyclic codes of length p^s.

Theorem 4: Let $\mathcal{C}_r = \langle(x-1)^{p^s-\varepsilon_{r,1}}(x+1)^{p^s-\varepsilon_{r,2}}\rangle$ be a cyclic code of length $2p^s$ with $\varepsilon_{1,1} \leqslant \varepsilon_{2,1}$, $\varepsilon_{1,2} \leqslant \varepsilon_{2,2}$, $\frac{p^s}{2} \leqslant \varepsilon_{r,1}, \varepsilon_{r,2} \leqslant p^s$, and $r \in \{1,2\}$. Furthermore, $\mathcal{C}_i = \langle(\lambda_0 x+1)^{p^s-\varepsilon_i}\rangle$ and $\mathcal{C}_j = \langle(-\lambda_0 x+1)^{p^s-\varepsilon_j}\rangle$ are λ-constacyclic code and $-\lambda$-constacyclic code of length p^s respectively with $\frac{p^s}{2} \leqslant \varepsilon_i, \varepsilon_j \leqslant p^s$ for $i \in \{5,7\}$ and $j \in \{6,8\}$, where $\lambda = \xi^{\frac{p^m-1}{4}}$ and $\lambda_0^{p^s} = -\lambda^{-1}$. Assume that $\varepsilon_5 \leqslant \varepsilon_7$ and $\varepsilon_6 \leqslant \varepsilon_8$. If $\varepsilon_7-\varepsilon_5 \geqslant p^{s-1}$ or $\varepsilon_8-\varepsilon_6 \geqslant p^{s-1}$, then for any pair of nonnegative integers a_l, a_r such that $a_l + a_r < 4p^s$, we can construct an $(a_l, a_r) - [[4p^s + a_l + a_r, k]]$ quantum synchronizable code where $k = 2(\varepsilon_{1,1}+\varepsilon_{1,2}+\varepsilon_5+\varepsilon_6-2p^s)$.

Proof: $\mathcal{C}_r$ is a dual-containing code since the condition $\frac{p^s}{2} \leqslant \varepsilon_{r,1}, \varepsilon_{r,2} \leqslant p^s$ for $r \in \{1,2\}$. By Lemma 1, λ-constacyclic code $\mathcal{C}_i$ has a generator polynomial as follows:

$$g_i(x) = (\lambda_0 x+1)^{p^s-\varepsilon_i}, \quad i \in \{5,7\},$$

with $\lambda_0^{p^s} = -\lambda^{-1}$. Due to $\lambda^{-1} = -\lambda$, we can get $-\lambda$-constacyclic code $\mathcal{C}_j$ has a generator polynomial as follows:

$$g_j(x) = (-\lambda_0 x+1)^{p^s-\varepsilon_j}, \quad j \in \{6,8\}.$$

It is clear that $\mathcal{C}_3 = \mathcal{C}_5 \curlyvee \mathcal{C}_6$ and $\mathcal{C}_4 = \mathcal{C}_7 \curlyvee \mathcal{C}_8$ are negacyclic codes. Furthermore, the fact that $\mathcal{C}_1 \subset \mathcal{C}_2$ and $\mathcal{C}_3 \subset \mathcal{C}_4$ is obvious due to the assumption that $\varepsilon_{1,1} \leqslant \varepsilon_{2,1}$, $\varepsilon_{1,2} \leqslant \varepsilon_{2,2}$, and $\varepsilon_5 \leqslant \varepsilon_7$, $\varepsilon_6 \leqslant \varepsilon_8$. If $\varepsilon_7 - \varepsilon_5 \geqslant p^{s-1}$ or $\varepsilon_8 - \varepsilon_6 \geqslant p^{s-1}$, then the order of the polynomial

$$\begin{aligned} f(x) &= \frac{g_1(x)g_5(x)g_6(x)}{g_2(x)g_7(x)g_8(x)} \\ &= (x-1)^{\varepsilon_{2,1}-\varepsilon_{1,1}}(x+1)^{\varepsilon_{2,2}-\varepsilon_{1,2}} \\ &\quad \times (\lambda_0 x+1)^{\varepsilon_7-\varepsilon_5}(-\lambda_0 x+1)^{\varepsilon_8-\varepsilon_6} \end{aligned} \tag{4}$$

is $4p^s$. 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 investigete 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), $q = p^m$ and $m, s \geq 1$ are positive integers.

For any integer t, denote by C_t the q-cyclotomic coset of t modulo l over $\mathbb{F}_q$ by $C_t = \{t \cdot q^j (\mathrm{mod}\, l) | j = 0, 1, \ldots\}$. Let γ be a primitive l-th root of unity in the extension field $\mathbb{F}_{q^w}$, where $w = \mathrm{ord}_l(q)$ indicates the order of q in $\mathbb{Z}_l^*$. Let $e = \frac{l-1}{w}$. Then the following equality gives the irreducible factorization of $x^{lp^s}-1$ in $\mathbb{F}_q[x]$:

$$x^{lp^s} - 1 = (x^l-1)^{p^s} = \prod_{t=0}^{e} M_t(x)^{p^s} \tag{5}$$

where $M_t(x) = \prod_{i \in C_t}(x-\gamma^i)$ is the minimal polynomial of γ^t over $\mathbb{F}_q$ for $0 \leqslant t \leqslant e$. Denote by $\hat{M}_t(x)$ the monic polynomial of $M_t(x)$ dividing its leading coefficient. The following lemma gives the generator polynomials of λ-constacyclic codes of length lp^s.

Lemma 2 [12]: Suppose that $\mathcal{C} = \langle g(x)\rangle \subset \frac{\mathbb{F}_q[x]}{\langle x^{lp^s}-\lambda\rangle}$ is a λ-constacyclic code of length lp^s. Let $w = ord_l(q)$.
(I). If $\gcd(l, q-1) = 1$, then there exists a unique element $a \in \mathbb{F}_q^*$ such that $a^{lp^s}\lambda = 1$. And we have the generator polynomial of $\mathcal{C}$ as follows

$$g(x) = \prod_{t=0}^{e} \hat{M}_t(ax)^{p^s-\varepsilon_t}. \tag{6}$$

Especially, if w is odd, the generator polynomial of $\mathcal{C}$ can be written as

$$g(x) = (x-a^{-1})^{p^s-\varepsilon_0} \prod_{t=0}^{\frac{e}{2}} \hat{M}_t(ax)^{p^s-\varepsilon_t} \hat{M}_{-t}(ax)^{p^s-\varepsilon_{-t}}, \tag{7}$$

where $0 \leqslant \varepsilon_t, \varepsilon_{-t} \leqslant p^s$ for $0 \leqslant t \leqslant \frac{e}{2}$.
(II). If $\gcd(l, q-1) = l$, let $\zeta \in \mathbb{F}_q$ be a primitive l-th root of unity in $\mathbb{F}_q$. One of the following two cases holds:
(i). $\lambda \in \langle\xi^l\rangle$. Then there exists a unique element $b \in \mathbb{F}_q^*$ such that $b^{lp^s}\lambda = 1$, and the generator polynomial of $\mathcal{C}$ is

$$g(x) = (x-b^{-1})^{p^s-\varepsilon_0} \prod_{t=1}^{\frac{l-1}{2}} (x-b^{-1}\zeta^t)^{p^s-\varepsilon_t}(x-b^{-1}\zeta^{-t})^{p^s-\varepsilon_{-t}}, \tag{8}$$

where $0 \leqslant \varepsilon_t, \varepsilon_{-t} \leqslant p^s$ for $0 \leqslant t \leqslant \frac{l-1}{2}$.
(ii). $\lambda \notin \langle\xi^l\rangle$. A unique integer j with $1 \leqslant j \leqslant l-1$ and an element $d \in \mathbb{F}_q^*$ can be found such that $d^{lp^s}\lambda = \xi^{jp^s}$. Then the generator polynomial of $\mathcal{C}$ is

$$g(x) = (x-d^{-1}\xi^j)^{p^s-\varepsilon}, \quad 0 \leqslant \varepsilon \leqslant p^s. \tag{9}$$

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

Theorem 5: Let l be an odd prime satisfying $\gcd(l, q-1) = 1$. Assume that $\mathcal{C}_1 = \langle g_1(x)\rangle$, $\mathcal{C}_2 = \langle g_2(x)\rangle$ are cyclic codes of length $2lp^s$. $\mathcal{C}_5 = \langle g_5(x)\rangle$, $\mathcal{C}_7 = \langle g_7(x)\rangle$ are λ-constacyclic codes of length lp^s. $\mathcal{C}_6 = \langle g_6(x)\rangle$, $\mathcal{C}_8 = \langle g_8(x)\rangle$ are $-\lambda$-constacyclic codes of length lp^s. There exists a unique element $a \in \mathbb{F}_q^*$ such that $a^{lp^s}\lambda = 1$, where $\lambda = \xi^{\frac{p^m-1}{4}}$. Let $w = ord_l(q)$.
(I). If w is even, then the generator polynomial of cyclic code $\mathcal{C}_r$ for $r \in \{1,2\}$ is

$$g_r(x) = \prod_{t=0}^{e} M_t(x)^{p^s-\varepsilon_{r,t}} \hat{M}_t(-x)^{p^s-\delta_{r,t}}, \quad r \in \{1,2\}, \tag{10}$$

with $\frac{p^s}{2} \leqslant \varepsilon_{r,t}, \delta_{r,t} \leqslant p^s$ *for* $0 \leqslant t \leqslant e$. *Furthermore, constacyclic codes* $\mathcal{C}_i$, $\mathcal{C}_j$ *for* $i \in \{5,7\}$ *and* $j \in \{6,8\}$ *have generator polynomials*

$$g_i(x) = \prod_{t=0}^{e} \hat{M}_t(ax)^{p^s-\varepsilon_{i,t}}, \quad i \in \{5,7\},$$
$$g_j(x) = \prod_{t=0}^{e} \hat{M}_t(-ax)^{p^s-\varepsilon_{j,t}}, \quad j \in \{6,8\}, \tag{11}$$

respectively with $\frac{p^s}{2} \leqslant \varepsilon_{i,t}, \varepsilon_{j,t} \leqslant p^s$ *for* $0 \leqslant t \leqslant e$. *Assume that*

$$\varepsilon_{1,t} \leqslant \varepsilon_{2,t}, \quad \delta_{1,t} \leqslant \delta_{2,t},$$
$$\varepsilon_{5,t} \leqslant \varepsilon_{7,t}, \quad \varepsilon_{6,t} \leqslant \varepsilon_{8,t}, \tag{12}$$

for $0 \leqslant t \leqslant e$. *If there exists an integer* v *in the range* $0 \leqslant v \leqslant e$ *such that* $\varepsilon_{7,v} - \varepsilon_{5,v} > p^{s-1}$ *or* $\varepsilon_{8,v} - \varepsilon_{6,v} > p^{s-1}$, *then for any pair of nonnegative integers* a_l, a_r *such that* $a_l + a_r < 4lp^s$, *we can construct an* $(a_l, a_r) - [[4lp^s + a_l + a_r, k]]$ *quantum synchronizable code where*

$$k = 2(\sum_{t=1}^{e}(\varepsilon_{1,t} + \delta_{1,t} + \varepsilon_{5,t} + \varepsilon_{6,t})w + (\varepsilon_{1,0} + \delta_{1,0} + \varepsilon_{5,0} + \varepsilon_{6,0}) - 2lp^s). \tag{13}$$

(II). If w *is odd, then the generator polynomial of cyclic code* $\mathcal{C}_r$ *for* $r \in \{1,2\}$ *is*

$$g_r(x) = (x-1)^{p^s-\varepsilon_{r,0}}(x+1)^{p^s-\delta_{r,0}} \prod_{t=1}^{\frac{e}{2}} [M_t(x)^{p^s-\varepsilon_{r,t}} \times M_{-t}(x)^{p^s-\varepsilon_{r,-t}} \hat{M}_t(x)^{p^s-\delta_{r,t}} \hat{M}_{-t}(x)^{p^s-\delta_{r,-t}}], \quad r \in \{1,2\},$$

with $\frac{p^s}{2} \leqslant \varepsilon_{1,0}, \varepsilon_{2,0} \leqslant p^s$, $\frac{p^s}{2} \leqslant \delta_{1,0}, \delta_{2,0} \leqslant p^s$, $p^s \leqslant \varepsilon_{r,t} + \varepsilon_{r,-t}, \delta_{r,t} + \delta_{r,-t} \leqslant 2p^s$ *for* $1 \leqslant t \leqslant \frac{e}{2}$. *Furthermore, constacyclic codes* $\mathcal{C}_i$, $\mathcal{C}_j$ *for* $i \in \{5,7\}$ *and* $j \in \{6,8\}$ *have generator polynomials*

$$g_i(x) = (x-a^{-1})^{p^s-\varepsilon_{i,0}} \prod_{t=0}^{\frac{e}{2}} \hat{M}_t(ax)^{p^s-\varepsilon_{i,t}} \hat{M}_{-t}(ax)^{p^s-\varepsilon_{i,-t}}, \quad i \in \{5,7\},$$
$$g_j(x) = (x+a^{-1})^{p^s-\varepsilon_{j,0}} \prod_{t=0}^{\frac{e}{2}} \hat{M}_t(-ax)^{p^s-\varepsilon_{j,t}} \hat{M}_{-t}(-ax)^{p^s-\varepsilon_{j,-t}}, \quad j \in \{6,8\}, \tag{14}$$

respectively with $\frac{p^s}{2} \leqslant \varepsilon_{i,t}, \varepsilon_{j,t} \leqslant p^s$, $p^s \leqslant \varepsilon_{i,t} + \varepsilon_{i,-t}, \varepsilon_{j,t} + \varepsilon_{j,-t} \leqslant 2p^s$ *for* $1 \leqslant t \leqslant \frac{e}{2}$, *where* $a^{lp^s}\lambda = 1$. *Assume that*

$$\varepsilon_{1,0} \leqslant \varepsilon_{2,0}, \quad \varepsilon_{1,t} \leqslant \varepsilon_{2,t}, \ \varepsilon_{1,-t} \leqslant \varepsilon_{2,-t}, \ \varepsilon_{5,0} \leqslant \varepsilon_{7,0},$$
$$\varepsilon_{5,t} \leqslant \varepsilon_{7,t}, \ \varepsilon_{6,t} \leqslant \varepsilon_{8,t}, \ \delta_{1,0} \leqslant \delta_{2,0}, \ \delta_{1,t} \leqslant \delta_{2,t},$$
$$\delta_{1,-t} \leqslant \delta_{2,-t}, \ \varepsilon_{6,0} \leqslant \varepsilon_{8,0}, \ \varepsilon_{5,-t} \leqslant \varepsilon_{7,-t}, \ \varepsilon_{6,-t} \leqslant \varepsilon_{8,-t}, \tag{15}$$

for $1 \leqslant t \leqslant \frac{e}{2}$. *If there exists an integer* v *in the range* $-\frac{e}{2} \leqslant v \leqslant \frac{e}{2}$ *such that* $\varepsilon_{7,v} - \varepsilon_{5,v} > p^{s-1}$ *or* $\varepsilon_{8,v} - \varepsilon_{6,v} > p^{s-1}$, *then for any pair of nonnegative integers* a_l, a_r *such that* $a_l + a_r < 4lp^s$, *we can construct an* $(a_l, a_r) - [[4lp^s + a_l + a_r, k]]$ *quantum synchronizable code where*

$$k = 2(\sum_{-\frac{e}{2} \leqslant t \leqslant \frac{e}{2}, t \neq 0} (\varepsilon_{1,t} + \delta_{1,t} + \varepsilon_{1,-t} + \delta_{1,-t} + \varepsilon_{5,t} + \varepsilon_{6,t} + \varepsilon_{5,-t} + \varepsilon_{6,-t})w + (\varepsilon_{1,0} + \delta_{1,0} + \varepsilon_{5,0} + \varepsilon_{6,0}) - 2lp^s). \tag{16}$$

Proof: Assume w is even. We have the factorization

$$x^{2lp^s} - 1 = (x^{2l}-1)^{p^s} = \prod_{t=0}^{e} M_t(x)^{p^s} \hat{M}_t(-x)^{p^s}. \tag{17}$$

The generator polynomial of $\mathcal{C}_r$ is obvious. It is easy to verify that $\mathcal{C}_r$ is dual-containing code due to the condition that $\frac{p^s}{2} \leqslant \varepsilon_{r,t}, \delta_{r,t} \leqslant p^s$ for $0 \leqslant t \leqslant e$ and $r \in \{1,2\}$. By Lemma 2(I), λ-constacyclic code $\mathcal{C}_i$ has a generator polynomial as follows

$$g_i(x) = \prod_{t=0}^{e} \hat{M}_t(ax)^{p^s-\varepsilon_{i,t}}, \quad i \in \{5,6\},$$

with a unique element $a \in \mathbb{F}_q^*$ such that $a^{lp^s}\lambda = 1$, where $\frac{p^s}{2} \leqslant \varepsilon_{i,t} \leqslant p^s$ for $0 \leqslant t \leqslant e$. In a similar way, we can know that $-\lambda$-constacyclic code $\mathcal{C}_j$ has a generator polynomial as follows

$$g_j(x) = \prod_{t=0}^{e} \hat{M}_t(-ax)^{p^s-\varepsilon_{j,t}}, \quad j \in \{6,8\},$$

with a unique element $-a \in \mathbb{F}_q^*$ such that $(-a)^{lp^s} \cdot (-\lambda) = 1$, where $\frac{p^s}{2} \leqslant \varepsilon_{j,t} \leqslant p^s$ for $0 \leqslant t \leqslant e$. Let $\mathcal{C} = \mathcal{C}_5 \curlyvee \mathcal{C}_6$ and $\mathcal{D} = \mathcal{C}_7 \curlyvee \mathcal{C}_8$. $\mathcal{C}$ and $\mathcal{D}$ are negacyclic codes by Theorem 2. Then $\mathcal{C}$ and $\mathcal{D}$ have generator polynomials

$$g_{\mathcal{C}}(x) = \prod_{t=0}^{e} \hat{M}_t(ax)^{p^s-\varepsilon_{5,t}} \hat{M}_t(-ax)^{p^s-\varepsilon_{6,t}},$$
$$g_{\mathcal{D}}(x) = \prod_{t=0}^{e} \hat{M}_t(ax)^{p^s-\varepsilon_{7,t}} \hat{M}_t(-ax)^{p^s-\varepsilon_{8,t}}, \tag{18}$$

respectively. $\mathcal{C}$ and $\mathcal{D}$ are also dual-containing codes due to the condition that $\frac{p^s}{2} \leqslant \varepsilon_{i,t}, \varepsilon_{j,t} \leqslant p^s$ for $0 \leqslant t \leqslant e$. According to the assumption (12), we get $\mathcal{C}_1 \subset \mathcal{C}_2$ and $\mathcal{C} \subset \mathcal{D}$. Next we prove the order of $f(x)$ in Theorem 3 is $4n$. Under the assumptions, the polynomial $f(x)$ is

$$\begin{aligned} f(x) &= \frac{g_1(x)g_5(x)g_6(x)}{g_2(x)g_7(x)g_8(x)} \\ &= \frac{\prod_{t=0}^{e} M_t(x)^{p^s-\varepsilon_{1,t}} \hat{M}_t(-x)^{p^s-\delta_{1,t}} \hat{M}_t(ax)^{p^s-\varepsilon_{5,t}} \hat{M}_t(-ax)^{p^s-\varepsilon_{6,t}}}{\prod_{t=0}^{e} M_t(x)^{p^s-\varepsilon_{2,t}} \hat{M}_t(-x)^{p^s-\delta_{2,t}} \hat{M}_t(ax)^{p^s-\varepsilon_{7,t}} \hat{M}_t(-ax)^{p^s-\varepsilon_{8,t}}} \\ &= \prod_{t=0}^{e} [M_t(x)^{\varepsilon_{1,t}-\varepsilon_{2,t}} \hat{M}_t(-x)^{\delta_{1,t}-\delta_{2,t}} \times \hat{M}_t(ax)^{\varepsilon_{7,t}-\varepsilon_{5,t}} \hat{M}_t(-ax)^{\varepsilon_{8,t}-\varepsilon_{6,t}}]. \end{aligned}$$

Pick an integer v in the range $0 \leqslant v \leqslant e$ satisfying $\varepsilon_{7,v} - \varepsilon_{5,v} > p^{s-1}$ or $\varepsilon_{8,v} - \varepsilon_{6,v} > p^{s-1}$, then $\mathrm{ord}(f(x))$ has a factor $p^s \cdot \mathrm{ord}(\hat{M}_v(ax))$. It is easily known that $\mathrm{ord}(\hat{M}_v(ax)) = 4l$. We have $\mathrm{ord}(f(x)) \geqslant 4lp^s$. There is also $\mathrm{ord}(f(x)) \leqslant 4lp^s$, so we get $\mathrm{ord}(f(x)) = 4lp^s$. Finally, $\mathcal{C}_r$ has dimension

$$\begin{aligned} k_r &= 2lp^s - (\sum_{t=1}^{e}(p^s - \varepsilon_{r,t} + p^s - \delta_{r,t})w \\ &\quad + (p^s - \varepsilon_{r,0} + p^s - \delta_{r,0})) \\ &= \sum_{t=1}^{e}(\varepsilon_{r,t} + \delta_{r,t})w + (\varepsilon_{r,0} + \delta_{r,0}). \end{aligned}$$

Similarly, $\mathcal{C}$ and $\mathcal{D}$ have dimensions

$$\begin{aligned} k_{\mathcal{C}} &= \sum_{t=1}^{e}(\varepsilon_{5,t} + \varepsilon_{6,t})w + (\varepsilon_{5,0} + \varepsilon_{6,0}), \\ k_{\mathcal{D}} &= \sum_{t=1}^{e}(\varepsilon_{7,t} + \varepsilon_{8,t})w + (\varepsilon_{7,0} + \varepsilon_{8,0}), \end{aligned}$$

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 $\gcd(l, q-1) = l$. *Assume that $\mathcal{C}_1 = \langle g_1(x)\rangle$, $\mathcal{C}_2 = \langle g_2(x)\rangle$ are cyclic codes of length $2lp^s$. $\mathcal{C}_5 = \langle g_5(x)\rangle$, $\mathcal{C}_7 = \langle g_7(x)\rangle$ are λ-constacyclic codes of length lp^s with $\lambda = \xi^{\frac{p^m-1}{4}}$. $\mathcal{C}_6 = \langle g_6(x)\rangle$, $\mathcal{C}_8 = \langle g_8(x)\rangle$ are $-\lambda$-constacyclic codes of length lp^s. Then cyclic code $\mathcal{C}_r$ has a generator polynomial $g_r(x) = g_{r1}(x)g_{r2}(x)$ for $r \in \{1, 2\}$, where*

$$\begin{aligned} g_{r1}(x) &= (x-1)^{p^s-\varepsilon_{r,0}} \prod_{t=1}^{\frac{l-1}{2}} (x-\zeta^t)^{p^s-\varepsilon_{r,t}} (x-\zeta^{-t})^{p^s-\varepsilon_{r,-t}}, \\ g_{r2}(x) &= (x+1)^{p^s-\delta_{r,0}} \prod_{t=1}^{\frac{l-1}{2}} (x+\zeta^t)^{p^s-\delta_{r,t}} (x+\zeta^{-t})^{p^s-\delta_{r,-t}}, \end{aligned} \tag{19}$$

with $\frac{p^s}{2} \leqslant \varepsilon_{1,0}, \varepsilon_{2,0} \leqslant p^s$, $\frac{p^s}{2} \leqslant \delta_{1,0}, \delta_{2,0} \leqslant p^s$, $p^s \leqslant \varepsilon_{r,t} + \varepsilon_{r,-t}, \delta_{r,t} + \delta_{r,-t} \leqslant 2p^s$ for $1 \leqslant t \leqslant \frac{l-1}{2}$. Furthermore, constacyclic codes $\mathcal{C}_i$, $\mathcal{C}_j$ for $i \in \{5, 7\}$ and $j \in \{6, 8\}$ have generator polynomials

$$\begin{aligned} g_i(x) &= (x-b^{-1})^{p^s-\varepsilon_{i,0}} \prod_{t=1}^{\frac{l-1}{2}} (x-b^{-1}\zeta^t)^{p^s-\varepsilon_{i,t}} \\ &\quad \times (x-b^{-1}\zeta^{-t})^{p^s-\varepsilon_{i,-t}}, \quad i \in \{5, 7\}, \\ g_j(x) &= (x+b^{-1})^{p^s-\varepsilon_{j,0}} \prod_{t=1}^{\frac{l-1}{2}} (x+b^{-1}\zeta^t)^{p^s-\varepsilon_{j,t}} \\ &\quad \times (x+b^{-1}\zeta^{-t})^{p^s-\varepsilon_{j,-t}}, \quad j \in \{6, 8\}, \end{aligned} \tag{20}$$

respectively with $\frac{p^s}{2} \leqslant \varepsilon_{i,t}, \varepsilon_{j,t} \leqslant p^s$ and $p^s \leqslant \varepsilon_{i,t} + \varepsilon_{i,-t}, \varepsilon_{j,t} + \varepsilon_{j,-t} \leqslant 2p^s$ for $0 \leqslant t \leqslant e$, where $b^{lp^s}\lambda = 1$. Assume that

$$\begin{aligned} &\varepsilon_{1,0} \leqslant \varepsilon_{2,0}, \quad \varepsilon_{1,t} \leqslant \varepsilon_{2,t}, \ \varepsilon_{1,-t} \leqslant \varepsilon_{2,-t}, \\ &\varepsilon_{5,0} \leqslant \varepsilon_{7,0}, \quad \varepsilon_{5,t} \leqslant \varepsilon_{7,t}, \ \varepsilon_{6,t} \leqslant \varepsilon_{8,t}, \\ &\delta_{1,0} \leqslant \delta_{2,0}, \quad \delta_{1,t} \leqslant \delta_{2,t}, \ \delta_{1,-t} \leqslant \delta_{2,-t}, \\ &\varepsilon_{6,0} \leqslant \varepsilon_{8,0}, \quad \varepsilon_{5,-t} \leqslant \varepsilon_{7,-t}, \ \varepsilon_{6,-t} \leqslant \varepsilon_{8,-t}, \end{aligned} \tag{21}$$

for $1 \leqslant t \leqslant \frac{l-1}{2}$. If there exists an integer v in the range $-\frac{l-1}{2} \leqslant v \leqslant \frac{l-1}{2}$ such that $\varepsilon_{7,v} - \varepsilon_{5,v} > p^{s-1}$ or $\varepsilon_{8,v} - \varepsilon_{6,v} > p^{s-1}$, then for any pair of nonnegative integers a_l, a_r such that $a_l + a_r < 4lp^s$, we can construct an $(a_l, a_r) - [[4lp^s + a_l + a_r, k]]$ quantum synchronizable code where

$$\begin{aligned} k = 2(&\sum_{t=-\frac{l-1}{2}}^{\frac{l-1}{2}} (\varepsilon_{1,t} + \delta_{1,t} + \varepsilon_{1,-t} + \delta_{1,-t} + \varepsilon_{5,t} + \varepsilon_{6,t} \\ &+ \varepsilon_{5,-t} + \varepsilon_{6,-t})w + (\varepsilon_{1,0} + \delta_{1,0} + \varepsilon_{5,0} + \varepsilon_{6,0}) - 2lp^s). \end{aligned}$$

Proof: Note that $\frac{q-1}{l}$ is even, so $\lambda = \xi^{\frac{p^m-1}{4}} \in \langle \xi^l \rangle$. 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 $x^{4p^s} + 1 = (x^{2p^s} - \lambda)(x^{2p^s} + \lambda)$ with $\lambda = \xi^{\frac{p^m-1}{4}}$. Dinh [13] has discussed the generator polynomial of constacyclic codes of length $2p^s$. Divide the elements of $\mathbb{F}_q^*$ into two disjoint subsets $A_{odd} \cup A_{even}$, where

$$A_{odd} = \{\xi^i | 1 \leqslant i \leqslant p^m - 1, \ i \text{ is odd}\},$$

and

$$A_{even} = \{\xi^i | 1 \leqslant i \leqslant p^m - 1, \ i \text{ is even}\}.$$

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

Lemma 3 [13]: Suppose that $\mathcal{C} = \langle g(x)\rangle \subset \frac{\mathbb{F}_q[x]}{\langle x^{p^s}-\lambda\rangle}$ is a λ -constacyclic code of length $2p^s$. Then one of the following two cases holds:
(I). If $\lambda \in A_{even}$, then there exists a nonzero element $\theta_0 \in \mathbb{F}_q^*$ such that ${\theta_0}^{2p^s} = \lambda^{-1}$ and $\mathcal{C}$ is the ideal $\langle (\theta_0 x - 1)^i (\theta_0 x + 1)^j \rangle \subset \frac{F_q[x]}{\langle x^{2p^s}-\lambda\rangle}$, where $0 \leqslant i, j \leqslant p^s$.
(II). If $\lambda \in A_{odd}$, then there exists a nonzero element $\theta_1 \in \mathbb{F}_q^*$ such that ${\theta_1}^{p^s} = -\lambda$. $\mathcal{C}$ is the ideal $\langle (x^2 + \theta_1)^i \rangle \subset \frac{F_q[x]}{\langle x^{2p^s}-\lambda\rangle}$, where $0 \leqslant i \leqslant p^s$.

Now we give Theorem 7 on constructing quantum synchronizable codes from constacyclic codes of length $2p^s$.

Theorem 7: Assume that $\mathcal{C}_1 = \langle g_1(x)\rangle$, $\mathcal{C}_2 = \langle g_2(x)\rangle$ are cyclic codes of length $4p^s$. $\mathcal{C}_5 = \langle g_5(x)\rangle$, $\mathcal{C}_7 = \langle g_7(x)\rangle$ are λ-constacyclic codes of length $2p^s$ with $\lambda = \xi^{\frac{p^m-1}{4}}$. $\mathcal{C}_6 = \langle g_6(x)\rangle$, $\mathcal{C}_8 = \langle g_8(x)\rangle$ are $-\lambda$-constacyclic codes of length $2p^s$. Then the generator polynomial of cyclic code $\mathcal{C}_r$ for $r \in \{1, 2\}$ is

$$\begin{aligned} g_r(x) = (x-1)^{p^s-\varepsilon_{r,1}} &(x+1)^{p^s-\varepsilon_{r,2}} (x-\lambda)^{p^s-\delta_{r,1}} \\ &\times (x+\lambda)^{p^s-\delta_{r,2}}, \quad r \in \{1, 2\}. \end{aligned} \tag{22}$$

The generator polynomials of $\mathcal{C}_i$, $\mathcal{C}_j$, $i \in \{5,7\}$ 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 $\mathcal{C}_i$, $\mathcal{C}_j$ have generator polynomials

$$\begin{aligned} g_i(x) &= (\theta_0 x - 1)^{p^s-\varepsilon_{i,1}}(\theta_0 x + 1)^{p^s-\varepsilon_{i,2}}, \quad i \in \{5,7\}, \\ g_j(x) &= (\theta_0{}^{-1} x - 1)^{p^s-\varepsilon_{j,1}}(\theta_0{}^{-1} x + 1)^{p^s-\varepsilon_{j,2}}, \quad j \in \{6,8\}, \end{aligned} \tag{23}$$

respectively with $\theta_0{}^{2p^s} = \lambda^{-1}$, where $\frac{p^s}{2} \leqslant \varepsilon_{i,t}, \varepsilon_{j,t} \leqslant p^s$ for $t \in \{1,2\}$. Assume that $\varepsilon_{5,t} \leqslant \varepsilon_{7,t}$, $\varepsilon_{6,t} \leqslant \varepsilon_{8,t}$ for $t \in \{1,2\}$. If there exists an integer $v \in \{1,2\}$ such that $\varepsilon_{7,v} - \varepsilon_{5,v} > p^{s-1}$ or $\varepsilon_{8,v} - \varepsilon_{6,v} > p^{s-1}$, then for any pair of nonnegative integers a_l, a_r such that $a_l + a_r < 8p^s$, we can construct an $(a_l, a_r) - [[8p^s + a_l + a_r, k]]$ quantum synchronizable code where $k = 2(\sum_{t=1}^{2}(\varepsilon_{1,t} + \delta_{1,t} + \varepsilon_{5,t} + \varepsilon_{6,t}) - 4p^s)$.
(II). If $p \equiv 5 \bmod 8$ (m is odd), then $\mathcal{C}_i$, $\mathcal{C}_j$ have generator polynomials

$$\begin{aligned} g_i(x) &= (x^2 + \theta_1)^{p^s-\varepsilon_i}, \quad i \in \{5,7\}, \\ g_j(x) &= (x^2 + \theta_1{}^{-1})^{p^s-\varepsilon_j}, \quad j \in \{6,8\}, \end{aligned} \tag{24}$$

respectively with $\theta_1{}^{p^s} = -\lambda$, where $\frac{p^s}{2} \leqslant \varepsilon_i, \varepsilon_j \leqslant p^s$. Assume that $\varepsilon_5 \leqslant \varepsilon_7$, $\varepsilon_6 \leqslant \varepsilon_8$. If there exists an integer $v \in \{1,2\}$ such that $\varepsilon_{7,v} - \varepsilon_{5,v} > p^{s-1}$ or $\varepsilon_{8,v} - \varepsilon_{6,v} > p^{s-1}$, then for any pair of nonnegative integers a_l, a_r such that $a_l + a_r < 8p^s$, we can construct an $(a_l, a_r) - [[8p^s + a_l + a_r, k]]$ quantum synchronizable code where $k = 2(\sum_{t=1}^{2}(\varepsilon_{1,t} + \delta_{1,t}) + (\varepsilon_5 + \varepsilon_6) - 4p^s)$.

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 even), and $\lambda \in A_{odd}$ if $p \equiv 5 \bmod 8$ (m is odd). We can get the generator polynomials of λ-constacyclic codes by Lemma 3. There does not exist λ-constacyclic codes of length $2p^s$ 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 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]

$$\begin{aligned} \varphi_a : \frac{\mathbb{F}_q[x]}{\langle x^{lp^s} - 1\rangle} &\to \frac{\mathbb{F}_q[x]}{\langle x^{lp^s} - \lambda\rangle}, \\ f(x) &\mapsto f(ax), \end{aligned} \tag{25}$$

where a is a nonzero element of $\mathbb{F}_q^*$. Therefore, the minimum distances of lp^s-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^s-length cyclic codes. Define a set of corresponding simple-root l-length λ-constacyclic codes $\{\overline{\mathcal{C}}_{i,v} | 0 \leqslant v \leqslant p^s - 1\}$ with the generator polynomial

$$\bar{g}_{i,v}(x) = \prod_{t=0}^{e} \hat{M}_t(ax)^{f_{v,\varepsilon_{i,t}}}, \tag{26}$$

where $f_{v,\varepsilon_{i,t}} = \begin{cases} 1, & \text{if } p^s - \varepsilon_{i,t} > v, \\ 0, & \text{otherwise.} \end{cases}$ Denote by P_v the Hamming weight of the polynomial $(x-1)^v$ and $P_v = \prod_{u=0}^{s-1}(v_u + 1)$, where $v = \sum_{u=0}^{s-1} v_u p^u$ for $0 \leqslant v_u \leqslant p-1$ and $0 \leqslant u \leqslant s-1$. Define the set [14]

$$\begin{aligned} V = \{v = \sum_{\mu=1}^{u-1}(p-1)p^{s-\mu} + \tau p^{s-\mu-1} | 1 \leqslant u \leqslant s, \\ 1 \leqslant \tau \leqslant p-1\} \cup \{0\}. \end{aligned} \tag{27}$$

Then the minimum distance $d(\mathcal{C}_i)$ of λ-constacyclic code $\mathcal{C}_i$ can be computed by

$$d(\mathcal{C}_i) = \min\{P_v \cdot d(\overline{\mathcal{C}}_{i,v}) | v \in V\}, \tag{28}$$

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

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

From the above, we take $3p^s$-length constacyclic codes as an example. Let $l = 3$ be a prime distinct from p and $\gcd(l, q-1) = 1$. Then we have $p^m \equiv 2 \pmod 3$. Due to (25) we can construct a $\mathbb{F}_q$-algebra isomorphism $\varphi_\theta : \frac{\mathbb{F}_q[x]}{\langle x^{3p^s}-1\rangle} \to \frac{\mathbb{F}_q[x]}{\langle x^{3p^s}-\lambda\rangle}$ that maps $f(x)$ to $f(\theta x)$, where $\theta \in \mathbb{F}_q^*$ such that $\theta^{3p^s}\lambda = 1$ [15]. When $l = 3$ and $p^m \equiv 2 \pmod 3$, $3p^s$-length cyclic code has a generator polynomial $g(x) = (x-1)^{p^s-i_1}(x^2 + x + 1)^{p^s-i_2}$ for $0 \leqslant i_1, i_2 \leqslant p^s$. According to the map φ_θ, the generator polynomials of $\mathcal{C}_i$, $\mathcal{C}_j$ are

$$\begin{aligned} g_i(x) &= (x+a)^{p^s-\varepsilon_{i,1}}(x^2 - ax + a^2)^{p^s-\varepsilon_{i,2}}, \quad i \in \{5,7\}, \\ g_j(x) &= (x-a)^{p^s-\varepsilon_{j,1}}(x^2 + ax + a^2)^{p^s-\varepsilon_{j,2}}, \quad j \in \{6,8\}, \end{aligned} \tag{29}$$

TABLE 1. The minimum distance of an lp^s-length constacyclic code $C_i = \langle \prod_{t=0}^{e} \hat{M}_t(ax)^{p^s-\varepsilon_{i,t}} \rangle$ with $0 \leqslant \varepsilon_{i,t} \leqslant p^s$ for $0 \leqslant t \leqslant e$.

Case	$\varepsilon_{\min}$	$\varepsilon_{\max}$	Minimum distances
1	$0 \leqslant \varepsilon_{\min} \leqslant p^{s-1}$	$0 \leqslant \varepsilon_{\max} \leqslant p^{s-1}$	2
2	$0 \leqslant \varepsilon_{\min} \leqslant p^{s-1}$	$\beta p^{s-1} \leqslant \varepsilon_{\max} \leqslant (\beta+1)\, p^{s-1}$	$\min\{2d', \beta+2\}$
3	$0 \leqslant \varepsilon_{\min} \leqslant p^{s-1}$	$p^s - p^{s-\mu} + (\tau-1)p^{s-\mu-1} \leqslant \varepsilon_{\max} \leqslant p^s - p^{s-\mu} + \tau p^{s-\mu-1}$	$\min\{2d', (\tau+1)\, p^{\mu}\}$
4	$\beta_1 p^{s-1} \leqslant \varepsilon_{\min} \leqslant (\beta_1+1)\, p^{s-1}$	$\beta_2 p^{s-1} \leqslant \varepsilon_{\max} \leqslant (\beta_2+1)\, p^{s-1}$	$\min\{(\beta_1+2)\, d', \beta_2+2\}$
5	$\beta p^{s-1} \leqslant \varepsilon_{\min} \leqslant (\beta+1)\, p^{s-1}$	$p^s - p^{s-\mu} + (\tau-1)p^{s-\mu-1} \leqslant \varepsilon_{\max} \leqslant p^s - p^{s-\mu} + \tau p^{s-\mu-1}$	$\min\{(\beta+2)\, d', (\tau+1)\, p^{\mu}\}$
6	$p^s - p^{s-\mu_1} + (\tau_1-1)p^{s-\mu_1-1} \leqslant \varepsilon_{\min} \leqslant p^s - p^{s-\mu_1} + \tau_1 p^{s-\mu_1-1}$	$p^s - p^{s-\mu_2} + (\tau_2-1)p^{s-\mu_2-1} \leqslant \varepsilon_{\max} \leqslant p^s - p^{s-\mu_2} + \tau_2 p^{s-\mu_2-1}$	$\min\{(\tau_1+1)\, p^{\mu_1} d', (\tau_2+1)\, p^{\mu_2}\}$
7	$0 \leqslant \varepsilon_{\min} \leqslant p^{s-1}$	p^s	$2d'$
8	$\beta p^{s-1} \leqslant \varepsilon_{\min} \leqslant (\beta+1)\, p^{s-1}$	p^s	$(\beta+2)\, d'$
9	$p^s - p^{s-\mu} + (\tau-1)p^{s-\mu-1} \leqslant \varepsilon_{\min} \leqslant p^s - p^{s-\mu} + \tau p^{s-\mu-1}$	p^s	$(\tau+1)\, p^{\mu} d'$

respectively with $\frac{p^s}{2} \leqslant \varepsilon_{i,1}, \varepsilon_{i,2}, \varepsilon_{j,1}, \varepsilon_{j,2} \leqslant p^s$. The minimum distances of $\overline{\mathcal{C}}_{i,v}$ and $\overline{\mathcal{C}}_{j,v}$ are given as follows

$$d(\overline{\mathcal{C}}_{i,v}) = \begin{cases} 1, & \text{if } p^s - \varepsilon_{i,1} \leqslant v,\ p^s - \varepsilon_{i,2} \leqslant v \\ 2, & \text{if } p^s - \varepsilon_{i,1} > v,\ p^s - \varepsilon_{i,2} \leqslant v \\ 3, & \text{if } p^s - \varepsilon_{i,1} \leqslant v,\ p^s - \varepsilon_{i,2} > v \\ \infty, & \text{if } p^s - \varepsilon_{i,1} > v,\ p^s - \varepsilon_{i,2} > v, \end{cases} \tag{30}$$

$$d(\overline{\mathcal{C}}_{j,v}) = \begin{cases} 1, & \text{if } p^s - \varepsilon_{j,1} \leqslant v,\ p^s - \varepsilon_{j,2} \leqslant v \\ 2, & \text{if } p^s - \varepsilon_{j,1} > v,\ p^s - \varepsilon_{j,2} \leqslant v \\ 3, & \text{if } p^s - \varepsilon_{j,1} \leqslant v,\ p^s - \varepsilon_{j,2} > v \\ \infty, & \text{if } p^s - \varepsilon_{j,1} > v,\ p^s - \varepsilon_{j,2} > v. \end{cases} \tag{31}$$

Assume that $p^s - \varepsilon_{i,1} < p^s - \varepsilon_{i,2}$ and $p^s - \varepsilon_{j,1} < p^s - \varepsilon_{j,2}$, then there exsits an element $v' \in V$ such that $d(\overline{\mathcal{C}}_{i,v'}) = 3$ and $P_{v'} = \min\{P_v | v \in V, p^s - \varepsilon_{i,1} \leqslant v < p^s - \varepsilon_{i,2}\}$. We also can find an element $v_1{}' \in V$ such that $d(\overline{\mathcal{C}}_{j,v_1'}) = 3$. Table 2 lists sample parameters for constacyclic codes $\mathcal{C}_i$, $\mathcal{C}_j$ and negacyclic code $\mathcal{C}_i \curlyvee \mathcal{C}_j$ based on the $(\lambda(u+v)|u-v)$ construction.

Suppose that $\mathcal{C}_r$ is a $6p^s$-length cyclic code with a generator polynomial

$$g_r(x) = (x-1)^{p^s-\varepsilon_{r,1}}(x+1)^{p^s-\varepsilon_{r,2}}(x^2+x+1)^{p^s-\delta_{r,1}} \times (x^2-x+1)^{p^s-\delta_{r,2}}, \quad r \in \{1,2\}. \tag{32}$$

The minimum distance of a $6p^s$-length cyclic code be computed using the strategies in [8]. Then the $12p^s$-length cyclic code $\mathcal{C}_r \curlyvee (\mathcal{C}_i \curlyvee \mathcal{C}_j)$ can be determined. We list some parameters in Table 3.

TABLE 2. Sample parameters for $3p^s$-length constacyclic codes $\mathcal{C}_i$, $\mathcal{C}_j$ and a $6p^s$-length negacyclic code $\mathcal{C}_i \curlyvee \mathcal{C}_j$ with $i \in \{5, 7\}$ and $j \in \{6, 8\}$.

Case	p	s	$\varepsilon_{i,1}$	$\varepsilon_{i,2}$	$\varepsilon_{j,1}$	$\varepsilon_{j,2}$	n_{ij}[a]	d_i	d_j	d_{ij}[b]	k_{ij}[c]
1	5	2	23	13	21	12	150	4	4	4	94
2	7	3	172	171	200	172	2058	5	5	5	1058
3	11	2	64	61	80	65	726	7	7	7	396
4	17	2	216	144	144	110	1734	10	12	12	868
5	19	2	270	181	305	288	2166	11	5	10	1513

[a] n_{ij} denotes the length of negacyclic code $\mathcal{C}_i \curlyvee \mathcal{C}_j$.
[b] d_{ij} denotes the minimum distance of negacyclic code $\mathcal{C}_i \curlyvee \mathcal{C}_j$.
[c] k_{ij} denotes the dimension of negacyclic code $\mathcal{C}_i \curlyvee \mathcal{C}_j$.

TABLE 3. Sample parameters for a $12p^s$-length cyclic code $\mathcal{C}_r \curlyvee (\mathcal{C}_i \curlyvee \mathcal{C}_j)$ with $r \in \{1, 2\}$, $i \in \{5, 7\}$ and $j \in \{6, 8\}$.

Case	p	s	n[a]	d_i	d_j	d_r	k_{ij}	k_r	d[b]	k[c]
1	5	2	300	4	4	3	94	125	4	219
2	7	3	4116	5	5	5	1058	1109	5	2167
3	11	2	1452	7	7	5	396	563	7	959
4	17	2	3468	10	12	12	868	1084	12	1952
5	19	2	4332	11	5	11	1513	1487	11	3000

[a] n denotes the length of $\mathcal{C}_r \curlyvee (\mathcal{C}_i \curlyvee \mathcal{C}_j)$.
[b] d denotes the minimum distance of $\mathcal{C}_r \curlyvee (\mathcal{C}_i \curlyvee \mathcal{C}_j)$.
[c] k denotes the dimension of $\mathcal{C}_r \curlyvee (\mathcal{C}_i \curlyvee \mathcal{C}_j)$.

We can know that the constacyclic codes and cyclic codes in Table 3 meet the conditions of Theorem 5(II). According to Theorem 5(II), the quantum synchronizable codes from constacyclic codes and cyclic codes with the parameters in Table 3 reach maximum tolerance against misalignment. According to the sample parameters in Table 2 and 3, we can

TABLE 4. Sample parameters for p-ary projective geometry codes.

Case	p	Length	Dimension	Minimum distance
1	5	781	654	5
2	7	2801	2590	7
3	11	1464	1177	10
4	17	5220	4609	17
5	19	7240	5909	19

TABLE 5. Sample parameters for a $12p^s$-length cyclic code $\mathcal{C}_r \curlyvee (\mathcal{C}_i \curlyvee \mathcal{C}_j)$ with $r \in \{1, 2\}$, $i \in \{5, 7\}$ and $j \in \{6, 8\}$.

Case	p	n	Dimension	Correcting bit errors	Correcting phase errors
1	5	300	138	1	2
2	7	4116	218	2	2
3	11	1452	466	3	3
4	17	3468	578	5	4
5	19	4332	1668	5	5

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 $\mathcal{C}_r \curlyvee (\mathcal{C}_i \curlyvee \mathcal{C}_j)$ has 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 $(a_l, a_r) - [[1452 + a_l + a_r, 466]]$ quantum synchronizable code $\mathcal{Q}_1$. $\mathcal{Q}_1$ can correct at least up 3 bit errors. Besides, we can construct an $(a_l, a_r) - [[1464 + a_l + a_r, 890]]$ quantum synchronizable code $\mathcal{Q}_2$ from a projective geometry code [5], [16] with the parameters of case 3 in Table 4. $\mathcal{Q}_2$ also reach maximum tolerance against misalignment. And $\mathcal{Q}_2$ can corrects at least up to 1 bit errors.

Comparing $\mathcal{Q}_1$ with $\mathcal{Q}_2$, we can see that $\mathcal{Q}_1$ from cyclic codes and constacyclic codes can correct more bit errors than $\mathcal{Q}_2$ from a projective geometry code over the same base fields of close lengths. In other words, although both of $\mathcal{Q}_1$ and $\mathcal{Q}_2$ 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 $(a_l, a_r) - [[3468 + a_l + a_r, 436]]$ quantum synchronizable code $\mathcal{Q}_3$. $\mathcal{Q}_3$ can correct at least up 5 bit errors and 5 phase errors. However, an $(a_l, a_r) - [[5220 + a_l + a_r, 4609]]$ quantum synchronizable code $\mathcal{Q}_4$ 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^s 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 supercodes," *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. Process.*, vol. 18, no. 9, p. 277, Sep. 2019.

[10] G. Hughes, "Constacyclic codes, cocycles and a u+vlu−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 $F_{pm}+uF_{pm}$," *J. Algebra*, vol. 324, no. 5, pp. 940–950, 2010.

[12] B. Chen, Q. D. Hai, and H. Liu, "Repeated-root constacyclic codes of length ℓp^s and their duals," *Discrete Appl. Math.*, vol. 177, pp. 60–70, Nov. 2014.

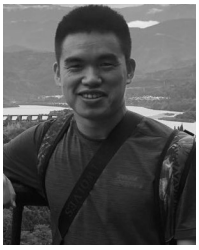
[13] H. Q. Dinh, "Repeated-root constacyclic codes of length $2p^s$," *Finite Fields Their Appl.*, vol. 18, no. 1, pp. 133–143, 2012.

[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 are 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, Synergetic 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.

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.