# Two New Families of Quantum Synchronizable Codes 

Lan Luo • Zhi Ma • Dongdai Lin

Received: date / Accepted: date


#### Abstract

In this paper, we present two new ways of quantum synchronization coding based on the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction and the product construction respectively, and greatly enrich the varieties of available quantum synchronizable codes. The circumstances where the maximum synchronization error tolerance can be reached are explained for both constructions. Furthermore, repeated-root cyclic codes derived from the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction are shown to be able to provide better Pauli error-correcting capability than BCH codes.


Keywords Quantum synchronizable codes $\cdot(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction . Product construction • Minimum distances

## 1 Introduction

Block synchronization (or frame synchronization) is a critical problem in virtually any area in classical digital communications to ensure that the information transmitted can be correctly decoded by the receiver. To achieve this goal, existing classical synchronization techniques commonly require that the information receiver or processing device constantly monitors the data to exactly identify the inserted boundary signals of an information block (see Refs. [1,2] for the basics of block synchronization techniques in classical digital communications). Quantum block synchronization is also significant because the block

[^0]structure is typically used in quantum information coding [3,4] as in classical domain and procedures for manipulating it demand precise alignment [5-7]. However, since measurement of qubits usually destroys their contained quantum information, quantum analogues of above methods don't apply.

Aiming at this problem, Fujiwara [7] proposed a solution-quantum synchronizable error-correcting codes, which allow us to eliminate the effects caused by block misalignment and Pauli errors. In his scheme, the construction of good quantum synchronizable codes demands a pair of nested dualcontaining cyclic codes, both of which guarantee large minimum distances. Later, authors of Ref. [8] improved the original result by widening the range of tolerable magnitude of misalignment and presented several quantum synchronizable codes from classical BCH codes and punctured Reed-Muller (RM) codes. After that, finite geometric codes [9], quadratic residue codes [10], duadic codes [11] and repeated-root codes $[12,13]$ etc., were shown to be applicable in synchronization coding. However, apart from the case with repeatedroot cyclic codes, code parameters of other available quantum synchronizable codes are strongly limited [13]. Besides, the difficulty in computing the exact minimum distances of cyclic codes keeps us away from an accurate estimate on the error-correcting capability against Pauli errors of the obtained quantum codes.

In this work, we provide two new ways of constructing quantum synchronizable codes. The first method exploits the well-known $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction on cyclic codes and negacyclic codes to generate new cyclic codes with twice the lengths. Two circumstances where the obtained quantum codes can achieve the maximum synchronization error tolerance are provided. In particular, repeated-root cyclic codes are shown to be able to provide better performance in correcting Pauli errors than non-primitive, narrow-sense BCH codes. The second method exploits the product construction to produce new cyclic codes from two cyclic codes with coprime lengths. With a broad range of cyclic codes as ingredients, the varieties of quantum synchronizable codes are greatly extended using cyclic product codes. Furthermore, the obtained codes can also reach the best attainable tolerance against misalignment under certain circumstances.

The rest of this paper is organized as follows: First we describe the general formalism of quantum synchronization coding in Section 2. Then we build quantum synchronizable codes based upon the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction in Section 3.1. Two circumstances where the obtained quantum codes reach the maximum synchronization error tolerance are elaborated with repeatedroot codes in Section 3.2. Afterwards, we discuss the minimum distances of above repeated-root codes in Section 3.3. In Section 4, we produce quantum synchronizable codes from cyclic product codes. Finally, we give concluding remarks in Section 5.

## 2 Preliminaries

In this section, we give a brief review of quantum synchronization coding. To start with, we describe some basic facts in classical and quantum coding theory. For further details, the readers can refer to Refs. [3,14].

Let $\mathbb{F}_{q}$ be a finite field where $q=p^{m}$ is a prime power. A classical $[n, k, d]$ linear code $C$ over $\mathbb{F}_{q}$ is a $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$ such that $\min \{\mathrm{wt}(\boldsymbol{c})$ : $\boldsymbol{c} \in C \backslash\{\mathbf{0}\}\}=d$, where $\mathrm{wt}(\boldsymbol{c})$ denotes the number of non-zero coordinates of a codeword $\boldsymbol{c}$. $C$ can be determined as the null space of an $(n-k) \times k$ paritycheck matrix $H$, i.e., $C=\left\{\boldsymbol{c} \in \mathbb{F}_{q}^{n}: H \boldsymbol{c}^{\top}=\mathbf{0}\right\}$. Accordingly, there exists a $k \times n$ generator matrix $G$ with its row space corresponding to $C$ such that $H G^{\boldsymbol{T}}=\mathbf{0}$. The dual code $C^{\perp}:=\left\{\boldsymbol{c}^{\prime} \in \mathbb{F}_{q}^{n}: \boldsymbol{c c}^{\prime \boldsymbol{\top}}=0, \forall \boldsymbol{c} \in C\right\}$ is an $[n, n-k]$ code with a generator matrix $H$ and a parity-check matrix $G$. If $C \subset C^{\perp}$, we call $C$ a self-orthogonal code. Otherwise if $C^{\perp} \subset C, C$ is a dual-containing code.

A classical linear code $C$ is (nega)cyclic if it remains unchanged under a (nega)cyclic shifting of the coordinates, i.e., for a codeword $\boldsymbol{c}=\left(c_{0}, c_{1}, \ldots, c_{n-1}\right) \in$ $C$, a cyclic shift $\left(c_{n-1}, c_{0}, \ldots, c_{n-2}\right)$ (a negacyclic shift $\left(-c_{n-1}, c_{0}, \ldots, c_{n-2}\right)$ ) is also a codeword of $C$. Especially, repeated-root (nega)cyclic codes [15-20] are those whose lengths are divisible by the characteristic $p$ of $\mathbb{F}_{q}$. Identify each codeword $\boldsymbol{c}$ as the coefficient vector of a polynomial $c(x)=\sum_{i=0}^{n-1} c_{i} x^{i}$. Then an $[n, k]$ (nega)cyclic code $C$ is equivalent with an ideal $\langle g(x)\rangle$ in the quotient ring $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}-1\right\rangle}\left(\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}+1\right\rangle}\right)$. We call the monic polynomial $g(x)$ of degree $n-k$ as the generator polynomial of $C$. If the value $\frac{q-1}{\operatorname{gcd}(n, q-1)}$ is even, there exists an isomorphism $\phi$ between the quotient rings $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}-1\right\rangle}$ and $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}+1\right\rangle}$ that maps $g(x)$ to $g(\lambda x)$ [16], where $\lambda^{n}=-1$. Define the parity-check polynomial $h(x)$ of a (nega)cyclic code $C$ as $h(x)=\frac{x^{n}-1}{g(x)}\left(h(x)=\frac{x^{n}+1}{g(x)}\right)$. Accordingly, the dual (nega)cyclic code $C^{\perp}$ has a generator polynomial $g^{\perp}(x)=h^{*}(x)$, where $h^{*}(x)=h_{0}^{-1} x^{\operatorname{deg}(h(x))} h\left(\frac{1}{x}\right)$ represents the monic reciprocal polynomial of $h(x)$.

An $[[n, k, d]]$ quantum code $\mathcal{Q}$ is a $q^{k}$-dimensional subspace of a $q^{n}$-dimensional Hilbert space $\left(C^{q}\right)^{\otimes n}$. Typically, $Q$ is designed to correct the errors caused by Pauli operators $X_{\boldsymbol{\alpha}} Z_{\boldsymbol{\beta}}$ of weight less than $\left\lfloor\frac{d-1}{2}\right\rfloor$, where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{F}_{q}^{n}$. An $\left(a_{l}, a_{r}\right)-[[n, k]]$ quantum synchronizable code is a quantum code that corrects not only Pauli errors, but also block misalignment to the left by $a_{l}$ qudits ( $q$-ary quantum systems) and to the right by $a_{r}$ qudits for some non-negative integers $a_{l}$ and $a_{r}$. Denote the order of a polynomial $f(x)$ with $f(0) \neq 0$ by $\operatorname{ord}(f(x))$, i.e., $\operatorname{ord}(f(x))=\left|\left\{x^{a}(\bmod f(x)): a \in \mathbb{N}\right\}\right|$. We give the quantum synchronization coding framework as follows.

Theorem 1 [12, 13] Let $C$ be a dual-containing $\left[n, k_{C}, d_{C}\right]$ cyclic code and $D$ be an $\left[n, k_{D}, d_{D}\right]$ cyclic code such that $C \subset D$. Denote by $g_{C}(x)$ and $g_{D}(x)$ the generator polynomials of $C$ and $D$ respectively. Define the polynomial $f(x)$ of degree $k_{D}-k_{C}$ to be the quotient of $g_{C}(x)$ divided by $g_{D}(x)$. Then for any pair $a_{l}, a_{r}$ of non-negative integers satisfying $a_{l}+a_{r}<\operatorname{ord}(f(x))$, there exists
an $\left(a_{l}, a_{r}\right)-\left[\left[n, 2 k_{C}-n\right]\right]$ quantum synchronizable code that can correct up to $\left\lfloor\frac{d_{D}-1}{2}\right\rfloor$ bit errors and $\left\lfloor\frac{d_{C}-1}{2}\right\rfloor$ phase errors.

We can tell from Theorem 1 that a valid construction of good quantum synchronizable codes relies on a pair of dual-containing cyclic codes, one of which is contained in the other and both guarantee large minimum distances. Furthermore, the obtained synchronizable code can correct synchronization errors (or misalignment) up to $\operatorname{ord}(f(x))$ qubits. If $\operatorname{ord}(f(x))=n$, then the quantum synchronizable code achieves the maximum synchronization error tolerance.

## 3 The $(u+v \mid u-v)$ construction

### 3.1 Synchronization coding

In this section, we describe the quantum synchronization coding based upon the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction. Compared with the well-known $(\boldsymbol{u} \mid \boldsymbol{u}+\boldsymbol{v})$ method-an iterative way to define RM codes, the ( $\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ technique has several advantages [21,22]. Apart from an estimate of minimum distances never worse than the other case, the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ scheme enables us to obtain a $2 n$-length cyclic code from an $n$-length cyclic code and an $n$-length negacyclic code.

To be specific, let $C_{1}$ and $C_{2}$ be $\left[n, k_{1}, d_{1}\right]$ and $\left[n, k_{2}, d_{2}\right]$ linear codes over $\mathbb{F}_{q}$ respectively, where $q=p^{m}$ is an odd prime power. (In this section, we leave the case with $p=2$ out of consideration.) 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. The $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction $C=C_{1} \curlyvee C_{2}=\left\{(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v}): \boldsymbol{u} \in C_{1}, \boldsymbol{v} \in C_{2}\right\}$ [21, $23]$ is a $\left[2 n, k_{1}+k_{2}, \min \left\{2 d_{1}, 2 d_{2}, \max \left\{d_{1}, d_{2}\right\}\right\}\right]$ code with a generator matrix

$$
G_{C}=\left(\begin{array}{cc}
G_{1} & G_{1}  \tag{1}\\
G_{2} & -G_{2}
\end{array}\right)
$$

Suppose that $C_{1}$ is cyclic with a generator polynomial $g_{1}(x)$ and $C_{2}$ is negacyclic with a generator polynomial $g_{2}(x)$, then $C$ is cyclic with a generator polynomial $g(x)=g_{1}(x) g_{2}(x)$ [21]. Clearly, $C$ is dual-containing if both $C_{1}$ and $C_{2}$ are dual-containing. Applying these properties to Theorem 1, we can build a family of quantum synchronizable codes from cyclic codes and negacyclic codes as follows.
Theorem 2 Let $C_{i}$ be an $\left[n, k_{i}, d_{i}\right]$ dual-containing code for $i \in\{1,2,3,4\}$. Suppose that $C_{1}, C_{3}$ are cyclic with respective generator polynomial $g_{1}(x), g_{3}(x)$ and $C_{2}, C_{4}$ are negacyclic with respective generator polynomial $g_{2}(x), g_{4}(x)$. If $C_{1} \subset C_{3}$ and $C_{2} \subset C_{4}$, define $f(x)=\frac{g_{1}(x) g_{2}(x)}{g_{3}(x) g_{4}(x)}$. Then for any pair of non-negative integers $a_{l}, a_{r}$ such that $a_{l}+a_{r}<\operatorname{ord}(f(x))$, there exists an $\left(a_{l}, a_{r}\right)-\left[\left[2 n, 2\left(k_{1}+k_{2}-n\right)\right]\right]$ quantum synchronizable code that can correct up to $\left\lfloor\frac{\min \left\{2 d_{3}, 2 d_{4}, \max \left\{d_{3}, d_{4}\right\}\right\}-1}{2}\right\rfloor$ bit errors and $\left\lfloor\frac{\min \left\{2 d_{1}, 2 d_{2}, \max \left\{d_{1}, d_{2}\right\}\right\}-1}{2}\right\rfloor$ phase errors.

Proof It is clear that $C=C_{1} \curlyvee C_{2}$ is a $\left[2 n, k_{1}+k_{2}, \min \left\{2 d_{1}, 2 d_{2}, \max \left\{d_{1}, d_{2}\right\}\right\}\right]$ cyclic code with a generator polynomial $g_{C}(x)=g_{1}(x) g_{2}(x)$ and $D=C_{3} \curlyvee$ $C_{4}$ is a $\left[2 n, k_{3}+k_{4}, \min \left\{2 d_{3}, 2 d_{4}, \max \left\{d_{3}, d_{4}\right\}\right\}\right]$ cyclic code with generator polynomial $g_{D}(x)=g_{3}(x) g_{4}(x)$. Furthermore, the condition $C \subset D$ holds because $C_{1} \subset C_{3}$ and $C_{2} \subset C_{4}$. By applying $C$ and $D$ to Theorem 1, we can then obtain the required quantum synchronizable codes.

Different from Theorem 1, Theorem 2 calls for two pairs of nested dualcontaining classical codes in quantum synchronization coding, one of which are cyclic and the other are negacyclic. All of these codes need to guarantee large minimum distances, and are desired to make as large ord $(f(x))$ as possible to offer better synchronization recovery capability. In particular, the maximum tolerable magnitude of misalignment is $2 n$. In that case, the quantum synchronizable codes from Theorem 2 can correct misalignment by up to $a_{l}$ qubits to the left and $a_{r}$ qubits to the right provided that $a_{l}+a_{r}<2 n$.

### 3.2 Maximum synchronization error tolerance

Under two circumstances could the maximum synchronization error tolerance $2 n$ be achieved, one of which is that $\operatorname{ord}\left(\frac{g_{1}(x)}{g_{3}(x)}\right)=n$ and $\operatorname{ord}\left(\frac{g_{2}(x)}{g_{4}(x)}\right)=2$ where $\operatorname{gcd}(n, 2)=1$, and the other is that $\operatorname{ord}\left(\frac{g_{2}(x)}{g_{4}(x)}\right)=2 n$ whatever the value of $\operatorname{ord}\left(\frac{g_{1}(x)}{g_{3}(x)}\right)$ is.

### 3.2.1 The first circumstance

The condition $\operatorname{ord}\left(\frac{g_{1}(x)}{g_{3}(x)}\right)=n$ in the first circumstance has been investigated on nearly all available quantum synchronizable codes, and is applicable to many cyclic codes, e.g., BCH codes [8], punctured RM codes [8], quadratic residue codes [10] and repeated-root cyclic codes [12,13]. The other condition $\operatorname{ord}\left(\frac{g_{2}(x)}{g_{4}(x)}\right)=2$, however, has limited applications subject to the dualcontaining constraint. One feasible solution is to use repeated-root codes of length $p^{s}$, where $s$ is a positive integer.

To be concrete, let $C_{1}, C_{3}$ be $p^{s}$-length dual-containing cyclic codes and $C_{2}, C_{4}$ be $p^{s}$-length dual-containing negacyclic codes. Then $C_{1}, C_{2}, C_{3}, C_{4}$ have generator polynomials [15]

$$
\begin{array}{lc}
g_{i}(x)=(x-1)^{p^{s}-k_{i}}, & i=1,3, \\
g_{j}(x)=(x+1)^{p^{s}-k_{j}}, & j=2,4, \tag{2}
\end{array}
$$

where $\frac{p^{s}}{2} \leq k_{i}, k_{j} \leq p^{s}$. With the help of these codes, we can build a family of quantum synchronizable codes that possess the maximum synchronization error tolerance.

Theorem 3 Let $C_{i}$ be a $\left[p^{s}, k_{i}\right]$ cyclic code and $C_{j}$ be a $\left[p^{s}, k_{j}\right]$ negacyclic code, where $\frac{p^{s}}{2} \leq k_{i}, k_{j} \leq p^{s}$ for $i \in\{1,3\}$ and $j \in\{2,4\}$. Suppose that
$k_{3}-k_{1}>p^{s-1}$ and $k_{4}=k_{2}+1$, then for non-negative integers $a_{l}$ and $a_{r}$ such that $a_{l}+a_{r}<2 p^{s}$, there exists an $\left(a_{l}, a_{r}\right)-\left[\left[2 p^{s}, 2\left(k_{1}+k_{3}-p^{s}\right)\right]\right]$ quantum synchronizable code.

Proof The fact that $C_{1} \subset C_{3}$ and $C_{2} \subset C_{4}$ is evident since $k_{1}<k_{3}$ and $k_{2}<k_{4}$. Furthermore, the order of the polynomial $f(x)=\frac{g_{1}(x) g_{2}(x)}{g_{3}(x) g_{4}(x)}=(x+$ 1) $(x-1)^{k_{3}-k_{1}}$ is $2 p^{s}$. By applying these properties to Theorem 2, we can naturally obtain the quantum synchronizable codes of desired parameters.

### 3.2.2 The second circumstance

Assume that $\frac{q-1}{\operatorname{gcd}(n, q-1)}$ is even, then there exists an isomorphism $\phi$ between the quotient rings $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}-1\right\rangle}$ and $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}+1\right\rangle}$ which maps $c(x)$ to $c(\lambda x)$, where $\lambda^{n}=$ 1 [16]. Furthermore, if the order of $c(x)$ is $n$, the order of $c(\lambda x)$ is $2 n$. Therefore, the condition $\operatorname{ord}\left(\frac{g_{2}(x)}{g_{4}(x)}\right)=2 n$ on negacyclic codes $C_{2}, C_{4}$ can be achieved by finding two suitable cyclic codes. On that condition, most existing quantum synchronizable codes that provide the highest tolerance against synchronization errors can be generalized to quantum synchronizable codes of twice the lengths. As an example, we consider the use of $l p^{s}$-length repeated-root codes where $l$ is a prime distinct from $p$.

We first deal with the case $l \neq 2$. Pick a primitive $l$-th root $\zeta$ of unity in the extension field $\mathbb{F}_{q^{w}}$ with $w=\operatorname{ord}_{l}(q)$ indicating the order of $q$ in $\mathbb{Z}_{l}^{*}$. For $0 \leq t \leq e=\frac{l-1}{w}$, denote by $M_{t}(x)$ the minimal polynomial of $\zeta^{t}$ over $\mathbb{F}_{q}$. The following lemma describes the structures of $l p^{s}$-length cyclic codes and negacyclic codes explicitly.

Lemma 1 [16] Let $C_{1}$ be an lps-length cyclic code with a generator polynomial $g_{1}(x)$ and let $C_{2}$ be an lp $p^{s}$-length negacyclic code with a generator polynomial $g_{2}(x)$.
(I). If $\operatorname{gcd}(l, q-1)=1$, then

$$
\begin{align*}
& g_{1}(x)=\prod_{t=0}^{e}\left(M_{t}(x)\right)^{p^{s}-a_{1, t}} \\
& g_{2}(x)=\prod_{t=0}^{e}\left(\hat{M}_{t}(-x)\right)^{p^{s}-a_{2, t}} \tag{3}
\end{align*}
$$

where $0 \leq a_{1, t}, a_{2, t} \leq p^{s}$ for all $t$. The notation $\hat{M}_{t}(x)$ denotes the monic polynomial of $M_{t}(x)$ dividing its leading coefficient. In particular when $w=$ $\operatorname{ord}_{l}(q)$ is odd, the generator polynomials of $C_{1}$ and $C_{2}$ are given by

$$
\begin{align*}
& g_{1}(x)=(x-1)^{p^{s}-a_{1,0}} \prod_{t=1}^{\frac{e}{2}}\left(M_{t}(x)\right)^{p^{s}-a_{1, t}}\left(M_{-t}(x)\right)^{p^{s}-a_{1,-t}}  \tag{4}\\
& g_{2}(x)=(x+1)^{p^{s}-a_{2,0}} \prod_{t=1}^{\frac{e}{2}}\left(\hat{M}_{t}(-x)\right)^{p^{s}-a_{2, t}}\left(\hat{M}_{-t}(-x)\right)^{p^{s}-a_{2,-t}}
\end{align*}
$$

where $0 \leq a_{1, t}, a_{2, t}, a_{1,-t}, a_{2,-t} \leq p^{s}$ for $0 \leq t \leq \frac{e}{2}$.
Correspondingly, if $w$ is even, the dual codes $C_{1}^{\perp}$ and $C_{2}^{\perp}$ have generator polynomials

$$
\begin{align*}
& g_{1}^{\perp}(x)=\prod_{t=0}^{e}\left(M_{t}(x)\right)^{a_{1, t}},  \tag{5}\\
& g_{2}^{\perp}(x)=\prod_{t=0}^{e}\left(\hat{M}_{t}(-x)\right)^{a_{2, t}},
\end{align*}
$$

respectively. Otherwise if $w$ is odd, the dual codes have respective generator polynomial

$$
\begin{align*}
& g_{1}^{\perp}(x)=(x-1)^{a_{1,0}} \prod_{t==1}^{\frac{e}{2}}\left(M_{t}(x)\right)^{a_{1,-t}}\left(M_{-t}(x)\right)^{a_{1, t}}  \tag{6}\\
& g_{2}^{\perp}(x)=(x+1)^{a_{2,0}} \prod_{t=1}^{\frac{e}{2}}\left(\hat{M}_{t}(-x)\right)^{a_{2,-t}}\left(\hat{M}_{-t}(-x)\right)^{a_{2, t}} .
\end{align*}
$$

(II). If $\operatorname{gcd}(l, q-1)=l$, then we have

$$
\begin{align*}
& g_{1}(x)=(x-1)^{p^{s}-a_{1,0}} \prod_{t=1}^{\frac{l-1}{2}}\left(x-\zeta^{t}\right)^{p^{s}-a_{1, t}}\left(x-\zeta^{-t}\right)^{p^{s}-a_{1,-t}}  \tag{7}\\
& g_{2}(x)=(x+1)^{p^{s}-a_{2,0}} \prod_{t=1}^{\frac{l-1}{2}}\left(x+\zeta^{t}\right)^{p^{s}-a_{2, t}}\left(x+\zeta^{-t}\right)^{p^{s}-a_{2,-t}}
\end{align*}
$$

where $0 \leq a_{1, t}, a_{2, t}, a_{1,-t}, a_{2,-t} \leq p^{s}$ for $0 \leq t \leq \frac{l-1}{2}$. The dual codes $C_{1}^{\perp}$ and $C_{2}^{\perp}$ have generator polynomials

$$
\begin{align*}
& g_{1}^{\perp}(x)=(x-1)^{a_{1,0}} \prod_{t=1}^{\frac{l-1}{2}}\left(x-\zeta^{t}\right)^{a_{1,-t}}\left(x-\zeta^{-t}\right)^{a_{1, t}}  \tag{8}\\
& g_{2}^{\perp}(x)=(x+1)^{a_{2,0}} \prod_{t=1}^{\frac{l-1}{2}}\left(x+\zeta^{t}\right)^{a_{2,-t}}\left(x+\zeta^{-t}\right)^{a_{2, t}}
\end{align*}
$$

respectively.
By applying above codes to Theorem 2, we can build quantum synchronizable codes of length $2 l p^{s}$ as follows.
Theorem 4 Let $l$ be an odd prime such that $\operatorname{gcd}(l, q-1)=1$. Suppose that $C_{1}, C_{3}$ are dual-containing cyclic codes of length $l p^{s}$ and $C_{2}, C_{4}$ are dualcontaining negacyclic codes of length $l p^{s}$.
(I). If $w$ is even, then $C_{i}, C_{j}$ have generator polynomials

$$
\begin{align*}
& g_{i}(x)=\prod_{t=0}^{e}\left(M_{t}(x)\right)^{p^{s}-a_{i, t}}, \quad i \in\{1,3\},  \tag{9}\\
& g_{j}(x)=\prod_{t=0}^{e}\left(\hat{M}_{t}(-x)\right)^{p^{s}-a_{j, t}}, \quad j \in\{2,4\},
\end{align*}
$$

respectively, where $\frac{p^{s}}{2} \leq a_{i, t}, a_{j, t} \leq p^{s}$ for $0 \leq t \leq e$. Assume that $a_{1, t} \leq$ $a_{3, t}$ and $a_{2, t} \leq a_{4, t}$ for all $t$. If there exists an integer $r$ in the range $0 \leq r \leq e$ such that $\operatorname{gcd}(r, l)=1$ and $a_{4, r}-a_{2, r}>p^{s-1}$, then we can construct an $\left(a_{l}, a_{r}\right)-\left[\left[2 l p^{s}, k\right]\right]$ quantum synchronizable code where

$$
\begin{equation*}
k=2\left(\sum_{t=1}^{e}\left(a_{1, t}+a_{2, t}\right) w+\left(a_{1,0}+a_{2,0}\right)-l p^{s}\right) . \tag{10}
\end{equation*}
$$

(II). If $w$ is odd, then $C_{i}$ and $C_{j}$ have generator polynomials

$$
\begin{align*}
& g_{i}(x)=(x-1)^{p^{s}-a_{i, 0}} \prod_{t=1}^{\frac{e}{2}}\left(M_{t}(x)\right)^{p^{s}-a_{i, t}}\left(M_{-t}(x)\right)^{p^{s}-a_{i,-t}}, \quad i \in\{1,3\}, \\
& g_{j}(x)=(x+1)^{p^{s}-a_{j, 0}} \prod_{t=1}^{\frac{e}{e}}\left(\hat{M}_{t}(-x)\right)^{p^{s}-a_{j, t}}\left(\hat{M}_{-t}(-x)\right)^{p^{s}-a_{j,-t}}, \quad j \in\{2,4\}, \tag{11}
\end{align*}
$$

respectively, where $\frac{p^{s}}{2} \leq a_{i, 0}, a_{j, 0} \leq p^{s}$ and $p^{s} \leq a_{i, t}+a_{i,-t}, a_{j, t}+a_{j,-t} \leq$ $2 p^{s}$ for $1 \leq t \leq \frac{e}{2}$. Assume that

$$
\begin{align*}
& a_{1,0} \leq a_{3,0}, \quad a_{2,0} \leq a_{4,0} \\
& a_{1, t} \leq a_{3, t}, \quad a_{2, t} \leq a_{4, t}  \tag{12}\\
& a_{1,-t} \leq a_{3,-t}, a_{2,-t} \leq a_{4,-t}
\end{align*}
$$

for $1 \leq t \leq \frac{e}{2}$. If there exists an integer $r$ in the range $-\frac{e}{2} \leq r \leq \frac{e}{2}$ such that $\operatorname{gcd}(r, l)=1$ and $a_{4, r}-a_{2, r}>p^{s-1}$, then for any non-negative integers $a_{l}, a_{r}$ satisfying $a_{l}+a_{r}<2 l p^{s}$, we can obtain an $\left(a_{l}, a_{r}\right)-\left[\left[2 l p^{s}, k\right]\right]$ quantum synchronizable code where

$$
\begin{equation*}
k=2\left(\sum_{1 \leq t \leq \frac{e}{2}}\left(a_{1, t}+a_{1,-t}+a_{2, t}+a_{2,-t}\right) w+\left(a_{1,0}+a_{2,0}\right)-l p^{s}\right) . \tag{13}
\end{equation*}
$$

Proof Given an even $w$, the dual-containing properties of $C_{i}$ and $C_{j}$, for $i \in$ $\{1,3\}$ and $j \in\{2,4\}$, are guaranteed when the parameters $a_{i, t}, a_{j, t}$ are in the range $\frac{p^{s}}{2} \leq a_{i, t}, a_{j, t} \leq p^{s}$ for all $t$. Furthermore, due to the assumption that $a_{1, t} \leq a_{3, t}$ and $a_{2, t} \leq a_{4, t}$ for $0 \leq t \leq e$, we have $C_{1} \subset C_{3}$ and $C_{2} \subset C_{4}$. In that case, the polynomial $f(x)$ in Theorem 2 is

$$
\begin{align*}
f(x) & =\frac{g_{1}(x) g_{2}(x)}{g_{3}(x) g_{4}(x)}=\frac{\prod_{t=0}^{e}\left(M_{t}(x)\right)^{p^{s}-a_{1, t}}\left(\hat{M}_{t}(-x)\right)^{p^{s}-a_{2, t}}}{\prod_{t=0}^{e}\left(M_{t}(x)\right)^{p^{3}-a_{3, t}\left(\hat{M}_{t}(-x)\right)^{p}-a_{4, t}}}  \tag{14}\\
& =\prod_{t=0}^{e}\left(M_{t}(x)\right)^{a_{3, t}-a_{1, t}}\left(\hat{M}_{t}(-x)\right)^{a_{4, t}-a_{2, t}}
\end{align*}
$$

Pick an integer $r$ that is relatively prime to $l$ such that $a_{4, r}-a_{2, r}>p^{s-1}$, then the order of $f(x)$ has a factor $p^{s} \cdot \operatorname{ord}\left(\hat{M}_{r}(-x)\right)$. Note that $\operatorname{ord}\left(\hat{M}_{r}(x)\right)=$ $\frac{l}{\operatorname{gcd}(r, l)}=l$. Hence we have $\operatorname{ord}\left(\hat{M}_{r}(-x)\right)=2 l$, indicating that $\operatorname{ord}(f(x)) \geq$ $2 l p^{s}$. Due to the fact that $\operatorname{ord}(f(x)) \leq 2 l p^{s}$, we can finally obtain that $\operatorname{ord}(f(x))=$ $2 l p^{s}$. Moreover, $C_{i}$ has dimension

$$
\begin{equation*}
k_{i}=l p^{s}-\left(\left(p^{s}-a_{i, 0}\right)+\sum_{t=1}^{e}\left(p^{s}-a_{i, t}\right) w\right)=a_{i, 0}+\sum_{t=1}^{e} a_{i, t} \cdot w \tag{15}
\end{equation*}
$$

And analogously, $C_{j}$ has dimension $k_{j}=a_{j, 0}+\sum_{t=1}^{e} a_{j, t} \cdot w$. Therefore, the quantum synchronizable code built on them has the desired parameters. For an odd $w$, the statements in (II) can be verified using similar arguments.

Theorem 5 Let $l$ be an odd prime such that $g c d(l, q-1)=l$. Suppose that $C_{1}, C_{3}$ are dual-containing cyclic codes of length lps and $C_{2}, C_{4}$ are dualcontaining negacyclic codes of length $l p^{s}$. The generator polynomials of $C_{i}, C_{j}$ for $i \in\{1,3\}$ and $j \in\{2,4\}$ are

$$
\begin{align*}
& g_{i}(x)=(x-1)^{p^{s}-a_{i, 0}} \prod_{t=1}^{\frac{l-1}{2}}\left(x-\zeta^{t}\right)^{p^{s}-a_{i, t}}\left(x-\zeta^{-t}\right)^{p^{s}-a_{i,-t}}  \tag{16}\\
& g_{j}(x)=(x+1)^{p^{s}-a_{j, 0}} \prod_{t=1}^{\frac{l-1}{2}}\left(x+\zeta^{t}\right)^{p^{s}-a_{j, t}}\left(x+\zeta^{-t}\right)^{p^{s}-a_{j,-t}}
\end{align*}
$$

respectively, where $\frac{p^{s}}{2} \leq a_{i, 0}, a_{j, 0} \leq p^{s}$ and $p^{s} \leq a_{i, t}+a_{i,-t}, a_{j, t}+a_{j,-t} \leq 2 p^{s}$ for $1 \leq t \leq \frac{l-1}{2}$. Assume that

$$
\begin{align*}
& a_{1,0} \leq a_{3,0}, \quad a_{2,0} \leq a_{4,0} \\
& a_{1, t} \leq a_{3, t}, \quad a_{2, t} \leq a_{4, t}  \tag{17}\\
& a_{1,-t} \leq a_{3,-t}, \\
& a_{2,-t} \leq a_{4,-t},
\end{align*}
$$

for $1 \leq t \leq \frac{l-1}{2}$. If we can pick an integer $r$ with $-\frac{l-1}{2} \leq r \leq \frac{l-1}{2}$ such that $\operatorname{gcd}(r, l)=1$ and $a_{4, r}-a_{2, r}>p^{s-1}$, then given a pair of non-negative integers $a_{l}, a_{r}$ satisfying $a_{l}+a_{r}<2 l p^{s}$, there exists a quantum synchronizable code of length $2 l p^{s}$ and dimension

$$
\begin{equation*}
k=2\left(\left(a_{1,0}+a_{2,0}\right)+\sum_{t=1}^{\frac{l-1}{2}}\left(a_{1, t}+a_{1,-t}+a_{2, t}+a_{2,-t}\right)-l p^{s}\right) . \tag{18}
\end{equation*}
$$

Proof Following a similar proof to that of Theorem 4, we can obtain the desired results.

In the case of $l=2$, quantum synchronizable codes that possess the maximum synchronization error tolerance can also be constructed from $l p^{s}$-length cyclic codes and negacyclic codes. The following lemma describes the structures of $2 p^{s}$-length repeated-root codes clearly.

Lemma 2 [16] Let $C_{1}$ be a cyclic code of length $2 p^{s}$. Then $C_{1}$ and its dual code $C_{1}^{\perp}$ have respective generator polynomial

$$
\begin{align*}
& g_{1}(x)=(x-1)^{p^{s}-a_{1,0}}(x+1)^{p^{s}-a_{1,1}}  \tag{19}\\
& g_{1}^{\perp}(x)=(x-1)^{a_{1,0}}(x+1)^{a_{1,1}}
\end{align*}
$$

where $0 \leq a_{1,0}, a_{1,1} \leq p^{s}$.
Let $C_{2}$ be a negacyclic code of length $2 p^{s}$. If $q \equiv 1(\bmod 4)$, there exists an element $\eta \in \mathbb{F}_{q}^{*}$ such that $\eta^{2}=-1$. In that case, $C_{2}$ and $C_{2}^{\perp}$ have generator polynomials

$$
\begin{align*}
& g_{2}(x)=(x-\eta)^{p^{s}-a_{2,0}}(x+\eta)^{p^{s}-a_{2,1}}  \tag{20}\\
& g_{2}^{\perp}(x)=(x-\eta)^{a_{2,1}}(x+\eta)^{a_{2,0}}
\end{align*}
$$

respectively, where $0 \leq a_{2,0}, a_{2,1} \leq p^{s}$. Otherwise if $q \equiv 3(\bmod 4)$, their generator polynomials are given by

$$
\begin{align*}
& g_{2}(x)=\left(x^{2}+1\right)^{p^{s}-a_{2}},  \tag{21}\\
& g_{2}^{\perp}(x)=\left(x^{2}+1\right)^{a_{2}}
\end{align*}
$$

where $0 \leq a_{2} \leq p^{s}$.
Taking similar arguments to the proof of Theorem 4, we can obtain the following results.

Theorem 6 Suppose that $C_{1}, C_{3}$ are dual-containing cyclic codes of length $2 p^{s}$ and $C_{2}, C_{4}$ are dual-containing negacyclic codes of length $2 p^{s}$.
(I). If $q \equiv 1(\bmod 4)$, the generator polynomials of $C_{1}, C_{2}, C_{3}, C_{4}$ are of the forms

$$
\begin{align*}
& g_{i}(x)=(x-1)^{p^{s}-a_{i, 0}}(x+1)^{p^{s}-a_{i, 1}}, i \in\{1,3\}, \\
& g_{j}(x)=(x-\eta)^{p^{s}-a_{j, 0}}(x+\eta)^{p^{s}-a_{j, 1}}, j \in\{2,4\} \tag{22}
\end{align*}
$$

where $\frac{p^{s}}{2} \leq a_{i, 0}, a_{i, 1} \leq p^{s}$ and $p^{s} \leq a_{j, 0}+a_{j, 1} \leq 2 p^{s}$. The notation $\eta$ denotes the element in $\mathbb{F}_{q}^{*}$ such that $\eta^{2}=-1$. Assume that

$$
\begin{align*}
& a_{1,0} \leq a_{3,0}, a_{1,1} \leq a_{3,1},  \tag{23}\\
& a_{2,0} \leq a_{4,0}, a_{2,1} \leq a_{4,1}
\end{align*}
$$

If either $a_{4,0}-a_{2,0}>p^{s-1}$ or $a_{4,1}-a_{2,1}>p^{s-1}$ holds, then for any nonnegative pair $a_{l}, a_{r}$ satisfying $a_{l}+a_{r}<4 p^{s}$, we can build an $\left(a_{l}, a_{r}\right)-$ [ $\left.\left[4 p^{s}, k\right]\right]$ quantum synchronizable code, where

$$
\begin{equation*}
k=2\left(a_{1,0}+a_{1,1}+a_{2,0}+a_{2,1}-2 p^{s}\right) . \tag{24}
\end{equation*}
$$

(II). If $q \equiv 3(\bmod 4)$, the generator polynomials of $C_{1}, C_{2}, C_{3}, C_{4}$ are given by

$$
\begin{array}{ll}
g_{i}(x)=(x-1)^{p^{s}-a_{i, 0}}(x+1)^{p^{s}-a_{i, 1}}, & i \in\{1,3\},  \tag{25}\\
g_{j}(x)=\left(x^{2}+1\right)^{p^{s}-a_{j}}, & j \in\{2,4\},
\end{array}
$$

where $\frac{p^{s}}{2} \leq a_{i, 0}, a_{i, 2}, a_{j} \leq p^{s}$. Assume that $a_{1,0} \leq a_{3,0}, a_{1,1} \leq a_{3,1}$ and $a_{2} \leq a_{4}$. If $a_{4}-a_{2}>p^{s-1}$, then for any non-negative integers $a_{l}, a_{r}$ such that $a_{l}+a_{r}<4 p^{s}$, there exists an $\left(a_{l}, a_{r}\right)-\left[\left[4 p^{s}, k\right]\right]$ quantum synchronizable code, where

$$
\begin{equation*}
k=2\left(a_{1,0}+a_{1,1}+2 a_{2}-2 p^{s}\right) . \tag{26}
\end{equation*}
$$

We can tell from Theorems 4, 5 and 6 that quantum synchronizable codes of length $2 l p^{s}$ that reach the maximum synchronization error tolerance can be derived from cyclic codes and negacyclic codes of length $l p^{s}$. This can be seen as a generalization of results in Ref. [13], where $l p^{s}$-length cyclic codes are exploited in the construction of $l p^{s}$-length quantum synchronizable codes that tolerate misalignment by $l p^{s}$ qubits. Similar generalizations can be applied to other existing quantum synchronizable codes of length $n$ due to the isomorphism $\phi$ between $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}-1\right\rangle}$ and $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{n}+1\right\rangle}[16]$ that maps $c(x)$ to $c(\lambda x)$ where $\lambda^{n}=-1$, when $\frac{q-1}{\operatorname{gcd}(n, q-1)}$ is even.

### 3.3 The minimum distances

From Theorem 2 we can see that, quantum synchronizable codes derived from cyclic codes $C_{1} \curlyvee C_{2}$ and $C_{3} \curlyvee C_{4}$ have minimum distances no worse or up to twice larger than those from the component cyclic codes $C_{1}$ and $C_{3}$. In other words, quantum synchronizable codes based on the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ scheme can provide good performance in correcting Pauli errors. Take the codes from Theorem 4 (I) for an example.

Suppose that $l$ is an odd prime such that $\operatorname{gcd}(l, q-1)$. If $w$ is even, then an $l p^{s}$-length cyclic code $C_{i}$ and an $l p^{s}$-length negacyclic code $C_{j}$, for $i \in\{1,3\}$ and $j \in\{2,4\}$, have respective generator polynomial

$$
\begin{align*}
g_{i}(x) & =\prod_{t=0}^{e}\left(M_{t}(x)\right)^{p^{s}-a_{i, t}}  \tag{27}\\
g_{j}(x) & =\prod_{t=0}^{e}\left(\hat{M}_{t}(-x)\right)^{p^{s}-a_{j, t}}
\end{align*}
$$

Table 1 The minimum distance of an $l p^{s}$-length negacyclic code $C_{j}=$ $\left\langle\prod_{t=0}^{e}\left(\hat{M}_{t}(-x)\right)^{p^{s}-a_{j, t}}\right\rangle$ with $0 \leq a_{j, t} \leq p^{s}$ for $0 \leq t \leq e$ and $j \in\{2,4\}$.

| Case | $b_{\text {min }}^{\dagger}$ | $b_{\text {max }}$ | minimum distance |
| :---: | :---: | :---: | :---: |
| 1 | (0, $\left.p^{s-1}\right]$ | (0, $\left.p^{s-1}\right]$ | 2 |
| 2 | $\left(0, p^{s-1}\right]$ | $\left(\beta^{\star} p^{s-1},(\beta+1) p^{s-1}\right]$ | $\min \left\{2 d^{\prime \ddagger}, \beta+2\right\}$ |
| 3 | (0, $p^{s-1}$ ] | $\left(p^{s}-p^{s-\mu}+(\tau-\right.$ 1) $p^{s-\mu-1}, p^{s}-p^{s-\mu}+$ $\left.\tau p^{s-\mu-1}\right]$ | $\min \left\{2 d^{\prime},(\tau+1) p^{\mu}\right\}$ |
| 4 | $\left(\beta_{0} p^{s-1},\left(\beta_{0}+1\right) p^{s-1}\right]$ | $\left(\beta_{1} p^{s-1},\left(\beta_{1}+1\right) p^{s-1}\right]$ | $\min \left\{\left(\beta_{0}+2\right) d^{\prime}, \beta_{1}+2\right\}$ |
| 5 | $\left(\beta p^{s-1},(\beta+1) p^{s-1}\right]$ | ${ }^{\left(p^{s}-p^{s-\mu}+(\tau-\right.}$ 1) $p^{s-\mu-1}, p^{s}-p^{s-\mu}+$ $\left.\tau p^{s-\mu-1}\right]$ | $\min \left\{(\beta+2) d^{\prime},(\tau+1) p^{\mu}\right\}$ |
| 6 | $\begin{gathered} \left(p^{s}-p^{s-\mu_{0}}+\left(\tau_{0}-\right.\right. \\ 1) p^{s-\mu_{0}-1}, p^{s}- \\ \left.p^{s-u_{0}}+\tau_{0} p^{s-\mu_{0}-1}\right] \end{gathered}$ | $\begin{gathered} \left(p^{s}-p^{s-\mu_{1}}+\left(\tau_{1}-\right.\right. \\ 1) p^{s-\mu_{1}-1}, p^{s}- \\ \left.p^{s-\mu_{1}}+\tau_{1} p^{s-\mu_{1}-1}\right] \end{gathered}$ | $\begin{gathered} \min \left\{\left(\tau_{0}+\right.\right. \\ \mu_{0} d_{\left.d^{\prime},\left(\tau_{1}+1\right) p^{\mu_{1}}\right\}} \end{gathered}$ |
| 7 | (0, $p^{s-1}$ ] | $p^{s}$ | $2 d^{\prime}$ |
| 8 | $\left(\beta p^{s-1},(\beta+1) p^{s-1}\right]$ | $p^{s}$ | $(\beta+2) d^{\prime}$ |
| 9 | ${ }^{\left(p^{s}-p^{s-\mu}+(\tau-\right.}$ 1) $p^{s-\mu-1}, p^{s}-p^{s-\mu}+$ $\left.\tau p^{s-\mu-1}\right]$ | $p^{s}$ | $(\tau+1) p^{\mu} d^{\prime}$ |

${ }^{\dagger}$ The notations $b_{\min }$ and $b_{\max }$ denote the minimum and maximum elements in the set
$\left\{p^{s}-a_{j, t}: 0 \leq t \leq e\right\}$, respectively.
${ }^{*}$ The parameters are in the ranges $1 \leq \beta, \beta_{0}, \beta_{1} \leq p-2,1 \leq \mu, \mu_{0}, \mu_{1} \leq s-1$ and
$1 \leq \tau, \tau_{0}, \tau_{1} \leq p-1$.
$\frac{d^{\prime}}{}$ denotes the minimum distance of $\bar{C}_{j, v^{\prime}}$ where $P_{v^{\prime}}=\min \left\{P_{v}: b_{\min } \leq v<b_{\max }, v \in\right.$ $V\}$.
where $0 \leq a_{i, t}, a_{j, t} \leq p^{s}$ for all $t$. The minimum distance of $C_{i}$ has been thoroughly investigated in Ref. [13]. Due to the isomorphism $\phi$ between $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{l} p^{s}-1\right\rangle}$ and $\frac{\mathbb{F}_{q}[x]}{\left\langle x^{p^{x}}+1\right\rangle}$ that maps $c(x)$ to $c(-x)$, the minimum distance of the negacyclic code $C_{j}$ can be computed using the same strategies.

Define a set of $l$-length negacyclic codes $\left\{\bar{C}_{j, v}: 0 \leq v \leq p^{s}-1\right\}$ with respective generator polynomial $\bar{g}_{j, v}(x)=\prod_{t=0}^{e}\left(\hat{M}_{t}(-x)\right)^{f_{v, a_{j, t}}}$, where $f_{v, a_{j, t}}=$ $\left\{\begin{array}{l}1, p^{s}-a_{j, t}>v, \\ 0, \text { otherwise. }\end{array}\right.$ For $0 \leq v \leq p^{s}-1$, denote by $P_{v}$ the Hamming weight of the polynomial $(x-1)^{v}$ [24] and define the set

$$
\begin{equation*}
V=\left\{\sum_{\mu=1}^{u-1}(p-1) p^{s-\mu}+\tau p^{s-u}: 1 \leq u \leq s, 1 \leq \tau \leq p-1\right\} \cup\{0\} \tag{28}
\end{equation*}
$$

The minimum distance of $C_{j}$ is demonstrated in Table 1.
Furthermore, set $l=3$ and $q \equiv 2(\bmod 3)$. Thus a $3 p^{s}$-length negacyclic code $C_{j}$ has a generator polynomial

$$
\begin{equation*}
g_{j}(x)=(x+1)^{p^{s}-a_{j, 0}}\left(x^{2}-x+1\right)^{p^{s}-a_{j, 1}}, \tag{29}
\end{equation*}
$$

Table 2 Sample parameters for an $\left[n_{j}, k_{j}, d_{j}\right]$ negacyclic code $C_{j}=\left\langle(x+1)^{p^{s}-a_{j, 0}}\left(x^{2}-\right.\right.$ $\left.x+1)^{p^{s}-a_{j, 1}}\right\rangle$ with $a_{j, 1}<a_{j, 0}$ for $j \in\{2,4\}$.

| $\boldsymbol{p}$ | $\boldsymbol{s}$ | $n_{\boldsymbol{j}}$ | $\boldsymbol{a}_{\boldsymbol{j}, \mathbf{0}}$ | $\boldsymbol{a}_{\boldsymbol{j}, \mathbf{1}}$ | $k_{\boldsymbol{j}}$ | $\boldsymbol{d}_{\boldsymbol{j}}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 5 | 2 | 75 | 19 | 18 | 55 | 3 |
| 5 | 2 | 75 | 19 | 4 | 27 | 9 |
| 5 | 2 | 75 | 14 | 3 | 20 | 12 |
| 5 | 2 | 75 | 4 | 2 | 8 | 20 |
| 5 | 3 | 375 | 14 | 4 | 22 | 50 |
| 5 | 3 | 375 | 9 | 3 | 15 | 75 |
| 5 | 4 | 1875 | 19 | 4 | 27 | 225 |
| 5 | 4 | 1875 | 9 | 3 | 15 | 375 |
| 11 | 2 | 363 | 109 | 65 | 239 | 7 |
| 11 | 2 | 363 | 21 | 10 | 41 | 33 |
| 11 | 2 | 363 | 10 | 6 | 22 | 66 |
| 11 | 3 | 3993 | 65 | 10 | 85 | 231 |
| 11 | 3 | 3993 | 32 | 9 | 50 | 330 |
| 23 | 2 | 1587 | 459 | 275 | 1009 | 13 |
| 23 | 2 | 1587 | 229 | 22 | 273 | 45 |
| 23 | 2 | 1587 | 45 | 22 | 89 | 69 |
| 23 | 2 | 1587 | 21 | 16 | 53 | 184 |
| 23 | 3 | 36501 | 68 | 21 | 110 | 1518 |
| 23 | 3 | 36501 | 45 | 21 | 87 | 1587 |
|  |  |  |  |  |  |  |

where $0 \leq a_{j, 0}, a_{j, 1} \leq p^{s}$. The $l$-length negacyclic code $\bar{C}_{j, v}$ has minimum distance

$$
d\left(\bar{C}_{j, v}\right)= \begin{cases}1, & \text { if } p^{s}-a_{j, 0} \leq v, p^{s}-a_{j, 1} \leq v  \tag{30}\\ 2, & \text { if } p^{s}-a_{j, 0}>v, p^{s}-a_{j, 1} \leq v \\ 3, & \text { if } p^{s}-a_{j, 0} \leq v, p^{s}-a_{j, 1}>v \\ \infty, & \text { if } p^{s}-a_{j, 0}>v, p^{s}-a_{j, 1}>v\end{cases}
$$

Hence if we assume that $p^{s}-a_{j, 0}<p^{s}-a_{j, 1}$, the minimum distance of $\bar{C}_{j, v^{\prime}}$ is 3 , where $P_{v^{\prime}}=\min \left\{p^{s}-a_{j, 0} \leq v<p^{s}-a_{j, 1}: v \in V\right\}$. On that condition, Table 2 lists sample parameters for $C_{j}$.

Combined with the results of Ref. [13] regarding a $3 p^{s}$-length cyclic code $C_{i}=\left\langle(x-1)^{p^{s}-a_{i, 0}}\left(x^{2}+x+1\right)^{p^{s}-a_{i, 1}}\right\rangle$ with $a_{i, 1}<a_{i, 0}$, the minimum distance of a $6 p^{s}$-length cyclic code $C_{i} \curlyvee C_{j}$ on $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction can thus be determined. Sample parameters are provided in Table 3.

We can tell that in the cases $3,7,8,10,12$ and 13 in Table $3, C_{i} \curlyvee C_{j}$ have minimum distances twice as large as the component cyclic codes $C_{i}$, for $i \in\{1,3\}$ and $j \in\{2,4\}$. As a consequence, the quantum synchronizable codes derived from $C_{i} \curlyvee C_{j}$ can correct Pauli errors of weight twice larger than those constructed from $C_{i}$. In many instances, the former codes also have better error-correcting capability against Pauli errors than the quantum synchronizable codes derived from non-primitive narrow-sense BCH codes [8]. Denote by $\delta$ the precise lower bound $[13,25]$ for the minimum distance of a dual-containing BCH code. Table 4 lists some sample parameters of dualcontaining non-primitive, narrow-sense BCH codes.

Table 3 Sample parameters for an $[n, k, d]$ cyclic code $C_{i} \curlyvee C_{j}$ with $i \in\{1,3\}$ and $j \in\{2,4\}$.

| Case | $\boldsymbol{p}$ | $\boldsymbol{s}$ | $\boldsymbol{n}$ | $\boldsymbol{a}_{\boldsymbol{i}, \mathbf{o}}$ | $\boldsymbol{a}_{\boldsymbol{i}, \boldsymbol{1}}$ | $\boldsymbol{a}_{\boldsymbol{j}, \mathbf{0}}$ | $\boldsymbol{a}_{\boldsymbol{j}, \boldsymbol{1}}$ | $\boldsymbol{d}_{\boldsymbol{i}}^{\dagger}$ | $\boldsymbol{d}_{\boldsymbol{j}}$ | $\boldsymbol{d}$ | $\boldsymbol{k}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 5 | 2 | 150 | 19 | 18 | 19 | 4 | 3 | 9 | 6 | 82 |
| 2 | 5 | 2 | 150 | 19 | 4 | 14 | 3 | 9 | 12 | 12 | 47 |
| 3 | 5 | 2 | 150 | 19 | 4 | 4 | 2 | 9 | 20 | 18 | 35 |
| 4 | 5 | 2 | 150 | 4 | 2 | 14 | 3 | 20 | 12 | 20 | 28 |
| 5 | 5 | 3 | 750 | 14 | 4 | 9 | 3 | 50 | 75 | 75 | 37 |
| 6 | 5 | 4 | 3750 | 19 | 4 | 9 | 3 | 225 | 375 | 375 | 42 |
| 7 | 11 | 2 | 726 | 109 | 65 | 21 | 10 | 7 | 33 | 14 | 280 |
| 8 | 11 | 2 | 726 | 21 | 10 | 10 | 6 | 33 | 66 | 66 | 63 |
| 9 | 11 | 3 | 7986 | 65 | 10 | 32 | 9 | 231 | 330 | 330 | 135 |
| 10 | 23 | 2 | 3174 | 459 | 275 | 229 | 22 | 13 | 45 | 26 | 1282 |
| 11 | 23 | 2 | 3174 | 229 | 22 | 45 | 22 | 45 | 69 | 69 | 362 |
| 12 | 23 | 2 | 3174 | 229 | 22 | 21 | 16 | 45 | 184 | 90 | 326 |
| 13 | 23 | 2 | 3174 | 45 | 22 | 21 | 16 | 69 | 184 | 138 | 142 |

${ }^{\dagger} d_{i}$ and $d_{j}$ denote the minimum distances of $C_{i}$ and $C_{j}$, respectively.

Table 4 Sample parameters for $p$-ary non-primitive, narrow-sense BCH codes.

| Case | $\boldsymbol{p}$ | length | $\boldsymbol{\delta}$ | dimension |
| :---: | :---: | :---: | :---: | :---: |
| 1 | 5 | 146 | 5 | 130 |
| 2 | 5 | 748 | 28 | 638 |
| 3 | 11 | 725 | 60 | 563 |
| 4 | 11 | 7985 | 65 | 7749 |
| 5 | 23 | 3172 | 132 | 2794 |

By the comparison between Tables 3 and 4 we can see that, given the same base field $\mathbb{F}_{p}$, repeated-root cyclic codes $C_{i} \curlyvee C_{j}$, with well-chosen parameters, can possess larger minimum distances than non-primitive, narrow sense BCH codes of close lengths. In particular, over the base fields $\mathbb{F}_{11}$ and $\mathbb{F}_{23}$, repeatedroot cyclic codes $C_{i} \curlyvee C_{j}$ of lengths 726 and 3174, respectively, can reach a larger minimum distance provided that parameters $a_{i, 0}, a_{i, 1}, a_{j, 0}, a_{j, 1}$ are sufficiently small. In that case, quantum sychronizable codes constructed from $C_{i} \curlyvee C_{j}$ have better performance in correcting Pauli errors than those from non-primitive, narrow-sense BCH codes.

## 4 The product construction

Apart from the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ method, the product construction is another useful technique of generating new cyclic codes from old ones. Without loss of generality, we restrict the following discussion to the binary case.

Let $C_{1}$ and $C_{2}$ be linear codes of parameters $\left[n_{1}, k_{1}, d_{1}\right]$ and $\left[n_{2}, k_{2}, d_{2}\right]$ respectively. A product code $C=C_{1} \otimes C_{2}[26]$ is defined to be an $\left[n_{1} n_{2}, k_{1} k_{2}, d_{1} d_{2}\right]$ linear code whose codewords are all the two-dimensional arrays where each row is a codeword in $C_{1}$ and each column is a codeword in $C_{2}$. Denote by $c_{i, j}$ the el-
ement in the $(i+1)^{\text {th }}$ row and $(j+1)^{\text {th }}$ column of the array, where $0 \leq i \leq n_{1}-1$ and $0 \leq j \leq n_{2}-1$. Then a codeword of $C$ can be identified with a bivariate polynomial $c(y, z)=\sum_{i=0}^{n_{1}-1} \sum_{j=0}^{n_{2}-1} c_{i, j} y^{i} z^{j} \in \frac{\mathbb{F}_{2}[x, y]}{\left\langle\left(y^{n_{1}}-1\right)\left(z^{n_{2}}-1\right)\right\rangle}$. According to the Chinese remainder theorem, there exists a unique integer $\theta$ in the range $0 \leq \theta \leq n_{1} n_{2}-1$ such that $\theta \equiv i\left(\bmod n_{1}\right)$ and $\theta \equiv j\left(\bmod n_{2}\right)$, provided that $\operatorname{gcd}\left(n_{1}, n_{2}\right)=1$. In that case, $c(x)=\sum_{\theta=0}^{n_{1} n_{2}-1} c_{\left(\theta\left(\bmod n_{1}\right), \theta\left(\bmod n_{2}\right)\right)} x^{\theta}$ is also a polynomial representation of code $C$.

Suppose that $C_{1}$ and $C_{2}$ are both cyclic. Then $C$ is also cyclic since $x c(x)\left(\bmod x^{n_{1} n_{2}}-1\right)$, which corresponds to $y z c(y, z)\left(\bmod y^{n_{1}}-1\right)\left(\bmod z^{n_{2}}-\right.$ 1 ), is a codeword of $C$. Denote by $g_{1}(x)$ and $g_{2}(x)$ the respective generator polynomial of $C_{1}$ and $C_{2}$. Then $C$ and the dual code $C^{\perp}$ have respective generator polynomial [27]

$$
\begin{align*}
& g_{C}(x)=\operatorname{gcd}\left(g_{1}\left(x^{\beta n_{2}}\right) g_{2}\left(x^{\alpha n_{1}}\right), x^{n_{1} n_{2}}-1\right), \\
& g_{C}^{\perp}(x)=\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{\beta n_{2}}\right), g_{2}^{\perp}\left(x^{\alpha n_{1}}\right)\right), \tag{31}
\end{align*}
$$

where $\alpha, \beta$ are integers satisfying $\alpha n_{1}+\beta n_{2}=1$, and $g_{1}^{\perp}(x)$ and $g_{2}^{\perp}(x)$ represent the respective generator polynomial of $C_{1}^{\perp}$ and $C_{2}^{\perp}$. Clearly, $C$ is selforthogonal if either $C_{1}$ or $C_{2}$ is self-orthogonal. Applying cyclic product codes to Theorem 1, we can then obtain a broad family of quantum synchronizable codes as follows.

Theorem 7 Let $C_{1}=\left\langle g_{1}(x)\right\rangle$ be a self-orthogonal $\left[n_{1}, k_{1}\right]$ cyclic code and $C_{2}=\left\langle g_{2}(x)\right\rangle$ be an $\left[n_{2}, k_{2}\right]$ cyclic code with $\alpha n_{1}+\beta n_{2}=1$, where $\alpha, \beta$ are integers. Suppose that $C_{3}$ is a cyclic code with a generator polynomial $g_{3}(x)=g_{2}(x) \rho(x)$, where $\rho(x)$ is a non-trivial polynomial such that $\rho(0)=1$. Assume that $\operatorname{gcd}\left(g_{3}^{\perp}(x), \rho^{*}(x)\right)=1$ where $\rho^{*}(x)$ denotes the reciprocal polynomial of $\rho(x)$. Then for any non-negative pair $a_{l}, a_{r}$ such that $a_{l}+a_{r}<$ $\operatorname{ord}\left(\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{\beta n_{2}}\right), \rho^{*}\left(x^{\alpha n_{1}}\right)\right)\right)$, there exists an $\left(a_{l}, a_{r}\right)-\left[\left[n_{1} n_{2}, n_{1} n_{2}-2 k_{1} k_{2}\right]\right]$ quantum synchronizable code.

Proof The cyclic product code $D=C_{1} \otimes C_{3}$ and its dual code $D^{\perp}$ have generator polynomials

$$
\begin{align*}
& g_{D}(x)=\operatorname{gcd}\left(g_{1}\left(x^{\beta n_{2}}\right) g_{3}\left(x^{\alpha n_{1}}\right), x^{n_{1} n_{2}}-1\right), \\
& g_{D}^{\perp}(x)=\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{\beta n_{2}}\right), g_{3}^{\perp}\left(x^{\alpha n_{1}}\right)\right), \tag{32}
\end{align*}
$$

respectively. Denote by $C$ the product code of $C_{1}$ and $C_{2}$. Then the dual codes $C^{\perp}$ and $D^{\perp}$ are dual-containing cyclic codes such that $C^{\perp} \subset D^{\perp}$. Note that

$$
\begin{equation*}
g_{2}^{\perp}(x)=\left(\frac{x^{n_{2}}-1}{g_{2}(x)}\right)^{*}=\left(\frac{x^{n_{2}}-1}{g_{3}(x)} \rho(x)\right)^{*}=g_{3}^{\perp}(x) \rho^{*}(x) . \tag{33}
\end{equation*}
$$

Hence the quotient polynomial $f(x)$ of the generator polynomials of $C^{\perp}$ and $D^{\perp}$ is given by
$f(x)=\frac{g_{C}^{\perp}(x)}{g_{D}^{\perp}(x)}=\frac{\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{\beta n_{2}}\right), g_{3}^{\perp}\left(x^{\alpha n_{1}}\right) \rho^{*}\left(x^{\alpha n_{1}}\right)\right)}{\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{\beta n_{2}}\right), g_{3}^{\perp}\left(x^{\alpha n_{1}}\right)\right)}=\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{\beta n_{2}}\right), \rho^{*}\left(x^{\alpha n_{1}}\right)\right)$.

Apply $C^{\perp}$ and $D^{\perp}$ to Theorem 1, we can then obtain the quantum synchronizable code with the desired parameters.

Note that the constraint $\operatorname{gcd}\left(g_{3}^{\perp}(x), \rho^{*}(x)\right)=1$ is equivalent with

$$
\begin{equation*}
\operatorname{gcd}\left(h_{3}^{*}(x), \rho^{*}(x)\right)=\operatorname{gcd}\left(h_{3}(x), \rho(x)\right)=\operatorname{gcd}\left(\frac{h_{2}(x)}{\rho(x)}, \rho(x)\right)=1 \tag{35}
\end{equation*}
$$

where $h_{i}(x)$ denotes the parity check polynomial of $C_{i}$ for $i \in\{2,3\}$. Hence the non-trivial polynomial $\rho(x)$ can always be found, provided that $h_{2}(x)$ has at least two irreducible factors. On that condition, a broad range of $n_{2}$-length cyclic codes can be applied to the construction in Theorem 7, which, accordingly, widen the family of quantum synchronizable codes to a large extent. In particular, the range of parameters' selection for quantum synchronization coding is greatly enlarged considering that lengths of previous quantum synchronizable codes, apart from those built on repeated-root cyclic codes, are of limited forms, e.g., $2^{s}-1[8]$ and $\frac{2^{s t}-1}{2^{s}-1}[9]$, where $s, t$ are positive integers.

Furthermore, the quantum synchronizable codes obtained from cyclic product codes can also reach the maximum synchronization error tolerance if

$$
\begin{equation*}
\operatorname{ord}\left(\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{\beta n_{2}}\right), \rho^{*}\left(x^{\alpha n_{1}}\right)\right)\right)=\operatorname{ord}\left(\operatorname{gcd}\left(h_{1}\left(x^{\beta n_{2}}\right), \rho\left(x^{\alpha n_{1}}\right)\right)\right)=n_{1} n_{2} \tag{36}
\end{equation*}
$$

where $h_{1}\left(x^{\beta n_{2}}\right)=\frac{x^{\beta n_{1} n_{2}}-1}{g_{1}\left(x^{\beta n_{2}}\right)}$. For example, let $C_{1}$ be a $[7,3]$ cyclic code with a generator polynomial

$$
\begin{equation*}
g_{1}(x)=(x+1)\left(x^{3}+x+1\right) . \tag{37}
\end{equation*}
$$

The dual code $C_{1}^{\perp}$ has a generator polynomial $g_{1}^{\perp}(x)=x^{3}+x+1$. Clearly, $C_{1}$ is a self-orthogonal code. Let $C_{2}$ be a $[15,11]$ cyclic code with a generator polynomial

$$
\begin{equation*}
g_{2}(x)=x^{4}+x^{3}+1 . \tag{38}
\end{equation*}
$$

Therefore, $C=C_{1} \otimes C_{2}$ is an $[105,33]$ cyclic code. Note that

$$
\begin{equation*}
h_{2}(x)=(x+1)\left(x^{2}+x+1\right)\left(x^{4}+x+1\right)\left(x^{4}+x^{3}+x^{2}+x+1\right) . \tag{39}
\end{equation*}
$$

By choosing $\rho(x)$ to be $x^{4}+x+1$, we can then obtain a [15, 7] cyclic code $C_{3}$ with a generator polynomial

$$
\begin{equation*}
g_{3}(x)=\left(x^{4}+x^{3}+1\right)\left(x^{4}+x+1\right) \tag{40}
\end{equation*}
$$

In that case, the cyclic product code $D=C_{1} \otimes C_{3}$ is an [105, 21] code.
Since $(-2) \times 7+1 \times 15=1$, we have

$$
\begin{align*}
& g_{1}^{\perp}\left(x^{15}\right)=x^{45}+x^{15}+1, \\
& \rho^{*}\left(x^{-14}\right)=x^{-56}+x^{-42}+1=x^{-56}\left(x^{56}+x^{14}+1\right) . \tag{41}
\end{align*}
$$

Their greatest common divisor is

$$
\begin{equation*}
\operatorname{gcd}\left(g_{1}^{\perp}\left(x^{15}\right), f^{*}\left(x^{-14}\right)\right)=x^{12}+x^{10}+x^{9}+x^{7}+x^{6}+x^{4}+1 \tag{42}
\end{equation*}
$$

which is of order 105. Hence following Theorem 7 , we can build an $[[105,39]]$ quantum synchronizable code that can tolerate misalignment by up to 105 qubits.

## 5 Conclusions

In this paper, we present two families of quantum synchronizable codes from cyclic codes built on the $(\boldsymbol{u}+\boldsymbol{v} \mid \boldsymbol{u}-\boldsymbol{v})$ construction and the product construction. In the former case, most existing quantum synchronizable codes that provide the highest tolerance against synchronization errors can be generalized to larger cases. In particular, repeated-root codes of length $l p^{s}$ have been thoroughly investigated in quantum synchronization coding and can provide a better performance in correcting Pauli errors than non-primitive, narrow-sense BCH codes. In the latter case, the loose restrictions on the component cyclic codes ensure a large augmentation of available quantum synchronizable codes. Besides, their synchronization error tolerance can also reach the maximum under certain circumstances.

## References

1. Bernard Sklar. Digital Communications: Fundamentals and Applications. Prentice Hall, Upper Saddle River, NJ, 2nd edition, 2001.
2. Stefano Bregni. Synchronization of Digital Telecommunications Networks. John Wiley \& Sons, New York, U.S., 2002.
3. Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2010.
4. Daniel A. Lidar and Todd A. Brun. Quantum Error Correction. Cambridge University Press, Cambridge, U.K., 2013.
5. Yuichiro Fujiwara and Vladimir D. Tonchev. High-rate self-synchronizing codes. IEEE Transactions on Information Theory, 59(4):2328-2335, 2013.
6. Yury Polyanskiy. Asynchronous communication: Exact synchronization, universality, and dispersion. IEEE Transactions on Information Theory, 59(3):1256-1270, 2013.
7. Yuichiro Fujiwara. Block synchronization for quantum information. Physical Review A, 87(2):109-120, 2013.
8. Yuichiro Fujiwara, Vladimir D. Tonchev, and Tony W. H. Wong. Algebraic techniques in designing quantum synchronizable codes. Physical Review A, 88(1):162-166, 2013.
9. Yuichiro Fujiwara and Peter Vandendriessche. Quantum synchronizable codes from finite geometries. IEEE Transactions on Information Theory, 60(11):7345-7354, 2014.
10. Yixuan Xie, Jinhong Yuan, and Yuichiro Fujiwara. Quantum synchronizable codes from augmentation of cyclic codes. Plos One, 6(2):e14641, 2014.
11. K. Guenda, G. G. La Guardia, and T. A. Gulliver. Algebraic quantum synchronizable codes. arXiv preprint: https://arxiv.org/abs/1508.05977, 2015.
12. Yixuan Xie, Lei Yang, and Jinhong Yuan. $q$-ary chain-containing quantum synchronizable codes. IEEE Communications Letters, 20(3):414-417, 2016.
13. Lan Luo and Zhi Ma. Non-binary quantum synchronizable codes from repeated-root cyclic codes. IEEE Transactions on Information Theory, 64(3):1461-1470, 2018.
14. Cary W. Huffman and Vera Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, U.K., 2010.
15. Hai Q. Dinh. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. Finite Fields and Their Applications, 14(1):22-40, 2008.
16. Bocong Chen, Hai Q. Dinh, and Hongwei Liu. Repeated-root constacyclic codes of length $l p^{s}$ and their duals. Finite Fields and Their Applications, 177:60-70, 2014.
17. Hai Q. Dinh. Structure of repeated-root constacyclic codes of length $3 p^{s}$ and their duals. Finite Fields and Their Applications, 313:983-991, 2013.
18. Bocong Chen, Hai Q. Dinh, and Hongwei Liu. Repeated-root constacyclic codes of length $2 l^{m} p^{n}$. Finite Fields and Their Applications, 33:137-159, 2015.
19. Hakan Özadam and Ferruh Özbudak. The minimum hamming distance of cyclic codes of length $2 p^{s}$. In International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, pages 92-100. Springer, 2009.
20. Alexander Zeh and Markus Ulmschneider. Decoding of repeated-root cyclic codes up to new bounds on their minimum distance. Problems of Information Transmission, 51(3):217-230, 2015.
21. Garry Hughes. Constacyclic codes, cocycles and a $u+v \mid u-v$ construction. IEEE Transactions on Information Theory, 46(2):674-680, 2000.
22. San Ling and P Sole. On the algebraic structure of quasi-cyclic codes I: Finite fields. IEEE Transactions on Information Theory, 47(7):2751-2760, 2001.
23. Florence Jessie Macwilliams and Neil James Alexander Sloane. The Theory of ErrorCorrecting Codes. North-Holland Publishing Company, 1977.
24. Guy Castagnoli, J. L. Massey, P. A. Schoeller, and Niklaus Von Seemann. On repeatedroot cyclic codes. IEEE Transactions on Information Theory, 37(2):337-342, 1991.
25. Salah A. Aly, A. Klappenecker, and P. K. Sarvepalli. On quantum and classical BCH codes. IEEE Transactions on Information Theory, 53(3):1183-1188, 2007.
26. Richard E. Blahut. Algebraic Codes for Data Transmission. Cambridge University Press, 2003.
27. Shu Lin and Edward Weldon. Further results on cyclic product codes. IEEE Transactions on Information Theory, 16(4):452-459, 1970.

[^0]:    L. Lan

    Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China State Key Laboratory of Information Security, Beijing 100093, China
    Z. Ma

    Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China
    E-mail: ma_zhi@163.com
    D. D. Lin

    State Key Laboratory of Information Security, Beijing 100093, China

