IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 13, 2020, accepted June 27, 2020, date of publication June 30, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006001

Quantum MDS and Synchronizable Codes From Cyclic and Negacyclic Codes of Length $2p^s$ Over $\mathbb{F}_{p^m}$

HAI Q. DINH[1,2], BAC T NGUYEN[3], AND WORAPHON YAMAKA[4]

[1]Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[2]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[3]Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam
[4]Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University, Chiang Mai 52000, Thailand

Corresponding author: Bac T Nguyen (bactienminh2013@gmail.com)

This work was supported in part by the Centre of Excellence in Econometrics, Faculty of Economics, Chiang Mai University.

ABSTRACT Let p be an odd prime, and $\mathbb{F}_{p^m}$ is the finite field of p^m elements. In this paper, all maximum distance separable (briefly, MDS) cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are established. As an application, all quantum MDS (briefly, qMDS) codes are constructed from cyclic and negacyclic codes of length $2p^s$ over finite fields using the Calderbank- Shor-Steane (briefly, CSS) and Hermitian constructions. These codes are new in the sense that their parameters are different from all the previous constructions. Furthermore, quantum synchronizable codes (briefly, QSCs) are obtained from cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. To enrich the variety of available QSCs, many new QSCs are constructed to illustrate our results. Among them, there are QSCs codes with shorter lengths and much larger minimum distances than known primitive narrow-sense Bose–Chaudhuri–Hocquenghem (briefly, BCH) codes.

INDEX TERMS Cyclic codes, repeated-root codes, Hamming distance, MDS codes, quantum MDS codes, quantum synchronizable codes.

I. INTRODUCTION

Let p be a prime number and $\mathbb{F}_{p^m}$ a finite field. An $[n, k]$ linear code C over $\mathbb{F}_{p^m}$ is a k-dimensional subspace of $\mathbb{F}_{p^m}^n$. A linear code C of length n over $\mathbb{F}_{p^m}$ is called a λ-*constacyclic code* if it is an ideal of the quotient ring $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$, where the generator polynomial $g(x)$ is the unique monic polynomial of minimum degree in the code, which is a divisor of $x^n - \lambda$. If $\lambda = 1$, those λ-constacyclic codes are called *cyclic codes*, and when $\lambda = -1$, such λ-constacyclic codes are called *negacyclic codes*. Cyclic and negacyclic codes are interesting from both theoretical and practical perspectives which have been well studied since the late 1960's.

Cyclic codes are the most studied of all codes. Many well-known codes, such as BCH, Kerdock, Golay, Reed-Muller, Preparata, Justesen, and binary Hamming codes, are either cyclic codes or constructed from cyclic codes.

A linear code C is a cyclic code if $\tau(C) = C$, where τ is a cyclic shift defined as $\tau(x_0, x_1, \ldots, x_{n-1}) = (x_{n-1}, x_0, x_1, \cdots, x_{n-2})$ for all $x = (x_0, x_1, \ldots, x_{n-1}) \in C$. Cyclic codes are attractive because they are easy to encode and decode. They are especially fast when implemented in hardware. Therefore, cyclic codes are a good option for many networks.

Cyclic codes over finite fields were first studied in the late 1950s by Prange [69]. However, most of the research is concentrated on the situation when the code length is relatively prime to the characteristic of the field $\mathbb{F}$. The case when the code length n is divisible by the characteristic p of the field yields the so-called repeated-root codes, which were first studied since 1967 by Berman [3]. Recently, Dinh, in a series of papers ([17], [18]), determined the generator polynomials of all constacyclic codes of lengths $2p^s$, $3p^s$ and $6p^s$ over $\mathbb{F}_{p^m}$. Dual constacyclic codes of these lengths were also discussed. In [10], Dinh *et al.* studied repeated-root constacyclic codes of length lp^s over $\mathbb{F}_{p^m}$.

Given a code with the parameters $[n, k, \mathrm{d_H}]_q$, then $n, k, \mathrm{d_H}$ must satisfy the Singleton bound [61], i.e., $k \leq n - \mathrm{d_H} + 1$. If $k = n - \mathrm{d_H} + 1$, then the code is called an *MDS code*. If we fix n and k, then an MDS code has the greatest detecting and error-correcting capabilities. Therefore, the problem of constructing maximum distance separable codes is an important topic in coding theory.

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

With the realization in the 1980s by Deutsch [15], computers that use the interference and superposition principles of quantum mechanics might be able to solve certain problems, including prime factorization, exponentially faster than classical computers. In classical information theory, information is represented by bits which take two values 0 and 1. In quantum mechanics, quantum bits (briefly, *qubit*) are replacements for bits. Similar to classical bits, qubits can be stated as $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers satisfying the condition $|\alpha|^2 + |\beta|^2 = 1$. It is well-known that a complex square matrix U is *unitary* if its conjugate transpose $U^\star$ satisfies $U^\star U = UU^\star = I$, where I is the identity matrix. Quantum gates are represented by unitary matrices. This means that a gate acts on n qubits that are represented by a $2^n \times 2^n$ unitary matrix because the number of qubits in the input and output of the gate are equal. The quantum states that the gates act upon are vectors in 2^n complex dimensions.

A qubit can be realized in many different physical systems such as atoms, ions, photons, etc. The most prominent physical realization of a qubit given in a quantum communication network is with photons. Using photons, in quantum communication, the two values 0 and 1 of a bit can be encoded in many different ways. In a quantum computer, two qubits 0 and 1 can also represent four states (00, 01, 10, or 11). However, the qubits can represent all four states 00, 01, 10, 11 at the same time while classical computers always run by one state. This is the main difference between quantum computers and classical computers. If we add more qubits into a quantum computer, its speed grows exponentially. For mathematical computations, in general, if we have n qubits for quantum computers, we can simultaneously represent 2^n states in a computation. For example, if we have 64 qubits, quantum computers give us $2^{64} = 18.446.744.073.709.551.616$ states at the same time. If we use 64 classical bits, classical computers represent 2^{64} states, but it can only represent one state at a time. Hence, a classical computer needs to take about 300 years to complete 2^{64} states since the speed of a modern personal computer is around two billion states per second. Therefore, quantum computers could solve problems which are ''practically impossible'' for classical computers. But to get that exponential speed-up, all the qubits are linked together in a process called *quantum entanglement*.

Quantum entanglement is a physical phenomenon in which the quantum states of multiple subsystems cannot be described independently of each other, even though the subsystems are spatially separated. The creation of increasingly large entangled states is very important in quantum information. Entangled states have been intensively studied by many authors [4], [52], [63], [70], [71], [87]. Two-particle entanglements have been demonstrated experimentally by Kwiat *et al.* [52] in 1995 while Bouwmeester *et al.* [4] studied three-entangled photons in 1999. The main idea in [4] was to transform two pairs of entangled photons into three entangled photons and a fourth independent photon. However, the maximal number of entangled photons has been limited to six until 2012 ([63], [70], [71], [87]). In 2012, by a study of Yao *et al.*, eight-photon entanglement was considered and created [93].

One of the problems against the feasibility of quantum computation appears to be the difficulty of eliminating errors caused by inaccuracy and decoherence. Since the classical error-correcting techniques based on redundancy or repetition codes seemed to contradict the quantum no-cloning theorem, classical error-correcting codes can not be used in quantum computation. Therefore, quantum error-correcting codes (briefly, QEC codes) are proposed to protect quantum information from errors due to the decoherence and other quantum noise. QEC codes were first introduced by Shor in 1995 [83]. Many good QEC codes were constructed from Hamming codes, BCH codes and Reed-Solomon codes. Although the theory of QEC codes is quite different from the theory of classical error-correcting codes, Calderbank *et al.* transformed the problem of finding QEC codes from classical error-correcting codes over GF(4) [9]. Calderbank *et al.* also introduced a method to construct QEC codes from classical error-correcting codes [9]. After that, some researchers constructed QEC codes from classical codes such as Hamming, BCH and Reed-Solomon codes [8], [32], [33].

The study of QEC codes has developed rapidly in recent years. After the publications of several foundation papers [2], [8], [53], [83], [85], which were the key theoretical development, in rapid succession, QEC codes have been studied extensively. There have been many results on the structure, properties and operation of QEC codes [2], [9], [13], [35], [50]. In the last several years, CSS, Hermitian constructions are used to construct some classes of QEC codes.

Recently, entanglement-assisted quantum error-correcting (briefly, EAQEC) codes are considered as a new research direction of quantum coding theory. EAQEC codes which are QEC codes with the pre-shared entanglement between the sender and the receiver, were introduced by Brun *et al.* in 2006 [6]. Let Q be an $[[n, k, d; c]]_q$ EAQEC code. Then Q encodes k logical qubits into n physical qubits with the help of c pairs of maximally entangled Bell states (c is called an *entanglement bit (briefly, ebit)*), and corrects up to at least $\lceil \frac{d-1}{2} \rceil$-quantum errors, where d is the Hamming distance of the code. Entanglement can provide a way for QEC codes to achieve higher rates than the ones obtained via a traditional way. However, the ebit c of EAQEC codes is difficult to calculate. In recent years, a lot of research work has been done for the construction of EAQEC codes and several new families of EAQEC codes have been found by employing different methods [12], [39], [56], [57], [88], [89].

The theory of QEC codes can be extended to asymmetric quantum channels. Asymmetric quantum error-correcting (briefly, AQEC) codes were first introduced by Ioffe and Marc in 2007 [41]. They proved that in physical systems the noise is typically asymmetric. Therefore, AQEC codes are proposed to take advantage of the asymmetry in physical qubits. Ioffe and Marc constructed AQEC codes from BCH

and the low-density parity- check (LDPC) codes. They also proved that these codes have good parameters in terms of rate and distance. After that, in [21]–[23], [37], [38], some AQEC codes were constructed.

Since qMDS codes have great applications in quantum computation and quantum communication, constructing qMDS code has become a hot topic in coding theory. In classical coding theory, there are two main methods to construct the qMDS codes. Applying graph theory, some authors can also construct qMDS codes [31], [40], [75], [76]. However, the construction process seems difficult. The other method is to construct MDS codes by the known classical codes. Using stabilizer codes, algebraic geometric codes, classical self-orthogonal codes, Hermitian and Euclidean self-orthogonal codes, and generalized RS codes, some QEC codes were constructed [11], [36], [46]. By approaching from classical self-orthogonal codes over $\mathbb{F}_2$ or $\mathbb{F}_4$, Calderbank and Shor [8] showed that the construction of QEC codes can be found. After the realization in the 1990s by Calderbank *et al.* [9] that QEC codes can construct from classical codes, classical codes are used to obtain some good QEC codes. In the paper of Guardia [36], a class of QEC codes is constructed by cyclic codes. Kai and Zhu [46] provided two new classes of qMDS codes from negacyclic codes. However, the codes given by Guardia [36] and Kai and Zhu [46] have parameters with $\mathrm{d_H} \leq \frac{q}{2} + 1$. In 2014, Chen *et al.* [11] studied MDS constacyclic codes by using dual containing codes which are good parameters. Recently, some new qMDS codes are constructed in [24], [81], [82], [92], [94], and [74].

An $[[n, k]]$ QEC code is a coding scheme that encodes k logical qubits into n physical qubits. As in the classical case, n and k are the length and dimension of the code, respectively. Typically, QEC codes are designed to correct the effects of bit errors and phase errors caused by Pauli operators X and Z respectively under the assumption that both bit error due to X and phase error due to Z may occur on the same qubit. An $(a_l, a_r)-[[n, k]]$ QSC is an $[[n, k]]$ QEC code that corrects not only bit errors and phase errors but also misalignment to the left by a_l qubits and to the right by a_r qubits for some non-negative integers a_l and a_r.

In 2013, QSCs were first introduced by Fujiwara [25] that correct both quantum noise and block synchronization errors. Block synchronization (or frame synchronization) is an important problem in virtually any area in classical digital communications to ensure that the information transmitted can be correctly decoded by the receiver. In order to do so, 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, [5], [77]). Quantum block synchronization is also significant because the block structure is typically used in quantum information coding ([54], [65]) as in classical domain and procedures for manipulating it demands precise alignment ([26], [68]). Unfortunately, since measurement of qubits usually destroys their contained quantum information, quantum analogs of the above methods given in [5], [77] don't apply. However, in [25], QSCs are proposed to be functioning well, which allows for extracting the information about the magnitude and direction of misalignment and simultaneously correcting the Pauli errors on qubits, with nondisturbing measurement involved. In the coding scheme, QSCs can be constructed from a pair of dual-containing cyclic codes with one contained in the other. Motivated by [5] and [77], Luo and Ma [59] proposed a general construction of QSCs with CSS structure from classical dual-containing cyclic codes and obtained a distance bound using a rational function for the proposed QSCs.

Quantum noise is described by operators that act on qubits, with the most general model being the linear combinations of the Pauli operators I, X, Y, and Z acting on each qubit individually. As a measure of the ability to correct Pauli errors of the QSCs, the minimum distance of a cyclic code is shown to be confined by several bounds. So, the find for better bounds is still one of the central problems in classical coding theory. Repeated-root cyclic codes may greatly help solving the above problems, and therefore, be a good ingredient for constructing QSCs.

Motivated by these, in this research, we study MDS cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. We list all MDS cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. We also give some examples to illustrate. As an important application, we construct all qMDS codes from cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the CSS and Hermitian constructions. We establish all qMDS codes constructed from dual codes of cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. Furthermore, we also construct QSCs from cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$.

The rest of our paper is organized as follows. Section 2 gives some preliminaries and notations. Section 3 provides all MDS cyclic and negacyclic codes length $2p^s$ over $\mathbb{F}_{p^m}$. Section 4 focuses on constructing qMDS codes from cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the CSS and Hermitian constructions. Section 5 constructs QSCs from cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$.

II. PRELIMINARIES

Let $\mathbb{F}_{p^m}$ be a finite field, p be an odd prime, and m and s be positive integers. A code of length n over $\mathbb{F}_{p^m}$ is a nonempty subset C of $\mathbb{F}_{p^m}^n$. If a nonempty subset C is a vector space over $\mathbb{F}_{p^m}$, then C is called a *linear code*. For an invertible Λ of $\mathbb{F}_{p^m}$, the Λ-constacyclic (Λ-twisted) shift τ_Λ on $\mathbb{F}_{p^m}^n$ is the shift

$$\tau_\Lambda(x_0, x_1, \ldots, x_{n-1}) = (\Lambda x_{n-1}, x_0, x_1, \cdots, x_{n-2}).$$

If $\tau_\Lambda(C) = C$, then C is a Λ-constacyclic code.

The following fact is well-known in [61].

Lemma 1 ([61]): A linear code C of length n is λ-constacyclic over $\mathbb{F}_{p^m}$ if and only if C is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n-\lambda\rangle}$.

Let $C = (c_0, c_1, \ldots, c_{n-1})$ be a codeword. Then we have a bijective correspondence between C and the polynomial

TABLE 1. The Hamming distance $d_H(C_{i,j})$.

Case	i	j	$\mathrm{d_H}(C_{i,j})$
1	$0 \le i \le p^s$	$j = 0$	2
2	$0 \le i \le p^{s-1}$	$0 \le j \le p^{s-1}$	2
3	$p^{s-1} < i \le 2p^{s-1}$	$0 < j \le p^{s-1}$	3
4	$2p^{s-1} < i \le p^s$	$0 < j \le p^{s-1}$	4
5	$\beta p^{s-1} + 1 \le i \le (\beta+1)p^{s-1}$	$\beta' p^{s-1} + 1 \le j \le (\beta'+1)p^{s-1}$	$\min\{\beta+2, 2(\beta'+2)\}$
6	$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau p^{s-k-1}$	$\beta p^{s-1} + 1 \le j \le (\beta+1)p^{s-1}$	$2(\beta+2)$
7	$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau p^{s-k-1}$	$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le j \le p^s - p^{s-k} + \tau p^{s-k-1}$	$(\tau+1)p^k$
8	$p^s - p^{s-k} + (\tau^{(1)}-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau^{(1)} p^{s-k-1}$	$p^s - p^{s-k} + (\tau^{(2)}-1)p^{s-k-1} + 1 \le j \le p^s - p^{s-k} + \tau^{(2)} p^{s-k-1}$	$\min\{(\tau^{(2)}+1)p^k, (\tau^{(1)}+1)p^k\}$
9	$p^s - p^{s-k'} + (\tau^{(3)}-1)p^{s-k'-1} + 1 \le i \le p^s - p^{s-k'} + \tau^{(3)} p^{s-k'-1}$	$p^s - p^{s-k''} + (\tau^{(4)}-1)p^{s-k''-1} + 1 \le j \le p^s - p^{s-k''} + \tau^{(4)} p^{s-k''-1}$	$2(\tau^{(4)}+1)p^{k''}$
10	$i = p^s$	$\beta p^{s-1} + 1 \le j \le (\beta+1)p^{s-1}$	$(2\beta+2)$
11	$i = p^s$	$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le j \le p^s - p^{s-k} + \tau p^{s-k-1}$	$2(\tau+1)p^k$

$c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \frac{\mathbb{F}_{p^m}[x]}{\langle x^n - \Lambda\rangle}$. From this, a linear code C of length n over $\mathbb{F}_{p^m}$ is a Λ-constacyclic code of length n over $\mathbb{F}_{p^m}$ if and only if C is an ideal of $\frac{\mathbb{F}_{p^m}[x]}{\langle x^n - \Lambda\rangle}$ (cf. [67]).

Given n-tuples

$$e = (e_0, e_1, \ldots, e_{n-1}), t = (t_0, t_1, \ldots, t_{n-1}) \in \mathbb{F}_{p^m}^n,$$

the inner product (dot product) of two vectors e, t is expressed as follows:

$$e \cdot t = e_0 t_0 + e_1 t_1 + \cdots + e_{n-1} t_{n-1},$$

evaluated in $\mathbb{F}_{p^m}$. If $e \cdot t = 0$, then two vectors e, t are called *orthogonal*. Dual code of a linear code C over $\mathbb{F}_{p^m}$, denoted by $C^\perp$, is defined as follows:

$$C^\perp = \{e \in \mathbb{F}_{p^m}^n \mid e \cdot t = 0, \quad \forall t \in C\}.$$

The dual of a Λ-constacyclic code is given in the following result.

Proposition 2 (cf. [16]): The dual of a Λ-constacyclic code is a Λ^{-1}-constacyclic code.

Cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are ideals of the principal ideal ring

$$\mathcal{R}_1 = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{2p^s} - 1\rangle}.$$

Cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are investigated in [17, Theorem 4.1].

Theorem 3 [17, Theorem 4.1]: Cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are $\langle (x-1)^i (x+1)^j\rangle \subseteq \mathcal{R}_1$, where $0 \le i, j \le p^s$. Each code $C_{i,j} = \langle (x-1)^i (x+1)^j\rangle$ contains $p^{m(2p^s - i - j)}$ codewords, its dual is $C_{i,j}^\perp = \langle (x-1)^{p^s - i} (x+1)^{p^s - j}\rangle$.

Negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are ideals of the finite ring $\mathcal{R}_{-1} = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{2p^s} + 1\rangle}$. In [17], all negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are completely determined.

Theorem 4 [17, Theorem 3.2]:

(*a*) If $p^m \equiv 1 \pmod 4$, then negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are of the form $\langle (x-\gamma)^i (x+\gamma)^j\rangle \subseteq \mathcal{R}_{-1}$, where $\gamma^2 = -1$ and $0 \le i, j \le p^s$. Each code $\mathcal{C}_{i,j} = \langle (x-\gamma)^i (x+\gamma)^j\rangle$ contains $p^{m(2p^s - i - j)}$ codewords, its dual is $\mathcal{C}_{i,j}^\perp = \langle (x-\gamma)^{p^s - i} (x+\gamma)^{p^s - j}\rangle$.

(*b*) If $p^m \equiv 3 \pmod 4$, then negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are of the form $\langle (x^2+1)^i\rangle \subseteq \mathcal{R}_{-1}$, where $0 \le i \le p^s$. Each code $C_i = \langle (x^2+1)^i\rangle$ contains $p^{2m(p^s - i)}$ codewords, its dual is $C_i^\perp = \mathcal{C}_{p^s - i} = \langle (x^2+1)^{p^s - i}\rangle$.

We made the convention that the distance of the zero code is 0. Let $e, t \in \mathbb{F}_{p^m}^n$ be two vectors. The Hamming distance between e and t, denoted by $d_H(e, t)$, is the number of coordinates in which e and t differ. For a code C containing at least two words, the Hamming distance of the code C, denoted by $\mathrm{d_H}(C)$, is

$$\mathrm{d_H}(C) = \min\{d(e, t), e, t \in C, e \ne t\}.$$

If $p^m \equiv 3 \pmod 4$, then the Hamming distance $\mathrm{d_H}(C_i)$ is determined in [58, Theorem 7.9].

Theorem 5 [58, Theorem 7.9]: If $p^m \equiv 3 \pmod 4$, then the negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are of the form $C_i = \langle (x^2+1)^i\rangle$ for $i = 0, 1, \ldots, p^s$. Moreover, its Hamming distance $\mathrm{d_H}(C_i)$, as shown at the bottom of the next page.

In [66], the Hamming distances of all non-trivial cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ were provided. The parameters $1 \le \beta' \le \beta \le p-2, 1 \le \tau^{(2)} < \tau^{(1)} \le p-1, 1 \le \tau, \tau^{(3)}, \tau^{(4)} \le p-1, 1 \le k \le s-1, 1 \le k' < k \le s-1$ are integers. If $i \ge j$, its Hamming distance $\mathrm{d_H}(C_{i,j})$, as shown at the bottom of the next page, is completely determined in [66, Theorem 2] (Table 1 in our paper). The Hamming distances of cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are simplified into a better representation in [19] as follows:

The theory of QEC codes is a key part of quantum information theory. For a long time, the problem of how to protect information from quantum noise is very difficult to give a solution. However, by discovering of the first QEC codes introduced by Calderbank and Shor [8], a series of great progresses in QEC codes is provided.

Let q be a prime power and let $H_q(C)$ be a q-dimensional Hilbert vector space. We denote $H_q^n(C) = H_q(C) \otimes \cdots \otimes H_q(C)$ (n times). Then $H_q^n(C)$ is a q^n-dimensional Hilbert space. We recall the definition of QEC codes.

Definition 6 [72]: A quantum code of length n and dimension k over $\mathbb{F}_q$ is defined to be a q^k dimensional subspace of $H_q^n(C)$ and simply denoted by $[[n, k, d_H]]_q$, where d_H is the Hamming distance of the quantum code.

We finish this section by the following lemma.

Lemma 7: Let $0 < n \in \mathbb{N}$. Then there are $\frac{(n+2)(n+1)}{2}$ pairs of non-negative integers a, b satisfying $a + b \le n$.

Proof: If $a = 0$, then we have $n+1$ choices for b. If $a = 1$, then we have n choices for b. In general, for any $a = i$, where $0 \le i \le n$, there are $n - i + 1$ choices for b,

i.e., b can be any integer from 0 to $n-i$. Hence, there are $1+2+3+\cdots+n+(n+1)=\frac{(n+2)(n+1)}{2}$ pairs of non-negative integers a, b such that $a+b\le n$. □

III. MDS CYCLIC AND NEGACYCLIC CODES OF LENGTH $2p^s$ OVER $\mathbb{F}_{p^m}$

The Singleton bound relates the parameters of a code as follows: $|C|\le p^{m(n-\mathrm{d_H}(C)+1)}$ [73]. The proof of the binary case for the Singleton Bound was first introduced by Komaniya in 1954 [51]. After that, Joshi [42] continued to consider this problem. In [14], Denes and Keedwell showed that the proof of Joshi is also true for the general q-ary case. A code C satisfying $|C|=p^{m(n-\mathrm{d_H}(C)+1)}$ which is called an MDS code. It implies that if we fix n and k, then an MDS code has the greatest error-correcting and detecting capabilities. Results on MDS codes were first provided by Bush [7]. In 1960, Silverman [84] also gave several interesting results on MDS codes. In [34], by using Latin squares and hypercubus, Golomb and Posner constructed many MDS codes. Motivated by Silverman's work in 1960, Maneri and Silverman [62] proved some results on linear and general MDS codes in 1966. The weight enumerator for linear MDS codes was also studied by many authors (for examples, [61], [86]). In 2005, ElKhamy and McEliece [20] introduced the weight enumerator of linear MDS codes.

We see that the dimension of a negacyclic code $C_i=\langle(x^2+1)^i\rangle$ is $2p^s-2i$, where $p^m\equiv 3 \pmod 4$ and $0\le i\le p^s$. Applying the Singleton Bound, C_i is an MDS negacyclic code if and only if $2i=\mathrm{d_H}(C_i)-1$. We consider 3 cases, namely, $i=0$, $p^s-p^{s-k_1}+\beta p^{s-k_1-1}+1\le i\le p^s-p^{s-k_1}+(\beta+1)p^{s-k_1-1}$ and $i=p^s$.

Case 1: $i=0$. Then we have $\mathrm{d_H}(C_0)=1$. Hence, C_0 is an MDS negacyclic code.

Case 2: $p^s-p^{s-k_1}+\beta p^{s-k_1-1}+1\le i\le p^s-p^{s-k_1}+(\beta+1)p^{s-k_1-1}$. In this case, we have

$$\begin{aligned}2i &\ge 2(p^s-p^{s-k_1}+\beta p^{s-k_1-1}+1)\\ &= 2(p^{s-k_1}(p^{k_1}-1)+\beta p^{s-k_1-1}+1)\\ &= 2p(p^{k_1}-1)+2\beta+2\\ &\ge 2(\beta+2)p^{k_1}-2(\beta+2)+2\beta+2\\ &= 2(\beta+2)p^{k_1}\\ &> (\beta+2)p^{k_1}-1=\mathrm{d_H}(C_i)-1.\end{aligned}$$

Hence, $C_i=\langle(x^2+1)^i\rangle$ is not an MDS negacyclic code when $p^s-p^{s-k_1}+\beta p^{s-k_1-1}+1\le i\le p^s-p^{s-k_1}+(\beta+1)p^{s-k_1-1}$.

Case 3: $i=p^s$. Then we see that $2i=2p^s>\mathrm{d_H}(C_{p^s})-1=0-1$. Hence, C_{p^s} is not an MDS negacyclic code. Therefore, if p is odd and $p^m\equiv 3 \pmod 4$, then C_i is not an MDS negacyclic code.

We summarize our discussion above in the following theorem.

Theorem 8: Let p be an odd prime, and m be a positive integer such that $p^m\equiv 3 \pmod 4$. A negacyclic code C_i is an MDS negacyclic code if and only if $i=0$.

When $i\ge j$, all MDS cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are determined in the following theorem.

Theorem 9: Let $C_{i,j}=\langle(x-1)^i(x+1)^j\rangle\subseteq R_1$ be a cyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$, where $0\le j\le i\le p^s$. Then $C_{i,j}$ is an MDS cyclic code if and only if one of the following conditions holds:

- *If $i=0, j=0$, then $\mathrm{d_H}(C_{0,0})=1$.*
- *If $i=1, j=0$, then $\mathrm{d_H}(C_{1,0})=2$.*
- *If $i=p^s, j=p^s-1$, then $\mathrm{d_H}(C_{p^s,p^s-1})=2p^s$.*

Proof: We divide i, j into 11 cases as in the Table 1.

Case 1: $0\le i\le p^s, j=0$. In this case, we have $\mathrm{d_H}(C_{i,j})=2$. Hence, if $i=1$ and $j=0$, then $i+j=\mathrm{d_H}(C_{1,0})-1$, i.e., $C_{1,0}$ is an MDS cyclic code.

Case 2: $0\le i\le p^{s-1}, 0\le j\le p^{s-1}$. In this case, we see that $\mathrm{d_H}(C_{i,j})=2$. It is easy to see that if $i=1$ and $j=0$, then $i+j=\mathrm{d_H}(C_{1,0})-1=1$, i.e., $C_{1,0}$ is an MDS cyclic code. If $i>1$ and $j>1$, then $i+j>\mathrm{d_H}(C_{i,j})-1=1$. Hence, $C_{i,j}$ is not an MDS cyclic code.

Case 3: $p^{s-1}<i\le 2p^{s-1}, 0<j\le p^{s-1}$. Then we have $\mathrm{d_H}(C_{i,j})=3$. It is easy to check that $i+j>2=\mathrm{d_H}(C_{i,j})-1$ for all $p^{s-1}<i\le 2p^{s-1}$ and $0<j\le p^{s-1}$. Hence, $C_{i,j}$ is not an MDS cyclic code for all $p^{s-1}<i\le 2p^{s-1}$ and $0<j\le p^{s-1}$.

$$\mathrm{d_H}(C_i)=\begin{cases}1, & \text{if } i=0\\ (\beta+2)p^{k_1}, & \text{if } p^s-p^{s-k_1}+\beta p^{s-k_1-1}+1\le i\le p^s-p^{s-k_1}+(\beta+1)p^{s-k_1-1}\\ & \quad \text{where } 0\le\beta\le p-2, \text{ and } 0\le k_1\le s-1\\ 0, & \text{if } i=p^s.\end{cases}$$

$$\mathrm{d_H}(C_i)=\begin{cases}1, & \text{if } i=0\\ 2, & \text{if } j=0 \text{ and } 0<i\le p^s\\ \min\{(\beta+2)p^{k_1}, 2(\beta'+2)p^{k'}\} & \text{if } p^s-p^{s-k_1}+\beta p^{s-k_1-1}+1\le i\le p^s-p^{s-k_1}+(\beta+1)p^{s-k_1-1}\\ & \quad p^s-p^{s-k'}+\beta' p^{s-k'-1}+1\le i\le p^s-p^{s-k'}+(\beta'+1)p^{s-k'-1}\\ 0, & \text{if } i=p^s.\end{cases}$$

Case 4: $2p^{s-1} < i \le p^s, 0 < j \le p^{s-1}$. In this case, by Table 1, $\mathrm{d_H}(C_{i,j}) = 4$. We see that $i+j > \mathrm{d_H}(C_{i,j}) - 1 = 3$. Hence, $C_{i,j}$ is not an MDS cyclic code for all $2p^{s-1} < i \le p^s$ and $0 < j \le p^{s-1}$.
Case 5: $\beta p^{s-1} + 1 \le i \le (\beta+1)p^{s-1}$, $\beta' p^{s-1} + 1 \le j \le (\beta'+1)p^{s-1}$. In this case, by Table 1, $\mathrm{d_H}(C_{i,j}) = \min\{\beta+2, 2(\beta'+2)\}$. We have

$$\begin{aligned} i+j &\ge \beta p^{s-1} + 1 + \beta' p^{s-1} + 1 \\ &\ge \beta p + \beta' p + 2 > \beta + 1. \end{aligned}$$

This implies that $i+j > \mathrm{d_H}(C_{i,j}) - 1$. Therefore, $C_{i,j}$ is not an MDS cyclic code.
Case 6: $p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau p^{s-k-1}$, $\beta p^{s-1} + 1 \le j \le (\beta+1)p^{s-1}$. Then we see that

$$\begin{aligned} i+j &\ge p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 + \beta p^{s-1} + 1 \\ &= p^{s-k}(p^k - 1) + (\tau-1)p^{s-k-1} + \beta p^{s-1} + 2 \\ &\ge p(p^k - 1) + \tau - 1 + \beta p^{s-1} + 2 \\ &\ge (\beta+2)p^k - \beta - 2 + \tau + \beta + 1 \\ &\ge (\beta+2)(\beta+2) + \tau - 1 \\ &= \beta^2 + 2(\beta+2) + \tau + 3 \\ &> 2(\beta+2) - 1 = \mathrm{d_H}(C_{i,j}) - 1. \end{aligned}$$

This implies that $i+j > \mathrm{d_H}(C_{i,j}) - 1$. Therefore, $C_{i,j}$ is not an MDS cyclic code.
Case 7: $p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau p^{s-k-1}$, $p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le j \le p^s - p^{s-k} + \tau p^{s-k-1}$. In this case, we have

$$\begin{aligned} i+j &\ge p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \\ &\quad + p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \\ &\ge 2p(p^k - 1) + 2(\tau-1) + 2 \\ &> 2(\tau+1)(p^k - 1) + 2\tau \\ &> 2(\tau+1)p^k - 2. \end{aligned}$$

From $1 \le \tau < p-1$ and $1 \le k \le s-1$, we see that $(\tau+1)p^k > 3$. This implies that $i+j > (\tau+1)p^k - 1 = \mathrm{d_H}(C_{i,j}) - 1$. Hence, $C_{i,j}$ is not an MDS cyclic code.
Case 8: $p^s - p^{s-k} + (\tau^{(1)}-1)p^{s-k-1} + 1 \le i \le p^s - p^{s-k} + \tau^{(1)} p^{s-k-1}$, $p^s - p^{s-k} + (\tau^{(2)}-1)p^{s-k-1} + 1 \le j \le p^s - p^{s-k} + \tau p^{s-k-1}$. In this case, we see that

$$\begin{aligned} i+j &\ge p^s - p^{s-k} + (\tau^{(1)} - 1)p^{s-k-1} + 1 \\ &\quad + p^s - p^{s-k} + (\tau^{(2)} - 1)p^{s-k-1} + 1 \\ &\ge 2p(p^k - 1) + (\tau^{(1)} - 1) + (\tau^{(2)} - 1) + 2 \\ &\ge 2(\tau^{(1)} + 1)(p^k - 1) + (\tau^{(1)} - 1) \\ &\quad + (\tau^{(2)} - 1) + 2 \\ &\ge (\tau^{(1)} + 1)p^k + (\tau^{(1)} + 1)p^k \\ &\quad - \tau^{(1)} + \tau^{(2)} - 2 \\ &\ge (\tau^{(1)} + 1)p^k + (\tau^{(1)} + 1)(\tau^{(1)} + 1) \\ &\quad - \tau^{(1)} + \tau^{(2)} - 2 \\ &\ge (\tau^{(1)} + 1)p^k + (\tau^{(1)})^2 + 2\tau^{(1)} + 1 \\ &\quad - \tau^{(1)} + \tau^{(2)} - 2 \\ &\ge (\tau^{(1)} + 1)p^k + (\tau^{(1)})^2 + \tau^{(1)} + \tau^{(2)} - 1 \\ &> (\tau^{(1)} + 1)p^k - 1 \\ &> \min\{2(\tau^{(2)} + 1)p^k, (\tau^{(1)} + 1)p^k\} - 1. \end{aligned}$$

Hence, $i+j > \min\{2(\tau^{(2)}+1)p^k, (\tau^{(1)}+1)p^k\} - 1 = \mathrm{d_H}(C_{i,j}) - 1$. Therefore, $C_{i,j}$ is not an MDS cyclic code.
Case 9: $p^s - p^{s-k'} + (\tau^{(3)}-1)p^{s-k'-1} + 1 \le i \le p^s - p^{s-k'} + \tau^{(3)} p^{s-k'-1}$, $p^s - p^{s-k''} + (\tau^{(4)}-1)p^{s-k''-1} + 1 \le j \le p^s - p^{s-k''} + \tau^{(4)} p^{s-k''-1}$. From this, we have

$$\begin{aligned} i+j &\ge p^s - p^{s-k'} + (\tau^{(3)} - 1)p^{s-k'-1} + 1 \\ &\quad + p^s - p^{s-k''} + (\tau^{(4)} - 1)p^{s-k''-1} + 1 \\ &= p^{s-k'}(p^{k'} - 1) + \tau^{(3)} - 1 + \tau^{(4)} - 1 + 2 \\ &> 2p(p^{k''} - 1) + \tau^{(3)} + \tau^{(4)} \\ &\ge 2(\tau^{(4)} + 1)(p^{k''} - 1) + \tau^{(3)} + \tau^{(4)} \\ &> 2(\tau^{(4)} + 1)p^{k''} + \tau^{(3)} - \tau^{(4)} - 2 \\ &\ge (\tau^{(4)} + 1)p^{k''} + (\tau^{(4)} + 1)p^{k''} \\ &\quad + \tau^{(3)} - \tau^{(4)} - 2 \\ &\ge (\tau^{(4)} + 1)p^{k''} + (\tau^{(4)} + 1)(\tau^{(4)} + 1) \\ &\quad + \tau^{(3)} - \tau^{(4)} - 2 \\ &\ge (\tau^{(4)} + 1)p^{k''} + (\tau^{(4)})^2 + \tau^{(4)} + \tau^{(3)} - 1 \\ &> (\tau^{(4)} + 1)p^{k''} - 1. \end{aligned}$$

This implies that $i+j > (\tau^{(4)}+1)p^{k''} - 1 = \mathrm{d_H}(C_{i,j}) - 1$. Hence, $C_{i,j}$ is not an MDS cyclic code.
Case 10: $i = p^s$, $\beta p^{s-1} + 1 \le j \le (\beta+1)p^{s-1}$. If $s = 1$, then $i = p$ and $j \ge \beta + 1$. This implies that $i+j = \mathrm{d_H}(C_{i,j}) - 1 = 2(\beta+2) - 1$. Hence, $C_{i,j}$ is an MDS cyclic code if $s = 1$, $\beta = p-2$. If $s \ge 2$, then $\beta p^{s-1} > 2\beta$. This implies that $p^s + 2\beta + 1 > 2\beta + 5 > 2(\beta+2) - 1 = \mathrm{d_H}(C_{i,j}) - 1$. Hence, $C_{i,j}$ is not an MDS cyclic code.
Case 11: $i = p^s$, $p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \le j \le p^s - p^{s-k} + \tau p^{s-k-1}$. Then we have

$$\begin{aligned} i+j &\ge p^s + p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \\ &= p^s + p^{s-k}(p^k - 1) + (\tau-1)p^{s-k-1} + 1 \\ &\ge p.p^k + p(p^k - 1) + \tau - 1 + 1 \\ &\ge 2(\tau+1)p^k + \tau - p. \end{aligned}$$

This implies that $i+j = \mathrm{d_H}(C_{i,j}) - 1$ if $\tau + 1 = p$ and $s = k+1$. Hence, if $\tau + 1 = p$ and $s = k+1$, i.e., $i = p^s$ and $j = p^s - 1$, then C_{p^s, p^s-1} is an MDS cyclic code.

Remark 10: We obtain all MDS cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ for $i \ge j$ in Theorem 9. The corresponding case with $j \ge i$ can be determined by symmetries. For example, in case, $i = p^s, j = p^s - 1$, the corresponding case is $j = p^s$ and $i = p^s - 1$. In Theorem 9, it is shown that $C_{i,j} = C_{p^s, p^s-1}$

is an MDS cyclic code. Hence, $C_{i,j} = C_{p^s-1,p^s}$ is also an MDS cyclic code. Using the structure of negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ given in Theorem 4 (part (a)), if $p^m \equiv 1 \pmod 4$, then the Hamming distance of negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ coincides with the Hamming distance of cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ (Table 1). Therefore, by Theorem 9, we can determine all MDS negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ when $p^m \equiv 1 \pmod 4$. We see that some MDS cyclic codes in Theorem 9 are different from all the known ones. Moreover, MDS cyclic codes in our paper have good distance. For example, if $q = p^m, s = m^3, m > 1$ and $C_{i,j} = C_{p^s,p^s-1}$, then $\mathrm{d_H}(C_{i,j}) = 2p^{m^3}$. If $p = 5, m = 2$, then we have an MDS cyclic code with $\mathrm{d_H}(C_{i,j}) = 781250$. This shows that we can choose the parameter s to obtain some MDS cyclic codes with good distance.

To conclude this section, we provide some examples of MDS cyclic codes to illustrate our results.

Example 11: Consider all cyclic codes of length 6 over $\mathbb{F}_3$ which are the ideals $C_{i,j} = \langle (x-1)^i(x+1)^j \rangle$ of $\frac{\mathbb{F}_3[x]}{\langle x^6-1 \rangle}$, where $0 \le i, j \le 3$. Here, $p = 3, s = 1$ and $m = 1$. Using Theorem 9, all MDS cyclic codes of length 6 over $\mathbb{F}_3$ are determine in the following table.

TABLE 2. MDS cyclic codes of length 6 over $\mathbb{F}_3$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes
3	2	$C_{3,2} = \langle (x+1)^2(x-1)^3 \rangle$	6	Yes
2	3	$C_{2,3} = \langle (x+1)^3(x-1)^2 \rangle$	6	Yes

Example 12 Consider all cyclic codes of length 14 over $\mathbb{F}_7$ which are the ideals $C_{i,j} = \langle (x-1)^i(x+1)^j \rangle$ of $\frac{\mathbb{F}_7[x]}{\langle x^{14}-1 \rangle}$, where $0 \le i, j \le 7$. Here, $p = 7, s = 1$ and $m = 1$. We determine all MDS cyclic codes of length 14 over $\mathbb{F}_7$. Out of 64 cyclic codes, there are 5 MDS cyclic codes.

TABLE 3. MDS cyclic codes of length 14 over $\mathbb{F}_7$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes
6	7	$C_{6,7} = \langle (x+1)^7(x-1)^6 \rangle$	14	Yes
7	6	$C_{7,6} = \langle (x+1)^6(x-1)^7 \rangle$	14	Yes

Example 13: Consider all cyclic codes of length 18 over $\mathbb{F}_9$ which are the ideals $C_{i,j} = \langle (x-1)^i(x+1)^j \rangle$ of $\frac{\mathbb{F}_9[x]}{\langle x^{18}-1 \rangle}$, where $0 \le i, j \le 9$. Here, $p = 3, s = 2$ and $m = 2$. We list all Hamming distances of such codes. We also determine all MDS cyclic codes of length 18 over $\mathbb{F}_9$. Out of 100 cyclic codes, there are 5 MDS cyclic codes.

Example 14: Consider all cyclic codes of length 22 over $\mathbb{F}_{11}$ which are the ideals $C_{i,j} = \langle (x-1)^i(x+1)^j \rangle$ of $\frac{\mathbb{F}_{11}[x]}{\langle x^{22}-1 \rangle}$, where $0 \le i, j \le 11$. Here, $p = 11, s = 1$ and $m = 1$.

TABLE 4. MDS cyclic codes of length 18 over $\mathbb{F}_9$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code
0	0	$C_{0,0} = \langle 1 \rangle$	2	Yes
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes
8	9	$C_{8,9} = \langle (x+1)^9(x-1)^8 \rangle$	18	Yes
9	8	$C_{9,8} = \langle (x+1)^8(x-1)^9 \rangle$	18	Yes

We determine all MDS cyclic codes of length 22 over $\mathbb{F}_{11}$. Out of 132 cyclic codes, there are 5 MDS cyclic codes.

TABLE 5. MDS cyclic codes of length 22 over $\mathbb{F}_{11}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes
10	11	$C_{10,11} = \langle (x+1)^{11}(x-1)^{10} \rangle$	22	Yes
11	10	$C_{11,10} = \langle (x+1)^{10}(x-1)^{11} \rangle$	22	Yes

IV. QUANTUM MDS CODES

In 1995, Shor first introduced QEC codes [83]. After that, Calderbank and Shor [8] used classical codes over GF(4) to find some QEC codes. In 1998, a new method to construct QEC codes from classical error-correcting codes is proposed by Calderbank *et al.* [9]. Recently, some QEC codes over finite fields and some classes of finite rings are constructed [2], [9], [13], [35], [50]. However, qMDS codes constructed from cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the CSS and Hermitian constructions have not been studied in the past. In this section, we construct qMDS codes from cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the CSS and Hermitian constructions.

We recall a construction of QEC codes, the so-called CSS construction.

Theorem 15 (CSS Construction) [8]: Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ such that $C_2 \subseteq C_1$, respectively. Then there exists a QEC code with the parameters $[[n, k_1 - k_2, \min\{d_1, d_2^\perp\}]]_q$, where $d_2^\perp$ is the Hamming distance of the dual code $C_2^\perp$. Moreover, if $C_2 = C_1^\perp$, then there exists a QEC code having the parameters $[[n, 2k_1 - n, d_1]]_q$.

In 1997, the binary version of the quantum Singleton bound was first given by Knill and Laflamme [49]. In 1998, Calderbank *et al.* [9] provided the quantum Singleton bound for all codes over finite fields, as follows.

Theorem 16 (Quantum Singleton Bound) [30, Theorem 1]: Let $C = [[n, k, d_H]]_q$ be a QEC code. Then $k + 2d_H \le n + 2$.

If $k + 2d_H = n + 2$, then C is called a qMDS code. Since the Hamming distance of qMDS codes is maximal, these codes form an important class of QEC codes. Therefore, in recent years, constructions of qMDS codes have been studied by many authors. Several new families of qMDS codes have been introduced (see [11], [30], [43]–[47], [55]). We list some main results in Table 6.

TABLE 6. Known families of qMDS codes.

n	q	$\mathrm{d_H}$	Reference
$n \le q+1$	prime power	$d \le \lfloor \frac{n}{2} \rfloor + 1$	[31]
$mq-l$	prime power	$d \le m-l+1, 0 \le l < m, 1 < m < q$	[57]
$mq-l$	prime power	$3 \le d \le (q+1-\lfloor \frac{l}{m} \rfloor)/2, 0 \le l \le q-1, 1 \le m \le 4$	[46]
$r(q-1)+1$	$q \equiv r-1 \ (mod\ 2r)$	$d \le \frac{q+r+1}{2}$	[47]
q^2-s	prime power	$\frac{q}{2}+1 < d \le q-s$	[47]
$\frac{q^2+1}{2}$	q odd	$3 \le d \le q, d$ odd	[48]
$4 \le n \le q^2+1, n \ne 4$	$q \ne 2$	3	[46]
q^2-1	prime power	$d \le q-l, 0 \le l \le q-2$	[57]
q^2+1	prime power	$2 \le d \le q+1$	[46], [48], [47]
$\frac{q^2-1}{2}$	q odd	$2 \le d \le q$	[49]
$\frac{q^2-1}{r}, r$ even, $r \ne 2, r \mid (q+1)$	q odd	$2 \le d \le \frac{q+1}{2}$	[49]
$\lambda(q+1), \lambda$ odd, $\lambda \mid (q-1)$	q odd	$2 \le d \le \frac{q+1}{2} + \lambda$	[49]
$2\lambda(q+1), \lambda$ odd, $\lambda \mid (q-1)$	$q \equiv 1 \ (mod\ 4)$	$2 \le d \le \frac{q+1}{2} + 2\lambda$	[49]
$\frac{q^2+1}{5}$	$q \equiv 20m+3, q \equiv 20m+7$	$2 \le d \le \frac{q+5}{2}, d$ even	[49]
$\frac{q^2-1}{3}$	$3 \mid (q+1)$	$2 \le d \le \frac{2(q-2)}{3} + 1$	[11]
$\frac{q^2-1}{5}$	$5 \mid (q+1)$	$2 \le d \le \frac{3(q+1)}{5} - 1$	[11]
$\frac{q^2-1}{7}$	$7 \mid (q+1)$	$2 \le d \le \frac{4(q+1)}{7} - 1$	[11]
$\frac{q^2+1}{10}4$	$q = 10m+3, q = 10m+7$	$3 \le d \le 4m+1, d$ odd	[11]
$n = 1 + \frac{r(q^2-1)}{2t+1}, 1 \le t \in \mathbb{Z}, 1 \le r \le 2t+1$	$\gcd(r,q) = 1, q \equiv -1 \ (mod\ 2t+1)$	$d \le \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} + 1$	[45]
$n = \frac{r(q^2-1)}{2t+1}, 1 \le t \in \mathbb{Z}, 1 \le r \le 2t+1$	$\gcd(r,q) > 1, q \equiv -1 \ (mod\ 2t+1)$	$d \le \frac{t+1}{2t+1} \times q - \frac{t}{2t+1} + 1$	[45]
$2(d-1) \le n \le (d^2-2d+2)$	prime power	$2 \le d \le q$	[45]

We now proceed to construct qMDS codes from cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$. In order to do so, we need to give all linear MDS cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ satisfying $C^\perp \subseteq C$. Let $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle \subseteq R_1$ be a cyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$, where $0 \le i, j \le p^s$. Then the dual of $C_{i,j}$ is a cyclic code $C_{i,j}^\perp = \langle (x-1)^{p^s-i} (x+1)^{p^s-j} \rangle$. If $C_{i,j}^\perp \subseteq C_{i,j}$, then $0 \le i \le \frac{p^s}{2}$ and $0 \le j \le \frac{p^s}{2}$. Combining Theorems 9, 15 and 16, we have the following result.

Theorem 17: Let $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle \subseteq R_1$ be a cyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$, for $0 \le i, j \le p^s$. Then the following statements hold:

- *If $i = j = 0$, then there exists a qMDS code with parameters $[[2p^s, 2p^s, 1]]_{p^m}$.*
- *If $i = 1, j = 0$, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_{p^m}$.*
- *If $i = 0, j = 1$, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_{p^m}$.*

Proof: Let $C_{i,j} = [2p^s, k_{i,j}, \mathrm{d_H}(C_{i,j})]_{p^m}$ be an MDS cyclic code satisfying $C_{i,j}^\perp \subseteq C_{i,j}$. Then we have $k_{i,j} = 2p^s - \mathrm{d_H}(C_{i,j}) + 1$ and $0 \le i, j \le \frac{p^s}{2}$. From $C_{i,j}^\perp \subseteq C_{i,j}$, by Theorem 15 (the CSS construction), there exists a quantum code $D_{i,j}$ with parameters $[[2p^s, 2k_{i,j} - 2p^s, \mathrm{d_H}(C_{i,j})]]_{p^m}$. Since $k_{i,j} = 2p^s - \mathrm{d_H}(C_{i,j}) + 1$, we have $2k_{i,j} - 2p^s = 2p^s - 2\,\mathrm{d_H}(C_{i,j}) + 2$. Using Theorem 16, $D_{i,j}$ is a qMDS code with parameters $[[2p^s, 2k_{i,j} - 2p^s, \mathrm{d_H}(C_{i,j})]]_{p^m}$. Hence, if $C_{i,j} = [2p^s, k_{i,j}, \mathrm{d_H}(C_{i,j})]_{p^m}$ is an MDS cyclic code and $C_{i,j}^\perp \subseteq C_{i,j}$, there exists a qMDS code with parameters $[[2p^s, 2p^s - 2\,\mathrm{d_H}(C_j) + 2, \mathrm{d_H}(C_j)]]_{p^m}$. We consider 3 cases as follows:

Case 1: $i = j = 0$. In this case, we have $\mathrm{d_H}(C_{0,0}) = 1$. By Theorem 9, we can see that $C_{0,0} = [2p^s, 2p^s, 1]_{p^m}$ is an MDS cyclic code. From $i = j = 0$, we have $C_{0,0}^\perp \subseteq C_{0,0}$. As there exists a qMDS code with parameters $[[2p^s, 2p^s - 2\,\mathrm{d_H}(C_{i,j}) + 2, \mathrm{d_H}(C_{i,j})]]_{p^m}$, we have a qMDS code with parameters $[[2p^s, 2p^s, 1]]_{p^m}$.

Case 2: $i = 1, j = 0$. From this, we have $\mathrm{d_H}(C_{1,0}) = 2$. Applying Theorem 9, we can see that $C_{1,0}$ is an MDS cyclic code. From $i = 1, j = 0$, we have $C_{1,0}^\perp \subseteq C_{1,0}$. Hence, there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_{p^m}$.

Case 3: $i = 0, j = 1$. From Case 2, by symmetry, it is easy to see that if $i = 1, j = 0$, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_{p^m}$. □

We construct qMDS codes from negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ in the following theorem.

Theorem 18:

(a) If $p^m \equiv 1 \pmod 4$, then negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are $\langle (x-\gamma)^i (x+\gamma)^j \rangle \subseteq \mathcal{R}_{-1}$, where $\gamma^2 = -1$ and $0 \le i, j \le p^s$. Each code $\mathcal{C}_{i,j} = \langle (x-\gamma)^i (x+\gamma)^j \rangle$ contains $p^{m(2p^s-i-j)}$ codewords, its dual is $\mathcal{C}_{i,j}^\perp = \langle (x-\gamma)^{p^s-i} (x+\gamma)^{p^s-j} \rangle$. Then the following statements hold:

- *If $i = j = 0$, then there exists a qMDS code with parameters $[[2p^s, 2p^s, 1]]_{p^m}$.*
- *If $i = 1, j = 0$, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_{p^m}$.*
- *If $i = 0, j = 1$, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_{p^m}$.*

(b) If $p^m \equiv 3 \pmod 4$, then negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are $\langle (x^2+1)^i \rangle \subseteq \mathcal{R}_{-1}$, where $0 \le i \le p^s$. Then there exists a qMDS code with parameters $[[2p^s, 2p^s, 1]]_{p^m}$.

Proof: Using the proof in Theorem 17, we can prove (a). If $p^m \equiv 3 \pmod 4$, then negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are of the form $\langle (x^2+1)^i \rangle \subseteq \mathcal{R}_{-1}$, where $0 \le i \le p^s$.

Each code $C_i = \langle (x^2+1)^i \rangle$ contains $p^{2m(p^s-i)}$ codewords, its dual is $C_i^\perp = \mathcal{C}_{p^s-i} = \langle (x^2+1)^{p^s-i} \rangle$. This implies that $C_i^\perp \subseteq C_i$ if $i \leq \frac{p^s}{2}$. Let $C_i = [2p^s, k_i, \mathrm{d_H}(C_i)]_{p^m}$ be an MDS negacyclic code satisfying $C_i^\perp \subseteq C_i$. Then we have $k_i = 2p^s - \mathrm{d_H}(C_i) + 1$. From $C_i^\perp \subseteq C_i$, by Theorem 15 (the CSS construction), there exists a quantum code D_i with parameters $[[2p^s, 2k_i - 2p^s, \mathrm{d_H}(C_i)]]_{p^m}$. Since $k_i = 2p^s - \mathrm{d_H}(C_i) + 1$, we have $2k_i - 2p^s = 2p^s - 2\,\mathrm{d_H}(C_i) + 2$. Using Theorem 16, D_i is a qMDS code with parameters $[[2p^s, 2k_i - p^s, \mathrm{d_H}(C_i)]]_{p^m}$. Hence, if $C_i = [2p^s, k_{i,j}, \mathrm{d_H}(C_{i,j})]_{p^m}$ is an MDS negacyclic code and $C_i^\perp \subseteq C_i$, there exists a qMDS code with parameters $[[2p^s, 2p^s - 2\,\mathrm{d_H}(C_i) + 2, \mathrm{d_H}(C_j)]]_{p^m}$. Applying Theorem 8, there exists a qMDS code with parameters $[[2p^s, 2p^s, 1]]_{p^m}$, proving (b). □

Example 19: Consider all cyclic codes of length 6 over $\mathbb{F}_3$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_3[x]}{\langle x^6-1 \rangle}$, where $0 \leq i, j \leq 3$. Here, $p = 3, s = 1$ and $m = 1$. Applying Theorem 17, all qMDS codes constructed from $C_{i,j}$ using the CSS construction are determined in the following table.

TABLE 7. qMDS codes of length 6 over $\mathbb{F}_3$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[6,6,1]]_3$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[6,4,2]]_3$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[6,4,2]]_3$

Example 20: Consider all cyclic codes of length 14 over $\mathbb{F}_7$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_7[x]}{\langle x^{14}-1 \rangle}$, where $0 \leq i, j \leq 7$. Here, $p = 7, s = 1$ and $m = 1$. Applying Theorem 17, all qMDS codes constructed from $C_{i,j}$ using the CSS construction are determined in the following table.

TABLE 8. qMDS codes of length 14 over $\mathbb{F}_7$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[14,14,1]]_7$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[14,12,2]]_7$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[14,12,2]]_7$

Example 21: Consider all cyclic codes of length 18 over $\mathbb{F}_9$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_9[x]}{\langle x^{18}-1 \rangle}$, where $0 \leq i, j \leq 9$. Here, $p = 3, s = 2$ and $m = 2$. Applying Theorem 17, all qMDS codes constructed from $C_{i,j}$ using the CSS construction are determined in the following table.

TABLE 9. qMDS codes of length 18 over $\mathbb{F}_9$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[18,18,1]]_9$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[18,16,2]]_9$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[18,16,2]]_9$

Example 22: Consider all cyclic codes of length 22 over $\mathbb{F}_{11}$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_{11}[x]}{\langle x^{22}-1 \rangle}$, where $0 \leq i, j \leq 11$. Here, $p = 11, s = 1$ and $m = 1$. We determine all MDS cyclic codes of length 22 over $\mathbb{F}_{11}$. Applying Theorem 17, all qMDS codes constructed from $C_{i,j}$ using the CSS construction are determined in the following table.

TABLE 10. qMDS cyclic codes of length 22 over $\mathbb{F}_{11}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[22,22,1]]_{11}$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[22,20,2]]_{11}$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[22,20,2]]_{11}$

We now construct qMDS codes from cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the Hermitian construction. Let $q = p^m$ and $\mathbb{F}_{q^2}$ be a finite field of q^2 elements. If $e = (e_0, e_1, \ldots, e_{n-1}), t = (t_0, t_1, \cdots, t_{n-1})$ are two vectors of $\mathbb{F}_{q^2}$, then Hermitian inner product of e and t is

$$e \circ_{\mathbb{F}_{q^2}} t = e_0 \bar{t}_0 + e_1 \bar{t}_1 + \cdots + e_{n-1} \bar{t}_{n-1},$$

where $\bar{t}_i = t_i^q$. The Hermitian dual code of C is defined as

$$C^{\perp_H} = \{ e \in \mathbb{F}_{q^2}^n \mid \sum_{i=0}^{n-1} e_i \bar{t}_i = 0, \forall t \in C \}.$$

If $C^{\perp_H} \subseteq C$, then C is said to be *Hermitian dual-containing*.

Other than the CSS construction, the so-called Hermitian construction is also an important construction, which is given in [1].

Theorem 23 (Hermitian Construction) [1]: If C is a q^2-ary $[n, k, d_H]$ linear code such that $C^{\perp_H} \subseteq C$, then there exists a q-ary quantum code with parameters $[[n, 2k-n, \geq d_H]]_q$.

Let $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ be a cyclic code of length $2p^s$ over $\mathbb{F}_{q^2}$, where $0 \leq i, j \leq p^s$. This implies that $C_{i,j}^{\perp_H} = \langle (x-1)^{p^s-i} (x+1)^{p^s-j} \rangle$. If $0 \leq i, j \leq \frac{p^s}{2}$, then $C_{i,j}^{\perp_H} \subseteq C_{i,j}$.

We now construct qMDS codes from $C_{i,j}$ using the Hermitian construction.

Theorem 24: Let $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ be a cyclic code of length $2p^s$ over $\mathbb{F}_{q^2}$, where $0 \leq i, j \leq p^s$. Then the following statements hold:

- *If $i = j = 0$, there exists a qMDS code with parameters $[[p^s, p^s, 1]]_q$.*
- *If $i = 1, j = 0$, there exists a qMDS code with parameters $[[p^s, p^s - 2, 2]]_q$.*
- *If $i = 0, j = 1$, there exists a qMDS code with parameters $[[p^s, p^s - 2, 2]]_q$.*

Proof: Let $C_{i,j} = [2p^s, k_{i,j}, \mathrm{d_H}(C_{i,j})]_{q^2}$ be an MDS cyclic code satisfying $C_{i,j}^{\perp_H} \subseteq C_{i,j}$. Then we have $k_{i,j} = p^s - \mathrm{d_H}(C_{i,j}) + 1$ and $0 \leq i, j \leq \frac{p^s}{2}$. From $C_{i,j}^{\perp_H} \subseteq C_{i,j}$, by Theorem 22 (the Hermitian construction), there exists a quantum code $E_{i,j}$ with parameters $[[2p^s, 2k_{i,j} - 2p^s, d^\star]]_q$, where $d^\star \geq \mathrm{d_H}(C_{i,j})$. Applying Theorem 16 for $E_{i,j}$, we see that $2k_{i,j} - 2p^s + 2d^\star \leq 2p^s + 2$. It means that $d^\star \leq 2p^s - k_{i,j} + 1 = \mathrm{d_H}(C_{i,j})$. Hence, if $C_{i,j} = [2p^s, k_{i,j}, \mathrm{d_H}(C_{i,j})]_q$ is an MDS cyclic code and $C_{i,j}^{\perp_H} \subseteq C_{i,j}$, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2\,\mathrm{d_H}(C_{i,j}) + 2, \mathrm{d_H}(C_{i,j})]]_q$. We consider 2 cases as follows:

Case 1: $i = j = 0$. In this case, we have $\mathrm{d_H}(C_{0,0}) = 1$. By Theorem 9, $C_{0,0} = [2p^s, 2p^s, 1]_{q^2}$ is an MDS constacyclic code. From $i = j = 0$, we see that $C_{0,0}^{\perp_H} \subseteq C_{0,0}$. As there exists a qMDS code with parameters $[[2p^s, 2p^s - 2\,\mathrm{d_H}(C_{i,j}) + 2, \geq \mathrm{d_H}(C_{i,j})]]_q$, we have a qMDS code with parameters $[[2p^s, 2p^s, 1]]_q$.

Case 2: $i = 1, j = 0$. In this case, $\mathrm{d_H}(C_{1,0}) = 2$. Applying Theorem 9, we can see that $C_{1,0}$ is an MDS cyclic code. As $i = 1$ and $j = 0$, we have $C_{1,0}^{\perp_H} \subseteq C_{1,0}$. Because there exists a qMDS code with parameters $[[2p^s, 2p^s - 2\,\mathrm{d_H}(C_{i,j}) + 2, \mathrm{d_H}(C_{i,j})]]_q$, we have a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_q$.

Case 3: $i = 0, j = 1$. From Case 2, by symmetry, if $i = 0, j = 1$, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_q$. □

Using the proof of Theorem 24, we can construct qMDS codes from negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the Hermitian construction.

Theorem 25: (a) If $p^m \equiv 1 \pmod 4$, *then negacyclic codes of length* $2p^s$ *over* $\mathbb{F}_{p^m}$ *are* $\langle (x-\gamma)^i (x+\gamma)^j \rangle \subseteq \mathcal{R}_{-1}$, *where* $\gamma^2 = -1$ *and* $0 \leq i, j \leq p^s$. *Then the following statements hold*:

- *If* $i = j = 0$, *then there exists a qMDS code with parameters* $[[2p^s, 2p^s, 1]]_q$.
- *If* $i = 1, j = 0$, *then there exists a qMDS code with parameters* $[[2p^s, 2p^s - 2, 2]]_q$.
- *If* $i = 0, j = 1$, *then there exists a qMDS code with parameters* $[[2p^s, 2p^s - 2, 2]]_q$.

(b) If $p^m \equiv 3 \pmod 4$, *then negacyclic codes of length* $2p^s$ *over* $\mathbb{F}_{p^m}$ *are* $\langle (x^2+1)^i \rangle \subseteq \mathcal{R}_{-1}$, *where* $0 \leq i \leq p^s$. *Then there exists a qMDS code with parameters* $[[2p^s, 2p^s, 1]]_q$.

We give some examples of qMDS codes constructed from cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the Hermitian construction.

Example 26: Consider all cyclic codes of length 6 over $\mathbb{F}_9$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_9[x]}{\langle x^6 - 1 \rangle}$, where $0 \leq i, j \leq 3$. Here, $p = 3, s = 1$ and $m = 2$. We give all qMDS codes constructed from $C_{i,j}$ using the Hermitian construction.

TABLE 11. qMDS codes of length 6 over $\mathbb{F}_9$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[6, 6, 1]]_3$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[6, 4, 2]]_3$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[6, 4, 2]]_3$

Example 27: Consider all cyclic codes of length 14 over $\mathbb{F}_{49}$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_{49}[x]}{\langle x^{14} - 1 \rangle}$, where $0 \leq i, j \leq 7$. Here, $p = 7, s = 1$ and $m = 2$. We give all qMDS codes constructed from $C_{i,j}$ using the Hermitian construction.

Example 28: Consider all cyclic codes of length 18 over $\mathbb{F}_{81}$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_{81}[x]}{\langle x^{18} - 1 \rangle}$, where $0 \leq i, j \leq 9$. Here, $p = 3, q = 9, s = 2$ and $m = 4$. We give all qMDS codes constructed from $C_{i,j}$ using the Hermitian construction.

TABLE 12. qMDS codes of length 14 over $\mathbb{F}_{49}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[14, 14, 1]]_7$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[14, 12, 2]]_7$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[14, 12, 2]]_7$

TABLE 13. qMDS codes of length 18 over $\mathbb{F}_{81}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[18, 18, 1]]_9$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[18, 16, 2]]_9$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[18, 16, 2]]_9$

Example 29: Consider all cyclic codes of length 22 over $\mathbb{F}_{11}$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_{11}[x]}{\langle x^{22} - 1 \rangle}$, where $0 \leq i, j \leq 11$. Here, $p = 11, s = 1$ and $m = 1$. We determine all MDS cyclic codes of length 22 over $\mathbb{F}_{11}$. Applying Theorem 17, all qMDS codes constructed from $C_{i,j}$ using the CSS construction are determined in the following table.

TABLE 14. qMDS cyclic codes of length 22 over $\mathbb{F}_{11}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
0	0	$C_{0,0} = \langle 1 \rangle$	1	Yes	$[[22, 22, 1]]_{11}$
0	1	$C_{0,1} = \langle (x+1) \rangle$	2	Yes	$[[22, 20, 2]]_{11}$
1	0	$C_{1,0} = \langle (x-1) \rangle$	2	Yes	$[[22, 20, 2]]_{11}$

The following lemma is known in [95].

Lemma 30 [95, Proposition 2.1.2]; The dual of an MDS code $C = [n, k, n-k+1]_q$ *is still an MDS code with parameters* $[n, n-k, k+1]_q$.

We spend the rest of this section to construct qMDS codes from dual codes of cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using the Hermitian construction. Let $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ be a cyclic code of length $2p^s$ over $\mathbb{F}_{q^2}$, where $0 \leq i, j \leq p^s$. Put $D_{i,j} = C_{i,j}^{\perp}$. By Theorem 2, we have $D_{i,j} = C_{i,j}^{\perp} = \langle (x-1)^{p^s - i} (x+1)^{p^s - j} \rangle$, where $0 \leq i, j \leq p^s$. It implies that $D_{i,j}^{\perp_H} = \langle (x-1)^i (x+1)^j \rangle$. Hence, if $i, j \geq \frac{p^s}{2}$, then $D_{i,j}^{\perp_H} \subseteq D_{i,j}$. We have the following result.

Theorem 31: Let $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ *be a cyclic code of length* $2p^s$ *over* $\mathbb{F}_{q^2}$, *where* $0 \leq i, j \leq p^s$. *Put* $D_{i,j} = C_{i,j}^{\perp} = \langle (x-1)^{p^s - i} (x+1)^{p^s - j} \rangle$, *where* $0 \leq i, j \leq p^s$. *Then the following statements hold*:

- *If* $i = p^s, j = p^s - 1$, *then there exists a qMDS code with parameters* $[[2p^s, 2p^s - 2, 2]]_q$.
- *If* $i = p^s - 1, j = p^s$, *then there exists a qMDS code with parameters* $[[2p^s, 2p^s - 2, 2]]_q$.

Proof: Assume that $C_{i,j} = [2p^s, k_{i,j}, 2p^s - k_{i,j} + 1]_{q^2}$ is an MDS cyclic code and $i, j \geq \frac{p^s}{2}$. Applying Lemma 30, we can see that $C_{i,j}^{\perp} = [p^s, p^s - k_{i,j}, k_{i,j} + 1]_{q^2}$ is also an MDS cyclic code. Put $D_{i,j} = C_{i,j}^{\perp} = [p^s, p^s - k_{i,j}, k_{i,j} + 1]_{q^2}$. From $i, j \geq \frac{p^s}{2}$, we have $D_{i,j}^{\perp_H} \subseteq D_{i,j}$. Using the Hermitian construction, there exists a q-ary quantum code with parameters

$D'_{i,j} = [[2p^s, 2p^s - 2k_{i,j}, d']]_q$, where $d' \geq k_{i,j} + 1$. Applying Theorem 16 for $D'_{i,j}$, we see that $d' \leq k_{i,j} + 1$. This implies that $d' = k_{i,j} + 1$. Hence, there exists a qMDS code $D'_{i,j}$ with parameters $[[2p^s, 2p^s - 2k_{i,j}, k_{i,j} + 1]]_q$. From $i = p^s > \frac{p^s}{2}$ and $j = p^s - 1 > \frac{p^s}{2}$, we have a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_q$. By symmetry, it is easy to see that there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_q$ when $i = p^s - 1, j = p^s$. □

Remark 32: If $p^m \equiv 3 \pmod 4$, then negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are $\langle (x^2+1)^i \rangle \subseteq \mathcal{R}_{-1}$, where $0 \leq i \leq p^s$. Put $D_i = C_i^{\perp} = \langle (x^2+1)^{p^s - i} \rangle$. If $i \geq \frac{p^s}{2}$, then $D_i^{\perp_H} \subseteq D_i$. From Theorem 8, we see that we can not construct any qMDS codes from D_i using the Hermitian construction when $p^m \equiv 3 \pmod 4$. If $p^m \equiv 1 \pmod 4$, by using Theorem 31, then there exists a qMDS code with parameters $[[2p^s, 2p^s - 2, 2]]_q$.

Using the Hermitian construction for $D_j = C_j^{\perp}$, we finish this section by giving some examples of qMDS codes.

Example 33: Consider all cyclic codes of length 6 over $\mathbb{F}_9$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_9[x]}{\langle x^6 - 1 \rangle}$, where $0 \leq i, j \leq 3$. Put $D_{i,j} = C_{i,j}^{\perp} = \langle (x-1)^{p^s - i} (x+1)^{p^s - j} \rangle$, where $0 \leq i, j \leq 3$. Here, $p = 3, s = 1$ and $m = 2$. We give all qMDS codes constructed from $D_{i,j}$ using the Hermitian construction.

TABLE 15. qMDS codes of length 6 over $\mathbb{F}_9$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
3	2	$C_{3,2} = \langle (x+1)^2 (x-1)^3 \rangle$	6	Yes	$[[6, 4, 2]]_3$
2	3	$C_{2,3} = \langle (x+1)^3 (x-1)^2 \rangle$	6	Yes	$[[6, 4, 2]]_3$

Example 34: Consider all cyclic codes of length 14 over $\mathbb{F}_{49}$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_{49}[x]}{\langle x^{14} - 1 \rangle}$, where $0 \leq i, j \leq 7$. Put $D_{i,j} = C_{i,j}^{\perp} = \langle (x-1)^{p^s - i} (x+1)^{p^s - j} \rangle$, where $0 \leq i, j \leq 7$. Here, $p = 7, s = 1$ and $m = 2$. We give all qMDS codes constructed from $D_{i,j}$ using the Hermitian construction.

TABLE 16. qMDS codes of length 14 over $\mathbb{F}_{49}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
6	7	$C_{6,7} = \langle (x+1)^7 (x-1)^6 \rangle$	14	Yes	$[[14, 12, 2]]_7$
7	6	$C_{7,6} = \langle (x+1)^6 (x-1)^7 \rangle$	14	Yes	$[[14, 12, 2]]_7$

Example 35: Consider all cyclic codes of length 18 over $\mathbb{F}_{81}$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_{81}[x]}{\langle x^{18} - 1 \rangle}$, where $0 \leq i, j \leq 9$. Put $D_{i,j} = C_{i,j}^{\perp} = \langle (x-1)^{p^s - i} (x+1)^{p^s - j} \rangle$, where $0 \leq i, j \leq 18$. Here, $p = 3, s = 2$ and $m = 4$. We give all qMDS codes constructed from $D_{i,j}$ using the Hermitian construction.

TABLE 17. qMDS codes of length 18 over $\mathbb{F}_{81}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
8	9	$C_{8,9} = \langle (x+1)^9 (x-1)^8 \rangle$	18	Yes	$[[18, 16, 2]]_9$
9	8	$C_{9,8} = \langle (x+1)^8 (x-1)^9 \rangle$	18	Yes	$[[18, 16, 2]]_9$

Example 36: Consider all cyclic codes of length 22 over $\mathbb{F}_{121}$ which are the ideals $C_{i,j} = \langle (x-1)^i (x+1)^j \rangle$ of $\frac{\mathbb{F}_{121}[x]}{\langle x^{22} - 1 \rangle}$, where $0 \leq i, j \leq 11$. Here, $p = 11, s = 1$ and $m = 1$. We determine all MDS cyclic codes of length 22 over $\mathbb{F}_{121}$. Applying Theorem 17, all qMDS codes constructed from $C_{i,j}$ using the CSS construction are determined in the following table.

TABLE 18. qMDS cyclic codes of length 22 over $\mathbb{F}_{11}$.

i	j	$C_{i,j}$	$\mathrm{d_H}(C_{i,j})$	MDS code	qMDS code
10	11	$C_{10,11} = \langle (x+1)^{11} (x-1)^{10} \rangle$	22	Yes	$[[22, 20, 2]]_{11}$
11	10	$C_{11,10} = \langle (x+1)^{10} (x-1)^{11} \rangle$	22	Yes	$[[22, 20, 2]]_{11}$

Remark 37: We can compare our qMDS codes and known families of qMDS codes (Table 6) and [29] to see that our qMDS codes are new in the sense that their parameters are different from all the known ones.

V. QUANTUM SYNCHRONIZABLE CODES

An $(a_l, a_r) - [[n, k]]$ QSC is an $[[n, k]]$ QEC code that corrects not only bit errors and phase errors but also misalignment to the left by a_l qubits and to the right by a_r qubits for some non-negative integers a_l and a_r. The class of QSCs is a special class of QEC codes that is constructed to correct quantum noise as well as block synchronization. In QEC codes, operators act on qubits through quantum noise. In quantum synchronizable, each qubit is acted by the Pauli operators I, X, Y, and Z which are usually appeared in the general model. Therefore, QSCs are proposed to correct Pauli operators. QSCs have allowed for knowing the extract the Pauli errors on qubits. Block synchronization is used to ensure that the information transmitted through block boundaries to a receiver. Several techniques for block synchronization have been constructed from classical communication systems. However, since a qubit measurement typically destroys the quantum states, these techniques for block synchronization can not be applicable to QSCs. To give a solution for this problem, in [25], Fujiwara provided a framework for quantum block synchronization which allows to prevent the destruction of qubits in the quantum states. The approach given in [25] allowed us to eliminate the effects caused by block misalignment and Pauli errors. In his paper, the construction of good QSCs demands a pair of nested dual-containing cyclic codes, both of which guarantee large minimum distances.

After that, several QSCs constructed from classical BCH codes and punctured RM codes are given in [27]. Later, the authors in [28], [59], [90], [91] showed that finite geometric codes, quadratic residue codes, duadic codes and repeated-root codes can be applied in synchronization coding. In [59], [60], Luo *et al.* proved that repeated-root cyclic codes are useful in QSCs with better parameters in correcting Pauli errors than non-primitive, narrow-sense BCH codes and other available QSCs.

Let ℓ be an integer such that $\ell \geq 2$ and $\gcd(\ell, p) = 1$. Assume that $C_{t,\ell}$ is the cyclotomic coset of t modulo ℓ over

$\mathbb{F}_{p^m}$ and denote by T_ℓ the set of representatives of all p^m-ary cyclotomic cosets. Let $M_t(x) = \prod_{i \in C_{t,\ell}}(x - \xi^i)$ be the minimal polynomial of ξ^t over $\mathbb{F}_{p^m}$, where ξ is a primitive ℓ-th root of unity in $\mathbb{F}_{p^m}$. Then the polynomial $x^{\ell p^s} - 1$ over $\mathbb{F}_{p^m}$ can be factored as

$$x^{\ell p^s} - 1 = (x^\ell - 1)^{p^s} = \prod_{t \in T_\ell} (M_t(x))^{p^s}.$$

In [59], Luo *et al.* gave some QSCs constructed from the class of cyclic codes of length ℓp^s over $\mathbb{F}_{p^m}$.

Theorem 38 [59, Theorem 3]: Let $C_1 = \langle \prod_{t \in T_\ell}(M_t(x))^{i_t} \rangle$ *and* $C_2 = \langle \prod_{t \in T_\ell}(M_t(x))^{j_t} \rangle$ *be cyclic codes of length* ℓp^s *over* $\mathbb{F}_{p^m}$ *satisfying* $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$, *and* $C_1 \subset C_2$. *Then the following conditions hold*:

(*i*) $i_t + i_{-t} \le p^s$.
(*ii*) $j_t + j_{-t} \le p^s$.
(*iii*) $0 \le j_t < i_t \le p^s$.

In such cases, if there exists an integer $r \in T_\ell$ *with* $\gcd(r, \ell) = 1$ *satisfying either* $i_r - j_r > p^{s-1}$ *or* $i_r - j_r > 0$ *and* $i_{r'} - j_{r'} > p^{s-1}$ *for some* $r' \ne r \in T_\ell$, *then for any pair of non-negative integers* a_l, a_r *satisfying* $a_l + a_r < \ell p^s$, *there exists an* (a_l, a_r)-$[[\ell p^s + a_l + a_r, \ell p^s - 2\sum_{t \in T_\ell} i_t |C_{t,\ell}|]]_{p^m}$ *QSC.*

Applying Theorem 38, we can obtain QSCs from repeated-root cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ as follows.

Theorem 39: Let $C_1 = \langle (x-1)^{u_0}(x+1)^{u_1} \rangle \subseteq R_1$ *and* $C_2 = \langle (x-1)^{j_0}(x+1)^{j_1} \rangle$ *be cyclic codes of length* $2p^s$ *over* $\mathbb{F}_{p^m}$ *satisfying* $C_1^\perp \subseteq C_1$, $C_2^\perp \subseteq C_2$ *and* $C_1 \subseteq C_2$, *where* $0 \le u_0, u_1, j_0, j_1 \le p^s$. *Then the following conditions hold*:

(*i*) $0 \le u_0 \le \frac{p^s}{2}$, $0 \le u_1 \le \frac{p^s}{2}$.
(*ii*) $0 \le j_0 \le \frac{p^s}{2}$, $0 \le j_1 \le \frac{p^s}{2}$.
(*iii*) $0 \le j_i < u_i \le p^s$, *where* $i = 0, 1, 2$.

In such cases, if there exists an integer $r \in T_2$ *satisfying either* $u_r - j_r > p^{s-1}$ *or* $u_r - j_r > 0$ *and* $u_{r'} - j_{r'} > p^{s-1}$ *for some* $r' \ne r \in T_2$, *then for any pair of non-negative integers* a_l, a_r *satisfying* $a_l + a_r < 2p^s$, *there exists an* $(a_l, a_r) - [[2p^s + a_l + a_r, 2p^s - 2u_0 - 2u_1]]_{p^m}$ *QSC. If we fix* u_i, j_i, r, *where* $i = 0, 1$ *and* $r \in T_2$, *then there are* $p^s \cdot (2p^s + 1)$ *such QSCs.*

Proof: Since $C_1^\perp = \langle (x-1)^{p^s - u_0}(x+1)^{p^s - u_1} \rangle \subseteq C_1$ and $C_2^\perp = \langle (x-1)^{p^s - j_0}(x+1)^{p^s - j_1} \rangle \subseteq C_2$, we have $p^s - u_0 \ge u_0, p^s - u_1 \ge u_1, p^s - j_0 \ge j_0$ and $p^s - j_1 \ge j_1$, i.e., $0 \le u_0 \le \frac{p^s}{2}$, $0 \le u_1 \le \frac{p^s}{2}$, $0 \le j_0 \le \frac{p^s}{2}$, and $0 \le j_1 \le \frac{p^s}{2}$, showing (*i*) and (*ii*). From $C_1 \subseteq C_2$, it implies that $0 \le j_i < u_i \le p^s$, proving (*iii*). Since $C_1^\perp \subseteq C_1$, $C_2^\perp \subseteq C_2$, and $C_1 \subseteq C_2$, applying Theorem 38, if there exists an integer $r \in T_2$ satisfying either $u_r - j_r > p^{s-1}$ or $u_r - j_r > 0$ and $u_{r'} - j_{r'} > p^{s-1}$ for some $r' \ne r \in T_2$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 2p^s$, there exists an $(a_l, a_r) - [[2p^s + a_l + a_r, 2p^s - u_0 - u_1]]_{p^m}$ QSC. Assume that u_i, j_i, r are fixed, where $i = 0, 1$ and $r \in T_2$. Applying Lemma 7 for $n = 2p^s - 1$, we see that there are $p^s \cdot (2p^s + 1)$ pairs of non-negative integers a_l, a_r satisfying $a_l + a_r < 2p^s$. It means that there are $p^s \cdot (2p^s + 1)$ such QSCs. □

We finish this section by giving some examples of QSCs.

Example 40: Assume that $p = 7$ and $s = 1, m = 1$. Then we have $x^{14} - 1 = (x-1)^7(x+1)^7$.

- Let $C_1 = \langle (x-1)(x+1)^3 \rangle$ and $C_2 = \langle (x+1) \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_1^\perp \subseteq C_1$, $C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_1 - j_1 = 2 > p^{s-1} = 1$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 14$, there exists an $(a_l, a_r) - [[14 + a_l + a_r, 6]]_7$ QSC. In this case, there are 105 such QSCs.
- If $C_3 = \langle (x-1)^3(x+1)^3 \rangle$ and $C_4 = \langle (x-1)(x+1) \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_3^\perp \subseteq C_3$, $C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 = 2 > p^{s-1} = 1$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 14$, there exists an $(a_l, a_r) - [[14 + a_l + a_r, 2]]_7$ QSC. In this case, there are 105 such QSCs.

Example 41: Assume that $p = 7$ and $s = 2, m = 1$. Then we have $x^{98} - 1 = (x-1)^{49}(x+1)^{49}$.

- Let $C_1 = \langle (x-1)^5(x+1)^{20} \rangle$ and $C_2 = \langle (x-1)^2(x+1)^5 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_1^\perp \subseteq C_1$, $C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_1 - j_1 = 15 > p^{s-1} = 7$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 98$, there exists an $(a_l, a_r) - [[98 + a_l + a_r, 48]]_7$ QSC. In this case, there are 4851 such QSCs.
- If $C_3 = \langle (x-1)^4(x+1)^{22} \rangle$ and $C_4 = \langle (x-1)(x+1)^4 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_3^\perp \subseteq C_3$, $C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 = 18 > p^{s-1} = 7$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 98$, there exists an $(a_l, a_r) - [[98 + a_l + a_r, 46]]_7$ QSC. In this case, there are 4851 such QSCs.

Example 42: Assume that $p = 7$ and $s = 2, m = 2$. Then we have $x^{98} - 1 = (x-1)^{49}(x+1)^{49}$.

- Let $C_1 = \langle (x-1)^5(x+1)^{16} \rangle$ and $C_2 = \langle (x-1)^4(x+1)^3 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_1^\perp \subseteq C_1$, $C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_1 - j_1 = 13 > p^{s-1} = 7$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 98$, there exists an $(a_l, a_r) - [[98 + a_l + a_r, 48]]_{49}$ QSC. In this case, there are 4851 such QSCs.
- If $C_3 = \langle (x-1)^4(x+1)^{21} \rangle$ and $C_4 = \langle (x-1)(x+1)^8 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_3^\perp \subseteq C_3$, $C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 = 13 > p^{s-1} = 7$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 98$, there exists an $(a_l, a_r) - [[98 + a_l + a_r, 48]]_{49}$ QSC. In this case, there are 4851 such QSCs.

Example 43: Assume that $p = 11$ and $s = 1, m = 1$. Then we have $x^{22} - 1 = (x-1)^{11}(x+1)^{11}$.

• Let $C_1 = \langle (x-1)^5(x+1)^5 \rangle$ and $C_2 = \langle (x-1)^2(x+1) \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_1 - j_1 = 4 > p^{s-1} = 1$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 22$, there exists an $(a_l, a_r) - [[22 + a_l + a_r, 2]]_{11}$ QSC. In this case, there are 253 such QSCs.

• If $C_3 = \langle (x-1)^4(x+1)^5 \rangle$ and $C_4 = \langle (x-1)(x+1)^2 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_3^\perp \subseteq C_3, C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 = 3 > p^{s-1} = 1$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 22$, there exists an $(a_l, a_r) - [[22 + a_l + a_r, 4]]_{11}$ QSC. In this case, there are 253 such QSCs.

Example 44: Assume that $p = 11$ and $s = 2, m = 1$. Then we have $x^{242} - 1 = (x-1)^{121}(x+1)^{121}$.

• Let $C_1 = \langle (x-1)^{25}(x+1)^{35} \rangle$ and $C_2 = \langle (x-1)^2(x+1) \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_1 - j_1 = 34 > p^{s-1} = 11$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 242$, there exists an $(a_l, a_r) - [[242 + a_l + a_r, 122]]_{11}$ QSC. In this case, there are 29403 such QSCs.

• If $C_3 = \langle (x-1)^{14}(x+1)^{25} \rangle$ and $C_4 = \langle (x-1)(x+1)^5 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_3^\perp \subseteq C_3, C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 = 20 > p^{s-1} = 11$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 242$, there exists an $(a_l, a_r) - [[242 + a_l + a_r, 164]]_{11}$ QSC. In this case, there are 29403 such QSCs.

Example 45: Assume that $p = 11$ and $s = 2, m = 2$. Then we have $x^{242} - 1 = (x-1)^{121}(x+1)^{121}$.

• Let $C_1 = \langle (x-1)^{25}(x+1)^{39} \rangle$ and $C_2 = \langle (x-1)^2(x+1)^7 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. We see that $u_1 - j_1 = 32 > p^{s-1} = 11$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 242$, there exists an $(a_l, a_r) - [[242 + a_l + a_r, 122]]_{121}$ QSC. In this case, there are 29403 such QSCs.

• If $C_3 = \langle (x-1)^{14}(x+1)^{25} \rangle$ and $C_4 = \langle (x-1)(x+1)^5 \rangle$. It is easy to see that $0 \le j_0 < u_0 < \frac{p^s}{2}$, $0 \le j_1 < u_1 < \frac{p^s}{2}$, i.e., $C_3^\perp \subseteq C_3, C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. We see that $u_1 - j_1 = 20 > p^{s-1} = 11$, then for any pair of non-negative integers a_l, a_r satisfying $a_l + a_r < 242$, there exists an $(a_l, a_r) - [[242 + a_l + a_r, 164]]_{121}$ QSC. In this case, there are 29403 such QSCs.

Example 46: If $p = 17$ and $s = m = 1$, then we have $x^{34} - 1 = (x-1)^{17} f(x)^{17}$.

• If $C_1 = \langle (x-1)(x+1)^8 \rangle$ and $C_2 = \langle (x+1)^2 \rangle$, then $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 34$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 16]]_{17}$ QSC. In this case, there are 595 such QSCs.

• If $C_3 = \langle (x-1)^5(x+1)^7 \rangle$ and $C_4 = \langle (x-1)(x+1) \rangle$, then $C_3^\perp \subseteq C_3, C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 34$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 10]]_{17}$ QSC. In this case, there are 595 such QSCs.

• If $C_5 = \langle (x-1)^4(x+1)^6 \rangle$ and $C_6 = \langle (x-1)(x+1)^3 \rangle$, then $C_5^\perp \subseteq C_5, C_6^\perp \subseteq C_6$ and $C_5 \subseteq C_6$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 34$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 14]]_{17}$ QSC. In this case, there are 595 such QSCs.

Example 47: If $p = 17$ and $s = 2, m = 1$, then we have $x^{578} - 1 = (x-1)^{289}(x+1)^{289}$.

• If $C_1 = \langle (x-1)^7(x+1)^{48} \rangle$ and $C_2 = \langle (x+1)^5 \rangle$, then $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 578$, there exists an $(a_l, a_r) - [[578 + a_l + a_r, 523]]_{17}$ QSC. In this case, there are 167331 such QSCs.

• If $C_3 = \langle (x-1)^5(x+1)^7 \rangle$ and $C_4 = \langle (x-1)(x+1) \rangle$, then $C_3^\perp \subseteq C_3, C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 34$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 22]]_{17}$ QSC. In this case, there are 167331 such QSCs.

• If $C_5 = \langle (x-1)^4(x+1)^6 \rangle$ and $C_6 = \langle (x-1)(x+1) \rangle$, then $C_5^\perp \subseteq C_5, C_6^\perp \subseteq C_6$ and $C_5 \subseteq C_6$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 34$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 24]]_{17}$ QSC. In this case, there are 167331 such QSCs.

Example 48: If $p = 17$ and $s = 1, m = 2$, then we have $x^{34} - 1 = (x-1)^{17}(x+1)^{17}$.

• If $C_1 = \langle (x-1)(x+1)^9 \rangle$ and $C_2 = \langle (x+1)^2 \rangle$, then $C_1^\perp \subseteq C_1, C_2^\perp \subseteq C_2$ and $C_1 \subseteq C_2$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 85$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 25]]_{289}$ QSC. In this case, there are 595 such QSCs.

• If $C_3 = \langle (x-1)^5(x+1)^7 \rangle$ and $C_4 = \langle (x-1)(x+1) \rangle$, then $C_3^\perp \subseteq C_3, C_4^\perp \subseteq C_4$ and $C_3 \subseteq C_4$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 34$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 22]]_{289}$ QSC. In this case, there are 595 such QSCs.

• If $C_5 = \langle (x-1)^4(x+1)^6 \rangle$ and $C_6 = \langle (x-1)(x+1) \rangle$, then $C_5^\perp \subseteq C_5, C_6^\perp \subseteq C_6$ and $C_5 \subseteq C_6$. Applying Theorem 39, for any pair a_l, a_r of

non-negative integers satisfying $a_l + a_r < 34$, there exists an $(a_l, a_r) - [[34 + a_l + a_r, 24]]_{289}$ QSC. In this case, there are 595 such QSCs.

Example 49: If $p = 17$ and $s = 2, m = 2$, then we have $x^{578} - 1 = (x-1)^{289}(x+1)^{289}$.

- If $C_1 = \langle (x-1)^7(x+1)^{48} \rangle$ and $C_2 = \langle (x+1)^5$, then $C_1^{\perp} \subseteq C_1$, $C_2^{\perp} \subseteq C_2$ and $C_1 \subseteq C_2$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 578$, there exists an $(a_l, a_r) - [[578 + a_l + a_r, 468]]_{289}$ QSC. In this case, there are 167331 such QSCs.
- If $C_3 = \langle (x-1)^5(x+1)^{37} \rangle$ and $C_4 = \langle (x-1)(x+1) \rangle$, then $C_3^{\perp} \subseteq C_3$, $C_4^{\perp} \subseteq C_4$ and $C_3 \subseteq C_4$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 578$, there exists an $(a_l, a_r) - [[578 + a_l + a_r, 494]]_{289}$ QSC. In this case, there are 167331 such QSCs.
- If $C_5 = \langle (x-1)^4(x+1)^{56} \rangle$ and $C_6 = \langle (x-1)(x+1)^{10} \rangle$, then $C_5^{\perp} \subseteq C_5$, $C_6^{\perp} \subseteq C_6$ and $C_5 \subseteq C_6$. Applying Theorem 39, for any pair a_l, a_r of non-negative integers satisfying $a_l + a_r < 578$, there exists an $(a_l, a_r) - [[578 + a_l + a_r, 458]]_{289}$ QSC. In this case, there are 167331 such QSCs.

BCH codes are the most important class of cyclic codes. Due to their efficient encoding and decoding algorithms, BCH codes are widely used in error correction, communication and data storage. Let $\mathbb{F}_{p^m}$ be a finite field. Let n be a divisor of $p^m - 1$ and β be an element of $\mathbb{F}_{p^m}$ with multiplicative order n. A BCH code is a cyclic code with length n, whose generator polynomial has a set of $\delta - 1$ consecutive roots $\beta^b, \beta^{b+1}, \cdots, \beta^{b+\delta-2}$, where b is a positive integer. By the BCH bound, the minimum distance of the BCH code is at least δ. Thus, the BCH code has designed distance δ. A BCH code is called *primitive* if the length $n = p^m - 1$. A BCH code is called *narrow-sense* if $b = 1$, i.e., the $\delta - 1$ consecutive roots start from β.

Remark 50: Some parameters of primitive, narrow-sense BCH codes C over $\mathbb{F}_q$ provided in [59, Table 2] are given in Table 19. We list some parameters of repeated-root cyclic codes of length $2p^s$ over $\mathbb{F}_p$ in Table 20. The code lengths of repeated-root cyclic codes of length $2p^s$ over $\mathbb{F}_p$ are smaller than BCH codes given in Table 2 but the Hamming distances of repeated-root cyclic codes of length $2p^s$ over $\mathbb{F}_p$ are better than δ_{max}, where δ_{max} is a precise lower bound for the largest minimum distance of a dual-containing BCH code. Hence, QSCs constructed from repeated-root cyclic codes of length $2p^s$ over $\mathbb{F}_p$ are better than QSCs constructed from primitive, narrow-sense BCH codes.

TABLE 19. Some parameters of primitive, narrow-sense BCH codes over $\mathbb{F}_q$.

q	length	δ_{max}
3	242	25
7	342	43
11	1330	111
13	28560	168

TABLE 20. Some parameters of cyclic codes of length $2p^s$ over $\mathbb{F}_p$.

p	s	C	length	d_H
3	4	$\langle (x-1)^{81}(x+1)^{80} \rangle$	162	162
3	7	$\langle (x-1)^{2187}(x+1)^{2186} \rangle$	4374	2187
5	2	$\langle (x-1)^{125}(x+1)^{124} \rangle$	250	250
7	2	$\langle (x-1)^{49}(x+1)^{48} \rangle$	98	98
11	2	$\langle (x-1)^{121}(x+1)^{119} \rangle$	242	121
13	3	$\langle (x-1)^{2197}(x+1)^{2196} \rangle$	4394	4394

VI. CONCLUSION

In this paper, using the Singleton bound, we get all MDS cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ in Theorems 8 and 9. Examples $11 - 14$ provide some MDS codes over $\mathbb{F}_3, \mathbb{F}_7, \mathbb{F}_9, \mathbb{F}_{11}$. Theorems 17, 18, 24, 25, and 31 allow us to detemine all qMDS codes constructed from the class of cyclic and negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ using CSS and Hermitian constructions. Some examples of qMDS codes are provided (Examples 19-22, 26-29 and 33-36). As in Section 5, we construct QSCs from cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ (Theorem 39) and such codes are applicable in quantum synchronization. Examples 42-49 illustrate our work in Section 5. Remark 50 shows that QSCs constructed from repeated-root cyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ are better than QSCs constructed from primitive, narrow-sense BCH codes.

For future work, it is interesting to investigate the QSCs constructed from repeated-root constacyclic codes of length $4p^s$ over $\mathbb{F}_{p^m}$, or more generally $2^m p^s$, for any non-negative integer m. We believe that these lengths can provide good and new QSCs.

In addition, using the ideas in some papers [48], [64], [78]–[80], our results in this paper can be extended to generate some S-boxes for instance:

- BCH codes with computational approach and its applications in image encryption.
- Serpent algorithm: an improvement by S-box from finite chain rings.
- A new approach for image encryption and watermarking based on substitution box over the classes of chain rings.
- Maximal cyclic subgroups of the groups of units of Galois rings: a computational approach.
- Design of new S-box from finite commutative chain rings.

ACKNOWLEDGMENT

The authors sincerely thank the reviewers and the editor for their helpful comments and valuable suggestions, which have greatly improved the presentation of this article.

REFERENCES

[1] A. Ashikhmin and E. Knill, "Nonbinary quantum stablizer codes," *IEEE Trans. Inf. Theory*. vol. 47, no. 7, pp. 3065–3072, Nov. 2001.
[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and K. W. Wooters, "Mixed State Entanglement and Quantum Error Correction," *Phys. Rev. A, Gen. Phys.*, vol. 54, p. 3824, Oct. 1996.
[3] S. D. Berman, "Semisimple cyclic and Abelian codes. II," *Kibernetika*, vol. 3, no. 3, pp. 21–30, 1967.

[4] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon Greenberger-Horne-Zeilinger entanglement," *Phys. Rev. Lett.*, vol. 82, no. 7, pp. 1345–1349, Feb. 1999.
[5] S. Bregni, *Synchronization of Digital Telecommunications Networks*. New York, NY, USA: Wiley, 2002.
[6] T. Brun, I. Devetak, and H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, p. 436–439, Apr. 2006.
[7] K. A. Bush, "Orthogonal arrays of index unity," *Ann. Math. Statist.*, vol. 23, no. 3, pp. 426–434, Sep. 1952.
[8] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 2, pp. 1098–1106, Aug. 1996.
[9] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[10] B. Chen, H. Q. Dinh, and H. Liu, "Repeated-root constacyclic codes of length lp^s and their duals," *Discrete Appl. Math.*, vol. 177, pp. 60–70, Nov. 2014.
[11] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1474–1478, Mar. 2014.
[12] J. Chen, Y. Huang, C. Feng, and R. Chen, "Entanglement-assisted quantum MDS codes constructed from negacyclic codes," *Quantum Inf. Process.*, vol. 16, no. 12, p. 303, Dec. 2017.
[13] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A, Gen. Phys.*, vol. 56, no. 1, p. 76, 1997.
[14] J. Denes and A. D. Keedwell, *Latin Squares and Their Applications*. New York, NY, USA: Academic, 1974.
[15] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proc. Roy. Soc. London A*, vol. 400, no. 1818, pp. 97–117, Jul. 1985.
[16] H. Q. Dinh, "Constacyclic codes of length p^s over $\mathbb{F}_p^m + u\mathbb{F}_p^m$," *J. Algebra*, vol. 324, no. 5, pp. 940–950, 2010.
[17] H. Q. Dinh, "Repeated-root constacyclic codes of length $2p^s$," *Finite Fields Appl.*, vol. 18, no. 1, pp. 133–143, 2012.
[18] 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, May 2013.
[19] H. Q. Dinh, X. Wang, H. Liu, and S. Sriboonchitta, "On the symbol-pair distances of repeated-root constacyclic codes of length $2p^s$," *Discrete Math.*, vol. 342, no. 11, pp. 3062–3078, Nov. 2019.
[20] M. El-Khamy and R. J. McEliece, "The partition weight enumerator of MDS codes and its applications," in *Proc. Int. Symp. Inf. Theory*, May 2005, pp. 926–930.
[21] M. F. Ezerman, S. Jitman, M. Kiah, and S. Ling, "Pure asymmetric quantum MDS codes from CSS construction: A complete characterization," *Int. J. Quantum Inform.*, vol. 11, Dec. 2013, Art. no. 1350027.
[22] M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik, "CSS-like constructions of asymmetric quantum codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6732–6754, Oct. 2013.
[23] M. F. Ezerman, S. Ling, and P. Sole, "Additive asymmetric quantum codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5536–5550, Aug. 2011.
[24] W. Fang and F. Fu, "Two new classes of quantum MDS codes," *Finite Fields Appl.*, vol. 53, pp. 85–98, 2018.
[25] Y. Fujiwara, "Block synchronization for quantum information," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 2, p. 109, Feb. 2013.
[26] Y. Fujiwara and D. Tonchev, "High-rate self-synchronizing codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2328–2335, Apr. 2013.
[27] 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.
[28] Y. Fujiwara and P. Vandendriessche, "Quantum synchronizable codes from finite geometries," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7345–7354, Nov. 2014.
[29] M. Grassl. (2007). *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Apr. 19, 2011. [Online]. Available: http://www.codetables.de
[30] M. Grassl, T. Beth, and M. R. otteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, pp. 757–766, Oct. 2004.
[31] M. Grassl, A. Klappenecker, and M. Rotteler, "Graphs, quadratic forms, and quantum codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2002, p. 45.
[32] M. Grassl, T. Beth, and W. Geiselmann, "Quantum Reed–Solomon codes," in *Proc. AAECC*, Honolulu, HI, USA, Nov. 1999, pp. 231–244.
[33] M. Grassl and T. Beth, "Quantum BCH codes," in *Proc. Int. Symp. Theor. Electr. Eng.*, Magdeburg, Germany, 1999, pp. 207–212.
[34] S. Golomb and E. Posner, "Rook domains, Latin squares, affine planes, and error-distributing codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 3, pp. 196–208, Jul. 1964.
[35] D. Gottesman. (1997). *Caltech*. [Online]. Available: http://www.quantph.com/9705052
[36] G. G. La Guardia, "Constructions of new families of nonbinary quantum codes," *Phys. Rev. A, Gen. Phys.*, vol. 80, no. 4, Oct. 2009, Art. no. 042331.
[37] G. G. L. Guardia, "Asymmetric quantum Reed–Solomon and generalized Reed–Solomon codes," *Quantum Inf. Process.*, vol. 11, pp. 591–604, May 2012.
[38] G. G. L. Guardia, "Asymmetric quantum codes: New codes from old," *Quantum Inf Process*, vol. 12, pp. 2771–2790, 2013.
[39] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Designs, Codes Cryptogr.*, vol. 86, no. 1, pp. 121–136, Jan. 2018.
[40] D. Hu, W. Tang, M. Zhao, Q. Chen, S. Yu, and C. H. Oh, "Graphical nonbinary quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 1, pp. 1–11, Jul. 2008.
[41] L. Ioffe and M. Mézard, "Asymmetric quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 75, no. 3, Mar. 2007, Art. no. 032345.
[42] D. D. Joshi, "A note on upper bounds for minimum distance codes," *Inf. Control*, vol. 1, no. 3, pp. 289–295, Sep. 1958.
[43] L. Jin, H. Kan, and J. Wen, "Quantum MDS codes with relatively large minimum distance from hermitian self-orthogonal codes," *Des., Codes Cryptogr.*, vol. 84, no. 3, pp. 463–471, Sep. 2017.
[44] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical hermitian self-orthogonal MDS codes to quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4735–4740, Sep. 2010.
[45] L. Jin and C. Xing, "A construction of new quantum MDS codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2921–2925, May 2014.
[46] X. Kai and S. Zhu, "New quantum MDS codes from negacyclic codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1193–1197, Feb. 2013.
[47] X. Kai, S. Zhu, and P. Li, "A construction of new MDS symbol-pair codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5828–5834, Nov. 2015.
[48] M. Khan, T. Shah, and S. I. Batool, "A new approach for image encryption and watermarking based on substitution box over the classes of chain rings," *Multimedia Tools Appl.*, vol. 76, no. 22, pp. 24027–24062, Nov. 2017.
[49] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 2, pp. 900–911, Feb. 1997.
[50] E. Knill and R. Laflamme, "A Theory of Quantum Error-Correcting Codes," *Phys. Rev. Lett.*, vol. 84, p. 2525, 2000.
[51] Y. Komamiya, *Application of Logical Mathematics to Information Theory* (Application Theory Groups to Logical Mathematics). Tokyo, Japan: Science Council, 1954, pp. 437–442.
[52] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, no. 24, pp. 4337–4341, Dec. 1995.
[53] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, p. 198, 1996.
[54] A. Lidar and A. Brun, *Quantum Error Correction*. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[55] Z. Li, L.-J. Xing, and X.-M. Wang, "Quantum generalized Reed–Solomon codes: Unified framework for quantum maximum-distance-separable codes," *Phys. Rev. A, Gen. Phys.*, vol. 77, no. 1, pp. 1–4, Jan. 2008.
[56] X. Liu, H. Liu, and L. Yu, "Entanglement-assisted quantum codes from matrix-product codes," *Quantum Inf. Process.*, vol. 18, no. 6, p. 183, Jun. 2019.
[57] X. Liu, L. Yu, and P. Hu, "New entanglement-assisted quantum codes from k-Galois dual codes," *Finite Fields Appl.*, vol. 55, p. 21–32, May 2019.
[58] S. R. López-Permouth, H. Özadam, F. Özbudak, and S. Szabo, "Polycyclic codes over galois rings with applications to repeated-root constacyclic codes," *Finite Fields Their Appl.*, vol. 19, no. 1, pp. 16–38, Jan. 2013.
[59] 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. 2015.
[60] L. Luo, Z. Ma, and D. Lin, "Two new families of quantum synchronizable codes," *Quantum Inf. Process.*, vol. 18, no. 9, pp. 1–18, Sep. 2019.
[61] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error-Correcting Codes*, 10th ed. Amsterdam, The Netherlands: North-Holland, 1998.
[62] C. Maneri and R. Silverman, "A combinatorial problem with applications to geometry," *J. Combinat. Theory A*, vol. 11, no. 2, pp. 118–121, Sep. 1971.

[63] J. C. F. Matthews, A. Politi, A. Stefanov, and J. L. O'Brien, "Manipulation of multiphoton entanglement in waveguide quantum circuits," *Nature Photon.*, vol. 3, no. 6, pp. 346–350, Jun. 2009.
[64] M. Asif and T. Shah, "BCH codes with computational approach and its applications in image encryption," *J. Intell. Fuzzy Syst.*, vol. 37, no. 3, pp. 3925–3939, Oct. 2019.
[65] A. Nielsen and L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[66] H. Ozadam and F. Ozbudak, "The minimum Hamming distance of cyclic codes of length $2p^s$," *Proc. Int. Symp. Appl. Algebra, Algebraic Algorithms, Error-Correcting Codes*, 2009, pp. 92–100.
[67] V. Pless and W. C. Huffman, *Handbook Coding Theory*, Amsterdam, The Netherlands: Elsevier, 1998.
[68] Y. Polyanskiy, "Asynchronous communication: Exact synchronization, universality, and dispersion," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1256–1270, Mar. 2013.
[69] E. Prange, "Cyclic error-correcting codes in two symbols," Air Force Cambridge Res. Center, Wright-Patterson Air Force Base, OH, USA, Tech. Rep. TN-57-103, Sep. 1957.
[70] R. Prevedel, G. Cronenberg, M. S. Tame, M. Paternostro, P. Walther, M. S. Kim, and A. Zeilinger, "Experimental realization of dicke states of up to six qubits for multiparty quantum networking," *Phys. Rev. Lett.*, vol. 103, no. 2, Jul. 2009, Art. no. 020503.
[71] M. Rädmark, M. Zukowski, and M. Bourennane, "Experimental test of fidelity limits in six-photon interferometry and of rotational invariance properties of the photonic six-qubit entanglement singlet state," *Phys. Rev. Lett.*, vol. 103, no. 15, Oct. 2009, Art. no. 150501.
[72] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1388–1394, Jul. 1998.
[73] S. Roman, *Coding and Information Theory*. New York, NY, USA: Springer-Verlag, 1992.
[74] M. Sarä and E. Kolotoälu, "A different construction for some classes of quantum MDS codes," *Math. Comput. Sci.*, vol. 14, no. 1, pp. 35–44, Mar. 2020.
[75] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 1, Dec. 2001, Art. no. 012308.
[76] D. Schlingemann, "Stabilizer codes can be realized as graph codes," *Quantum Inf. Comput.*, vol. 2, pp. 307–323, Oct. 2002.
[77] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.
[78] T. Shah, T. U. Haq, and G. Farooq, "Serpent algorithm: An improvement by 4×4 S-Box from finite chain ring," in *Proc. Int. Conf. Appl. Eng. Math. (ICAEM)*, Sep. 2018, pp. 1–6.
[79] T. Shah, N. Mehmood, A. A. de Andrade, and R. Palazzo, "Maximal cyclic subgroups of the groups of units of galois rings: A computational approach," *Comput. Appl. Math.*, vol. 36, no. 3, pp. 1273–1297, Sep. 2017.
[80] T. Shah, S. Jahangir, and A. A. de Andrade, "Design of new 4×4 S-box from finite commutative chain rings," *Comput. Appl. Math.*, vol. 36, no. 2, pp. 843–857, Jun. 2017.
[81] X. Shi, Q. Yue, and Y. Chang, "Some quantum MDS codes with large minimum distance from generalized Reed–Solomon codes," *Cryptogr. Commun.*, vol. 10, no. 6, pp. 1165–1182, Nov. 2018.
[82] X. Shi, Q. Yue, and Y. Wu, "New quantum MDS codes with large minimum distance and short length from generalized Reed–Solomon codes," *Discrete Math.*, vol. 342, pp. 1989–2001, Jul. 2019.
[83] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A, Gen. Phys.*, vol. 52, p. 2493, May 1995.
[84] R. Silverman, "A metrization for power-sets with applications to combinatorial analysis," *Canad. J. Math.*, vol. 12, pp. 158–176, Dec. 1960.
[85] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, p. 793, 1996.
[86] L. M. G. M. Tolhuizen, "On maximum distance separable codes over alphabets of arbitrary size," in *Proc. IEEE Int. Symp. Inf. Theory*, Oct. 1994, p. 431.
[87] W. Wieczorek, R. Krischek, N. Kiesel, P. Michelberger, G. Tóth, and H. Weinfurter, "Experimental entanglement of a six-photon symmetric dicke state," *Phys. Rev. Lett.*, vol. 103, no. 2, Jul. 2009, Art. no. 020504.
[88] J. Wang, R. Li, J. Lv, and H. Song, "Entanglement-assisted quantum codes from cyclic codes and negacyclic codes," *Quantum Inf. Process.*, vol. 19, no. 5, p. 138, May 2020.
[89] L. Wang, S. Zhu, and Z. Sun, "Entanglement-assisted quantum MDS codes from cyclic codes," *Quantum Inf. Process.*, vol. 19, no. 2, p. 192, Feb. 2020.
[90] Y. Xie, J. Yuan, and Y. Fujiwara. "Quantum synchronizable codes from augmentation of cyclic codes," *PLoS ONE*, vol. 6, Apr. 2014, Art. no. e14641.
[91] Y. Xie, L. Yang, and J. Yuan, "Q-ary chain-containing quantum synchronizable codes," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 414–417, Mar. 2016.
[92] H. Yan, "A note on the construction of MDS self-dual codes," *Cryptogr. Commun.*, vol. 11, pp. 259–268, May 2019.
[93] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, "Observation of eight-photon entanglement," *Nature Photon.*, vol. 6, no. 4, pp. 225–228, Apr. 2012.
[94] T. Zhang and G. Ge, "Quantum MDS codes with large minimum distance," *Des., Codes Cryptogr.*, vol. 83, no. 3, pp. 503–517, Jun. 2017.
[95] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

HAI Q. DINH received the B.Sc., M.Sc., and Ph.D. degrees in mathematics from Ohio University, USA, in 1998, 2000, and 2003, respectively. He was a Visiting Professor with North Dakota State University, USA, for a period of one year. Since 2004, he has been with Kent State University, USA, as a tenured Professor in mathematics, where he is currently a Professor in applied mathematics with the Department of Mathematical Sciences. Since 2004, he has been published more than 75 articles at high-level SCI (E) research journals, such as *Journal of Algebra*, *Journal of Pure and Applied Algebra*, the IEEE TRANSACTIONS ON INFORMATION THEORY, the IEEE COMMUNICATIONS LETTERS, *Finite Fields and Their Applications*, *Applicable Algebra in Engineering Communication and Computing*, and *Discrete Applied Mathematics*. He has been a well-known invited/keynote speaker at numerous international conferences and mathematics colloquium. He also gave many honorary tutorial lectures at the international universities in China, Indonesia, Kuwait, Mexico, Singapore, Thailand, and Vietnam. His research interests include algebra and coding theory.

BAC T NGUYEN received the B.Sc. degree in mathematics from Thai Nguyen University, Vietnam, in 2008, the M.Sc. degree in mathematics from the Institute of Mathematics, Hanoi, Vietnam, in 2010, and the Ph.D. degree from Mahidol University, Bangkok, Thailand, in 2015. He has published 15 articles in high-ranked peer-review journals, such as the IEEE TRANSACTIONS ON INFORMATION THEORY, the IEEE COMMUNICATIONS LETTERS, *Discrete Applied Mathematics*, and *Finite Fields and Their Applications*. His research interests include algebraic coding theory and algebra.

WORAPHON YAMAKA received the bachelor's, master's, and Ph.D. degrees in economics from Chiang Mai University, Chiang Mai, Thailand, in 2011, 2014, and 2017, respectively. He has been a Lecturer with the Faculty of Economics, Chiang Mai University, since 2018, where he is currently the Vice-Director of the Centre of Excellence in Econometrics. Since 2015, he has been published more than 90 articles which indexed in Scopus. His research interests include economics and econometrics.