Quantum Stabilizer Codes Construction from Hermitian Self-Orthogonal Codes over GF(4)

Duc Manh Nguyen and Sunghwan Kim

Abstract: **In order to construct quantum error correction code, we consider additive codes over Galois field GF(4), which are self-orthogonal with respect to a certain Hermitian product. In this paper, we first propose a new approach to the construction of Hermitian self-orthogonal linear codes, applying the extension to get a longer length, and prove the codes have good minimum distance. Then, we investigate the corresponding quantum stabilizer codes from the classical codes. Six optimal quantum stabilizer codes have been achieved to show the effectiveness of the proposed construction.**

Index Terms: **Galois field, Hermitian product, quantum error correction codes, self-orthogonal code, stabilizer codes.**

I. INTRODUCTION

THE theory of quantum information is a result of the effort to generalize classical information theory. An important milestone in quantum computing occurred in 1994 when Shor published computationally efficient quantum algorithms for factoring integers and evaluating discrete logarithms [1]. With these algorithms, the owner of a quantum computer could crack popular, highly utilized public key cryptosystems. In addition, Grover discovered a quantum algorithm for the important problem of searching an unstructured database, which yields a substantial speed-up over classical search algorithms [2]. Hence, performance of these quantum algorithms promised a great deal. However, the effects of noise and imperfectly applied quantum gates would quash their performance advantages. To deal with the problems, the theory of quantum error correction code was developed to protect quantum states against noise. Discoveries of Shor code for nine-qubit codes [3] and Steane codes for seven-qubits [4] showed how data could be protected by containing more redundancy after encoding by quantum systems; these were the first examples of a quantum error correction code (QECC). The purpose of QECCs is to encode a k-qubit state into an n-qubit state such that all 2^k complex coefficients are perfectly stored and used to correct errors.

Stabilizer codes, first introduced by Gottesman [5], have become an important class of QECC. These codes are useful for building quantum fault-tolerant circuits [6]. Stabilizer codes append ancilla qubits to qubits to be protected, and the most important advantage of stabilizer codes is that errors can be detected and removed by stabilizer operators, rather than from the quantum state itself. In addition, the stabilizer formalism allows us to construct quantum stabilizer code from binary formalism as the classical parity-check matrix over binary in the constraint referred to as the symplectic inner product (SIP) [5]. Therefore, several stabilizer codes have been proposed where constructions are analogous to classical linear codes, such as quantum BCH codes [7], entanglement-assisted quantum code based on LDPC [8], quantum Reed-Solomon codes [9], quantum code based on classical cyclic and modified cyclic [10], and analogous to combinatorial design, such as cyclic difference sets [11], quadratic residue sets [12], and group association scheme [13]. It also turns out that another useful construction can be found by considering classical error correction codes, but instead of using binary vectors, we use vectors over the Galois field (GF) [14]. Since additive codes over GF can be defined as additive subgroups, the additive codes have been popularly used in construction of quantum codes. Hence, the problem of finding QECC is transformed into a problem of finding additive self-orthogonal code under a certain inner product over GF(4). So our proposal is to construct good Hermitian self-orthogonal code in order to construct good QECCs using the idea of Calderbank *et al.* [14].

The key result of this paper is to propose a new approach to the construction of additive codes over GF(4), which are self-orthogonal with respect to Hermitian product. The minimum distance of this classical linear code was proved to be 4 in all cases. The corresponding quantum stabilizer code can be transformed from this classical code; we prove all the optimal codes that can be accomplished from this construction with lengths 5, 6, 7, 8, 9, and 10. The organization of this paper is as follows. In Section II, we review the theory of quantum mechanics, the role of quantum stabilizer codes on quantum error correction as well as how general stabilizer codes are related to Hermitian additive code over GF(4). Then, the proposed construction of Hermitian additive linear code is explained; and in Section III, we investigate the quantum stabilizer codes that can be transformed. Finally, the conclusions are presented in Section IV.

II. QUANTUM STABILIZER CODES

In this section, we give some preliminary explanations about quantum mechanics, quantum error correction codes, and quantum stabilizer code interpretation from Hermitian self-orthogonal code through the paper.

A. Quantum Mechanics

The bit is the fundamental concept of classical computation and classical information. The fundamental unit of quantum in-

Manuscript received February 16, 2017; approved for publication by Yun Hee Kim, Division I Editor, April 08, 2018.

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF-2016R1D1A1B03934653).

The authors are with the Department of Electrical Engineering, University of Ulsan, Korea. email: nguyenmanhduc18@gmail.com, sungkim@ulsan.ac.kr.

S. Kim is the corresponding author.

Digital Object Identifier: 10.1109/JCN.2018.000043

formation is the quantum bit (qubit for short). Then, just as the classical bit has a state of either 0 or 1, the state in the quantum system is instead a two-state physical system (0 and 1) on which the superposition principle applies. It is better to translate all the physical features of quantum codes into a mathematical setting. For this purpose, we consider the qubit as an element of a two-dimensional complex Hilbert space, *H*. The base state is denoted as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

and the general state is a linear combination of the two base states:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. This concept is known as the superposition of base states $|0\rangle$, $|1\rangle$, the main property of quantum computation since it allows gate operations to deal with several values in one step. Hence, the amount of information that can be represented in quantum mechanism is infinite. In general, the quantum memory is a physical system composed of *n* qubits that can be considered as an element of the *n* times tensor-product of *H* as

$$|\psi\rangle = \sum_{i_k=\{0,1\}} \alpha_{i_1 i_2 \cdots i_n}\,|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle = \sum_i \alpha_i\,|i\rangle,$$

where $i = \sum_{k=1}^{n} 2^{n-k} i_k$. There are three major features that distinguish quantum information and classical information [19]:

1. Measurement destroys information.
2. The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state.
3. Qubits errors are a continuum.

To address the third feature, we consider the errors as operators in Hilbert space.

A particularly fruitful way to understand a quantum system is to look at the behavior of various operators acting on the states of the system. Quantum information processing requires unitary transformations operating on states. Hence, Pauli operators are one unitary transformation that can be used [5], [6]. In fact, a single error over a qubit can be viewed like an operator, $\mathbf{A}$:$H \rightarrow H$, i.e., a 2×2-complex matrix. Since a quantum system has the base configuration in n-qubits, we can view an error like the tensor product of n operators, each of them acting on a single qubit. Each single operator is the linear combination of the Pauli matrices:

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$\mathbf{Y} = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}, \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

where $j^2 = -1$. The Pauli operation acts on a qubit as follows:

$$\mathbf{I}|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle,$$

$$\mathbf{X}|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle,$$

$$\mathbf{Y}|\psi\rangle = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = j\begin{bmatrix} -\beta \\ \alpha \end{bmatrix} = j(-\beta|0\rangle + \alpha|1\rangle),$$

$$\mathbf{Z}|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle.$$

Pauli operators **X**, **Z**, and **Y** are regarded as a bit flip, a phase flip, and a combination of bit and phase flips, respectively. Multiplication of two Pauli operators satisfies the following equations:

$$\mathbf{X}^2 = \mathbf{Y}^2 = \mathbf{Z}^2 = \mathbf{I},$$

$$\mathbf{X} \times \mathbf{Y} = j\mathbf{Z}, \mathbf{Y} \times \mathbf{X} = -j\mathbf{Z} \rightarrow \mathbf{X} \times \mathbf{Y} = -\mathbf{Y} \times \mathbf{X},$$

$$\mathbf{Y} \times \mathbf{Z} = j\mathbf{X}, \mathbf{Z} \times \mathbf{Y} = -j\mathbf{X} \rightarrow \mathbf{Y} \times \mathbf{Z} = -\mathbf{Z} \times \mathbf{Y},$$

$$\mathbf{Z} \times \mathbf{X} = j\mathbf{Y}, \mathbf{X} \times \mathbf{Z} = -j\mathbf{Y} \rightarrow \mathbf{Z} \times \mathbf{X} = -\mathbf{X} \times \mathbf{Z}.$$

The single Pauli group, P_1, is a group formed by the Pauli operators, that is closed under multiplication. Therefore, the Pauli group consists of all the Pauli matrices, together with the multiplicative factors $\pm 1, \pm j$. We have: $P_1 = \pm\{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}, j\mathbf{X}, j\mathbf{Y}, j\mathbf{Z}\}$. The n-fold tensor product of single Pauli operators forms an n-qubit Pauli group, P_n. The main property of P_n is that any two elements, $\mathbf{A}, \mathbf{B} \in P_n$, either commute or anticommute. For n-qubit Pauli operators $\mathbf{A}, \mathbf{B} \in P_n$, the operator $(\circ)$ for commutativity is defined as

$$\mathbf{A} \circ \mathbf{B} = \prod_{i=1}^{n} \mathbf{A}_i \bullet \mathbf{B}_i,$$

$$\text{where } \mathbf{A}_i \bullet \mathbf{B}_i = \begin{cases} +1, & \text{if } \mathbf{A}_i \times \mathbf{B}_i = \mathbf{B}_i \times \mathbf{A}_i; \\ -1, & \text{if } \mathbf{A}_i \times \mathbf{B}_i = -\mathbf{B}_i \times \mathbf{A}_i \end{cases}.$$

Two operators, **A** and **B**, are commutative if and only if $\mathbf{A} \circ \mathbf{B} = +1$; otherwise, they are anti-commutative. Commutativity is an important feature of the Pauli group, since this can be used to detect errors within the stabilizer formalism in the next section.

B. Quantum Stabilizer Codes

The stabilizer formalism used Heisenberg representation for quantum mechanics. And quantum states can be described in terms of operators rather than the states. That is, let $H^{\otimes n} = |\psi\rangle$ be the quantum state space of n qubits. A stabilizer group, S, closed under multiplication is an Abelian subgroup of P_n such that a non-trivial subspace, C_S of $H^{\otimes n}$, is fixed (or stabilized) by S. The stabilized C_S defines a quantum code space such that

$$C_S = \{|\psi\rangle \in H^{\otimes n} | \boldsymbol{g}|\psi\rangle = |\psi\rangle, \forall \boldsymbol{g} \in S\}.$$

If S is generated by $g = \{\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_m\}$, where g is $m = n-k$ independent stabilizer operators, the code space C_S encodes k logical qubits into n physical qubits and it can correct $\lfloor \frac{d_{\min}-1}{2} \rfloor$ errors. This code C_S, is called $[[n, k, d_{\min}]]$ quantum stabilizer code. Note that quantum stabilizer code C_S has the following features:

1. $-\mathbf{I} \notin S$.
2. For any two stabilizers $\mathbf{E}, \mathbf{F} \in S$, $\mathbf{E} \circ \mathbf{F} = +1$.

Then, it is enough to check the commutative property of generators of $C_S : g = \{\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_m\}$, where two elements have to be commutative to each other. Considering a set of error operators, $\{\mathbf{E}\} \in P_n$, the collection of Pauli operators takes a state,

$|\psi\rangle$, to the corrupted state, $\mathbf{E}|\psi\rangle$. A given operator, $\mathbf{E}$, either commutes or anticommutes with each stabilizer, $\mathbf{S}_i$. Then, the corrupted state $\mathbf{E}|\psi\rangle$ is diagnosed by elements $\mathbf{S}_i$ of set S. The outcome of the diagnostic procedure is a vector of $\{+1, -1\}$ indicating whether or not $\mathbf{E}$ can be detected. The indication for the error detection is expressed as

$$\mathbf{S}_i \times \mathbf{E}|\psi\rangle = \begin{cases} \mathbf{E} \times \mathbf{S}_i|\psi\rangle = \mathbf{E}|\psi\rangle, & \text{error undetected;} \\ -\mathbf{E} \times \mathbf{S}_i|\psi\rangle = -\mathbf{E}|\psi\rangle, & \text{error detected} \end{cases}.$$

The condition for quantum error correction is that E is a set of correctable error operators for C_S if

$$\mathbf{E}_i^\dagger \mathbf{E}_j \notin N(S) \setminus S, \forall \mathbf{E}_i, \mathbf{E}_j \in E,$$

where $\mathbf{E}_i^\dagger$ is the conjugate transpose of $\mathbf{E}_i$, and $N(S)$ is the normalizer of S in P_n, such as

$$N(S) = \{\mathbf{A} \in P_n | \mathbf{A}^\dagger \mathbf{E} \mathbf{A} \in S, \forall \mathbf{E} \in S\}.$$

Note that $N(S)$ is the collection of all operators in P_n that commute with S, and $S \subset P_n$. Then, the minimum distance, $d_{\min}$, of stabilizer code is determined by

$$d_{\min} = \min\{W(\mathbf{E})\}, \text{ s.t., } \mathbf{E} \in N(S) \setminus S,$$

where the weight of an operator, W(*), is the number of positions not equal to Pauli operator **I**.

Quantum stabilizer code can be expressed in the binary field, since any given Pauli operator on n qubit can be composed into an **X**-containing operator and a **Z**-containing operator, as well as a phase factor, $\{+1, -1, +j, -j\}$. For example: **XYYZI** = − **XXXII**×**IZZZI**. This is achieved by mapping **I, X, Y,** and **Z** as follows: **I**→(0, 0), **X**→(1, 0), **Z**→(0, 1), and **Y**→(1, 1). Then, the $n - k$ generators of an $[[n, k]]$ stabilizer code can be expressed as a concatenation of a pair of $(n-k) \times n$ binary matrices $\mathbf{H_X}, \mathbf{H_Z}$. Then, the parity-check matrix $\mathbf{H}$ of the quantum stabilizer code is defined as $\mathbf{H} = [\mathbf{H_X}|\mathbf{H_Z}]$. The commutative property of the stabilizers can be transformed into the orthogonality of rows in the matrix forms with respect to the symplectic product. If the mth row r_m is expressed as $r_m = [x_m|z_m]$, where z_m and x_m are binary strings for **Z** and **X**, respectively, the symplectic product of the m_1th row and m_2th row in the parity-check matrix is expressed as

$$\begin{aligned} \mathbf{r}_{m_1} \odot \mathbf{r}_{m_2} &= [\mathbf{x}_{m_1}|\mathbf{z}_{m_1}] \odot [\mathbf{x}_{m_2}|\mathbf{z}_{m_2}] \\ &= \mathbf{x}_{m_1} * \mathbf{z}_{m_2} + \mathbf{x}_{m_2} * \mathbf{z}_{m_1} \text{ modulo } 2, \end{aligned}$$

where

$$\mathbf{x}_k * \mathbf{z}_l = \sum_{i=1}^{n} \mathbf{x}_{ki} \times \mathbf{z}_{li}.$$

The symplectic product between two rows is zero if the total number of positions with different values in **X** and **Z** is even. This condition is also required to satisfy the commutativity property. In other words, for a binary matrix $\mathbf{H} = [\mathbf{H_X}|\mathbf{H_Z}]$, size $(n-k) \times 2n$, the symplectic product is satisfied for all rows if and only if

$$\mathbf{H_X} \times \mathbf{H_Z}^T + \mathbf{H_Z} \times \mathbf{H_X}^T = \mathbf{0}_{n-k} \text{ modulo } 2$$

Table 1. Mapping between GF(4) and Pauli operators.

Pauli operator	GF(4)	Binary form
I	0	(0,0)
X	1	(1,0)
Y	ω^2	(1,1)
Z	ω	(0,1)

where 0_a is the $a \times a$ zero matrix. From the binary form of a stabilizer code, by using Gaussian elimination, the parity-check matrix $\mathbf{H}$ can be uniquely determined in standard form as follows,

$$\begin{bmatrix} \overbrace{\mathbf{I}}^{r} & \overbrace{\mathbf{A}_1}^{n-k-r} & \overbrace{\mathbf{A}_2}^{k} & \overbrace{\mathbf{B}}^{r} & \overbrace{\mathbf{C}_1}^{n-k-r} & \overbrace{\mathbf{C}_2}^{k} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{D} & \mathbf{I} & \mathbf{E} \end{bmatrix} \begin{matrix} \} \\ \} \end{matrix} \begin{matrix} r \\ n-k-r \end{matrix}$$

C. From Hermitian Self Orthogonal Codes over GF(4) to Quantum Stabilizer Codes

Proposition 1: We can consider a quantum stabilizer code as an additive code over the finite field GF(4) by identifying the four Pauli operators with the elements of GF(4). We denote $\mathrm{GF}(4) = \{0, 1, \omega, \omega^2\}$ where $\omega^2 = \omega + 1$. The mapping is in Table 1.

Given four elements in GF(4), some products have been defined as follows:

Definition 1: Conjugation in GF(4) is defined by $\overline{x} := x^2$. The trace function, *tr* : $\mathrm{GF}(4) \to \mathrm{GF}(2)$, is defined by $tr(x) := x + \overline{x}$. The trace inner product of two vector lengths, *n*, over GF(4), **u** and **v**, is given by $\mathbf{u} * \mathbf{v} := \sum_i tr(u_i \overline{v_i})$. The Hermitian product $(.)$ of two vector lengths, *n*, over GF(4), **u** and **v**, is defined as $\mathbf{u}.\mathbf{v} := \sum_i u_i \overline{v_i}$.

In particular, we have: $tr(0) = tr(1) = 0$, $tr(\omega) = tr(\omega^2) = 1$ and $\overline{0} = 0$, $\overline{1} = 1$, $\overline{\omega} = \omega^2$. Hence, as in the mapping in Table 1, adding two vectors over GF(4) corresponds to multiplying two mapping Pauli operators. For single Pauli operators, they commute when, in the first case, one of them is **I**, or in the second case, when they are equal to each other. Hence, their trace product is always 0, due to $tr(0) = 0$ and when $x \neq 0, x^3 = 1$, then, $tr(x^3) = tr(1) = 0$. Otherwise, the trace product of single Pauli operators is 0. From that, Pauli operators arising from vector **x**, **y** commute when the trace product (components-wise) is even; or stated another way, $\mathbf{x} * \mathbf{y} = \sum tr(x_i \overline{y_i}) = 0$. To state the relationship between QECC and additive code over GF(4), the two following lemmas have been studied [14]:

Lemma 1: An additive code $(n, 2^{n-k})$ code *C* such that there are no vectors of weight $< d$ in $C^\perp \backslash C$, where $C^\perp$ is the Hermitian dual of *C*, that yields a quantum code with parameters $[[n, k, d]]$.

Lemma 2: Linear code *C* is self-orthogonal with respect to trace if and only if it is self-orthogonal with respect to Hermitian product.

Proof: We notice *C* is linear, which means if $\mathbf{u}, \mathbf{v} \in C$, we have $\omega\mathbf{u}, \omega\mathbf{v} \in C$. From $\mathbf{u}.\overline{\mathbf{v}} = \alpha + \omega\beta$, we have: $0 = tr(\mathbf{u}.\overline{\mathbf{v}}) = tr(\alpha + \beta\omega) = \beta$. From $\omega^2\mathbf{u}.\overline{\mathbf{v}} = \omega^2\alpha + \omega^3\beta = \omega^2\alpha + \beta$, we have $0 = tr(\omega^2\mathbf{u}.\overline{\mathbf{v}}) = tr(\omega^2\alpha + \beta) = \alpha$. Since the linear code *C* is

an additive code, its parameters are $(n, 2^{2k}) = (n, 2^{n-(n-2k)})$. Therefore, as Lemma 1, the stabilizer code $[[n, n-2k, d]]$ is obtained. □

Combining Lemma 1 and Lemma 2, we have the following corollary:

Corollary 1: Let C be a Hermitian self-orthogonal linear $[n, k]$ code over GF(4) such that there are no vectors of weight $< d$ in $C^{\perp} \backslash C$, where $C^{\perp}$ is the Hermitian dual of C. Then, there is a quantum stabilizer code $[[n, n-2k, d]]$.

From Corollary 1, we will change the problem of building the stabilizer code into finding a Hermitian self-orthogonal linear code. First, it is an additive code over GF(4); then, it actually requires the two following conditions for each row vector, (for example, $\mathbf{u}_1$, $\mathbf{u}_2$):

1. To be orthogonal to each other; that is, $\mathbf{u}_i.\overline{\mathbf{u}_j} = 0$ for any $i, j \in \{1, 2\}$; and
2. To be orthogonal to itself; that is, the weight of $\mathbf{u}_1$, $\mathbf{u}_2$ (the number of elements with difference 0) has to be even.

III. CONSTRUCTION METHOD

In this section, the construction is first proposed and proven to satisfy the conditions of Hermitian self-orthogonal codes. We prove the codes have a good minimum distance. Then, six optimal quantum stabilizer codes are showed as transformation from the Hermitian self-orthogonal codes. In addition, the explanations for general length are mentioned.

A. Extension for Generator Matrix

Theorem 1: Let $\mathbf{G}$ be the generator matrix over GF(4) in following form: $\mathbf{G} = [\mathbf{I}|\mathbf{G}^0]$, where

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}, \mathbf{G}^0 = \begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_m \end{bmatrix}, \tag{1}$$

and all the elements of matrix $\mathbf{I}$ are in GF(4), and $\mathbf{g}_i (i = 1, 2, \cdots, m)$ are the vectors with finite length over GF(4) that satisfy two conditions:

1. The number of nonzero elements in $\mathbf{g}_i$ is odd, and
2. The Hermitian product of any pair $(\mathbf{g}_i, \mathbf{g}_j)$ (where $i, j = 1, 2, \cdots, m$) is zero.

Then, $\mathbf{G}$ is the generator matrix of a Hermitian self-orthogonal code over GF(4).

Proof: From Condition 1, each vector $\mathbf{g}_i (i = 1, 2, \cdots, m)$ has odd weight, and then, each row in $\mathbf{G}$ has even weight. Hence, the Hermitian product of each row in $\mathbf{G}$ with itself is zero (the summation of even numbers of 1 is 0). In addition, the Hermitian product of each of the two rows in $\mathbf{G}$ is 0 due to Condition 2; the Hermitian product of each pair $(\mathbf{g}_i, \mathbf{g}_j)$(where $i, j = 1, 2, \cdots, m$) is zero. □

We call $\mathbf{G}^0$ the matrix created from $\mathbf{g}_i (i = 1, 2, \cdots, m)$, or the right-part of generator matrix $\mathbf{G}$. Then, we have the extension from $\mathbf{G}^0$ as the following theorem to get larger matrices, $\mathbf{G}^1$, $\mathbf{G}^2$, that protect the two conditions in Theorem 1. $\mathbf{G}^1$, $\mathbf{G}^2$ can also be the right part of $\mathbf{G}$.

Theorem 2: From generator matrix $\mathbf{G}^0$ with length l and dimension m, Let's extend new matrices $\mathbf{G}^1$ and $\mathbf{G}^2$ with length $l+2$, and the dimension to $m+1$ or $m+2$, as in the following form:

$$\mathbf{G}^1 = \begin{bmatrix} \mathbf{A}^1 & \mathbf{X}^1 \\ \mathbf{Y} & \mathbf{G}^0 \end{bmatrix}, \mathbf{G}^2 = \begin{bmatrix} \mathbf{A}^2 & \mathbf{X}^2 \\ \mathbf{Y} & \mathbf{G}^0 \end{bmatrix}, \tag{2}$$

where $\mathbf{A}^1 = [0\ \ 1]$, $\mathbf{A}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{X}^1 = [x_1\ \ x_2\ \ \cdots\ \ x_n]$ is an even weight vector with the elements over GF(4), $\mathbf{X}^2 = \begin{bmatrix} \mathbf{X}^1 \\ \mathbf{X}^1 \end{bmatrix}$, $\mathbf{Y} = \begin{bmatrix} y_1 & y_1 \\ y_2 & y_2 \\ \cdots & \\ y_m & y_m \end{bmatrix}$ with elements $\overline{y_i} := \mathbf{X}^1.\mathbf{g}_i$ (where $\overline{y_i}$ denotes the conjugate of y_i and $(.)$ denotes the Hermitian product; $\mathbf{g}_i$ is ith row of $\mathbf{G}^0$. Then, $\mathbf{G}^1$ and $\mathbf{G}^2$ satisfy the two conditions in Theorem 1 and can be used as the right part in generator matrix $\mathbf{G}$ of a Hermitian self-orthogonal code over GF(4).

Proof: The weight of $[x_1\ \ x_2\ \ \cdots\ \ x_n]$ is even, and the weight of each $\mathbf{g}_i (i = 1, 2, \ldots, m)$ is odd, so it is clear that the weight of each row in $\mathbf{G}^1$ and $\mathbf{G}^2$ is odd. So, the first condition in Theorem 1 is satisfied. In addition, the extension elements help us to save the Hermitian product since it comes from the definition of y_i:

$$\overline{y_i} := [x_1\ \ x_2\ \ \cdots\ \ x_n].\mathbf{g}_i$$

$$\Rightarrow 1\overline{y_i} + [x_1\ \ x_2\ \ \cdots\ \ x_n].\mathbf{g}_i = 1\overline{y_i} + 1\overline{y_i} = 0.$$

So, the second condition in Theorem 1 is satisfied.

Since $\mathbf{G}^1$ and $\mathbf{G}^2$ satisfy the two conditions in Theorem 1 and can be used as the right part in generator matrix $\mathbf{G}$ of a Hermitian self-orthogonal code over GF(4), Theorem 2 is proven. □

B. Optimal Quantum Stabilizer Code Results

In this part, the results from our proposal have showed. We divide the results into two cases. We first consider the odd lengths with 5, 7, and 9 qubits. Then, we consider the qubits with even lengths 6, 8, and 10. The relations between the outcomes are explained in each example.

Example 1: In the case of five qubits, the optimal code we expected is QECC $[[5, 1, 3]]$ code. With the form in (1), it reduces to find that $\mathbf{G}^0$ with two vectors has size 3. Because elements of $\mathbf{G}^0$ are from $\mathrm{GF}(4) = \{0, 1, \omega, \omega^2\}$, it is trivial to check out the conditions, and we get three candidates for $\mathbf{G}^0$ as follows:

$${\mathbf{G}^0}_1 = \begin{bmatrix} 1 & \omega & \omega^2 \\ \omega^2 & \omega & 1 \end{bmatrix} \tag{3}$$

$${\mathbf{G}^0}_2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \end{bmatrix} \tag{4}$$

$${\mathbf{G}^0}_3 = \begin{bmatrix} 1 & \omega & \omega \\ \omega & \omega & 1 \end{bmatrix}. \tag{5}$$

As mapping between elements in Table 1, we can get the standard form (the theorem about binary form with standard form can be found at [5]) of generators for each stabilizer code as follows

Case 1: From ${\mathbf{G}^0}_1$ in (3), we have Hermitian self-orthogonal

code $[5,2,4]$ with the generators $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \omega & \omega^2 \end{bmatrix}$, and it corresponds to stabilizer code in binary standard form:

$$\begin{cases} \mathbf{g}_1 = [1000011110] \\ \mathbf{g}_2 = [0100011011] \\ \mathbf{g}_3 = [0010111101] \\ \mathbf{g}_4 = [0001110110] \end{cases}.$$

From standard form, the logical operators and minimum distance are calculated exactly and we have QECC $[[5,1,3]]$ code.

Case 2: From ${\mathbf{G}^0}_1$ in (4), we have Hermitian self-orthogonal code $[5,2,4]$ with the generators $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & \omega & \omega^2 \end{bmatrix}$, and it corresponds to stabilizer code in binary standard form:

$$\begin{cases} \mathbf{g}_1 = [1001100101] \\ \mathbf{g}_2 = [0101011001] \\ \mathbf{g}_3 = [0010110110] \\ \mathbf{g}_4 = [0000001111] \end{cases}.$$

This code was already reported in a database [17].

Case 3: From ${\mathbf{G}^0}_1$ in (5), we have Hermitian self-orthogonal code $[5,2,4]$ with the generators $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & \omega & \omega \\ 0 & 1 & \omega & \omega & 1 \end{bmatrix}$, and it corresponds to stabilizer code in binary standard form:

$$\begin{cases} \mathbf{g}_1 = [1000111011] \\ \mathbf{g}_2 = [0100100110] \\ \mathbf{g}_3 = [0010111000] \\ \mathbf{g}_4 = [0001110111] \end{cases}.$$

This code was already reported [5] as binary cyclic construction.

Example 2: With quantum stabilizer code length 7, the existing good code is $[[7,1,3]]$ QECC, which was reported as Steane code with CSS construction [4]. Here, the construction is based on Theorem 1 from following $\mathbf{G}^0$, and it is easy to verify that $\mathbf{G}^0$ satisfies the two conditions of Theorem 1 due to its trivial length:

$$\mathbf{G}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Applying Theorem 2, we get extension $\mathbf{G}^1$ from $\mathbf{G}^0$:

$$\mathbf{G}^1 = \begin{bmatrix} 1 & 0 & \omega^2 & \omega^2 \\ \omega & \omega & 1 & 0 \\ \omega & \omega & 0 & 1 \end{bmatrix}.$$

Then, the generator matrix for Hermitian self-orthogonal code is:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & \omega^2 & \omega^2 \\ 0 & 1 & 0 & \omega & \omega & 1 & 0 \\ 0 & 0 & 1 & \omega & \omega & 0 & 1 \end{bmatrix}. \tag{6}$$

The generators in (6) correspond to additive quaternary code $[7,3,4]$. We transform them to quantum stabilizer code $[[7,1,3]]$ with binary standard form:

$$\begin{cases} \mathbf{g}_1 = [10001001010110] \\ \mathbf{g}_2 = [01000011000100] \\ \mathbf{g}_3 = [00100010001100] \\ \mathbf{g}_4 = [00011000011101] \\ \mathbf{g}_5 = [00000111001000] \\ \mathbf{g}_6 = [00000000110011] \end{cases}.$$

Example 3: With quantum stabilizer code length 9, the existing good code is Shor code [3]. Here, we construct the new $[[9,1,3]]$ quantum code starting from the following $\mathbf{G}^0$ that satisfies the two conditions of Theorem 1

$$\mathbf{G}^0 = \begin{bmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{bmatrix}.$$

Applying Theorem 2, we get the extension from $\mathbf{G}^0$:

$$\mathbf{G}^1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & \omega & \omega \\ \omega^2 & \omega^2 & \omega & 1 & \omega \\ \omega^2 & \omega^2 & \omega & \omega & 1 \end{bmatrix}.$$

Then, the generator matrix for Hermitian self-orthogonal code is:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & \omega & \omega \\ 0 & 0 & 1 & 0 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 0 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega & \omega & 1 \end{bmatrix}. \tag{7}$$

Generators $\mathbf{G}$ in (7) correspond to additive linear code $[9,4,4]$, and it transforms to quantum stabilizer code $[[9,1,3]]$ in binary standard form:

$$\begin{cases} \mathbf{g}_1 = [100001101000100111] \\ \mathbf{g}_2 = [010000100000000011] \\ \mathbf{g}_3 = [001000100000111010] \\ \mathbf{g}_4 = [000100100001011001] \\ \mathbf{g}_5 = [000011101001000111] \\ \mathbf{g}_6 = [000000011001100000] \\ \mathbf{g}_7 = [000000000100010011] \\ \mathbf{g}_8 = [000000000011100111] \end{cases}.$$

In the following examples, we consider the codes when encoding lengths are $k = 0$. It is a special case of quantum code when stabilizer codes are $[[n,0,d]]$; it means quantum code has a one-dimensional code subspace, and there is only one encoded state. It is useful for studies of the correlations in decoherence, and code state is maximally entangled [18].

Example 4: We consider $\mathbf{G}^0$ with the size 3×3; it is a trivial case, and we get candidates as follows:

$${\mathbf{G}^0}_1 = \begin{bmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{bmatrix} \tag{8}$$

$${\mathbf{G}^0}_2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \tag{9}$$

The corresponding quantum stabilizer code $[[6,0,4]]$ over GF(4) from Hermitian self-orthogonal code has the following form:

Case 1: From ${\mathbf{G}^0}_1$ in (8), we have $[6,3,4]$ Hermitian self-orthogonal code with generator $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{bmatrix}$,

which corresponds to stabilizer code in binary standard form:

$$\begin{cases} \mathbf{g}_1 = [100001010100] \\ \mathbf{g}_2 = [010001011101] \\ \mathbf{g}_3 = [001001000110] \\ \mathbf{g}_4 = [000101010111] \\ \mathbf{g}_5 = [000011011000] \\ \mathbf{g}_6 = [000000111111] \end{cases}.$$

Case 2: From $\mathbf{G}^0{}_2$ in (9), we have $[6, 3, 4]$ Hermitian self-orthogonal code with generator $\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & \omega^2 & \omega \end{bmatrix}$, which corresponds to stabilizer code in binary standard form:

$$\begin{cases} \mathbf{g}_1 = [100100001101] \\ \mathbf{g}_2 = [010101000011] \\ \mathbf{g}_3 = [001101001110] \\ \mathbf{g}_4 = [000011001101] \\ \mathbf{g}_5 = [000000100111] \\ \mathbf{g}_6 = [000000011011] \end{cases}.$$

Example 5: With construction base on Theorem 1 from $\mathbf{G}^0$, QECCs with length eight satisfy the two conditions of Theorem 1 due to the simple form of $\mathbf{G}^0$:

$$\mathbf{G}^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Applying Theorem 2, we get extension $\mathbf{G}^2$ from $\mathbf{G}^0$:

$$\mathbf{G}^2 = \begin{bmatrix} 1 & 0 & \omega^2 & \omega^2 \\ 0 & 1 & \omega^2 & \omega^2 \\ \omega & \omega & 1 & 0 \\ \omega & \omega & 0 & 1 \end{bmatrix}.$$

Then, the generator matrix for Hermitian self-orthogonal code is:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & \omega^2 & \omega^2 \\ 0 & 1 & 0 & 0 & 0 & 1 & \omega^2 & \omega^2 \\ 0 & 0 & 1 & 0 & \omega & \omega & 1 & 0 \\ 0 & 0 & 0 & 1 & \omega & \omega & 0 & 1 \end{bmatrix}. \quad (10)$$

We have corresponding quantum stabilizer code $[[8, 0, 4]]$, interpreted from Hermitian self-orthogonal code $[8, 0, 4]$ with the generators in [12].

Example 6: We construct the new $[[10, 0, 4]]$ quantum code starting from $\mathbf{G}^0$. It is easy to verify the two conditions of Theorem 1 due to the simple form of $\mathbf{G}^0$:

$$\mathbf{G}^0 = \begin{bmatrix} 1 & \omega & \omega \\ \omega & 1 & \omega \\ \omega & \omega & 1 \end{bmatrix}.$$

Applying Theorem 2, we get extension $\mathbf{G}^2$ from $\mathbf{G}^0$ in the following form:

$$\mathbf{G}^2 = \begin{bmatrix} 0 & 1 & 0 & \omega^2 & \omega^2 \\ 1 & 0 & 0 & \omega^2 & \omega^2 \\ 0 & 0 & 1 & \omega & \omega \\ 1 & 1 & \omega & 1 & \omega \\ 1 & 1 & \omega & \omega & 1 \end{bmatrix}.$$

Then, the generator matrix for Hermitian self-orthogonal code is:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & \omega^2 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & \omega^2 & \omega^2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & \omega & \omega \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & \omega & 1 & \omega \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & \omega & \omega & 1 \end{bmatrix}. \quad (11)$$

We have corresponding QECC $[[10, 0, 4]]$ that interprets Hermitian self-orthogonal code $[10, 5, 4]$ with the generators in (11).

C. Extension to Get a Longer Length

We have already studied the proposed construction, and the optimal results of quantum stabilizer codes with odd lengths are $[[5, 1, 3]]$, $[[7, 1, 3]]$, $[[9, 1, 3]]$ and in the case of even lengths, we consider the optimal codes to be $[[6, 0, 4]]$, $[[8, 0, 4]]$, $[[10, 0, 4]]$. To analyze longer lengths, we considered the two following lemmas for $n = 2m$ and $n = 2m - 1$.

Lemma 3: Let $\mathbf{G}$ be the generator matrix of $[2(m-2), m-2, 4]$ Hermitian self-orthogonal code, where $\mathbf{G} = [\mathbf{I}|\mathbf{G}^0]$. Then, the generator matrix $\mathbf{G}$ of the Hermitian self-orthogonal $[2m, m, 4]$ code $(m > 5)$ will be $\mathbf{G} = [\mathbf{I}|\mathbf{G}^2]$ where $\mathbf{G}^2$ is achieved by extending it from $\mathbf{G}^0$ by Theorem 2. It is interpreted to be $[[2m, 0, 4]]$ QECC.

Proof: From Theorem 2, the construction of the generator matrix is $\mathbf{G}^2 = \begin{bmatrix} \mathbf{A}^2 & \mathbf{X}^2 \\ \mathbf{Y} & \mathbf{G}^0 \end{bmatrix}$, and we have the following comments.

1. The distance between the two first rows of $\mathbf{G}$ is 4. They are calculated directly.
2. The linear code comes from the last $(m-2)$ rows of $\mathbf{G}$ where the distance at least equals the distance of $[\mathbf{I}|\mathbf{G}^0]$, which is already known to have the distance 4.
3. We consider one row in the two first rows of $\mathbf{G}$ and one from the last $n-2$. In the first half, the distance is 2. In the second half, the first two elements have minimum distance at least 1, and the remaining have a minimum distance of at least 1 (because their weights are even and odd). Then, we have a minimum distance for two rows of at least 4.

From three comments above, minimum distance for linear code is 4. Then, the new code with proposed construction with $\mathbf{G}^2$ be the right part is $[2m, m, 4]$. □

Example 7: We construct the new [[12,0]] quantum code starting from $\mathbf{G}^0$ with the right part of the generator matrix in (10):

$$\mathbf{G}^0 = \begin{bmatrix} 1 & 0 & \omega^2 & \omega^2 \\ 0 & 1 & \omega^2 & \omega^2 \\ \omega & \omega & 1 & 0 \\ \omega & \omega & 0 & 1 \end{bmatrix}.$$

Then, from $\mathbf{G}^0$, for even length, we extend $\mathbf{G}^0$ to $\mathbf{G}^2$ under Theorem 2, with $x = [1 \ \omega \ 1 \ \omega]$. The generator matrix is as fol-

lows:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \omega & 1 & \omega \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \omega & 1 & \omega \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & \omega^2 \\ 0 & 0 & 0 & 1 & 0 & 0 & \omega & \omega & 0 & 1 & \omega^2 & \omega^2 \\ 0 & 0 & 0 & 0 & 1 & 0 & \omega & \omega & \omega & \omega & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \omega & \omega & 0 & 1 \end{bmatrix}. \quad (12)$$

Generators in (12) correspond to $[12, 6, 4]$ Hermitian linear code. Then, $[[12, 0, 4]]$ quantum stabilizer code is transformed. When we consider the extension by $\mathbf{G}^1 = \begin{bmatrix} \mathbf{A}^1 & \mathbf{X}^1 \\ \mathbf{Y} & \mathbf{G}^0 \end{bmatrix}$, we get the following lemma:

Lemma 4: Let $\mathbf{G}$ be the generator matrix of $[2(m-2), m-2, 4]$ Hermitian self-orthogonal code, where $\mathbf{G} = [\mathbf{I}|\mathbf{G}^0]$. Then, generator matrix $\mathbf{G}$ of Hermitian self-orthogonal $[2m-1, m-1, 4]$ code $(m > 5)$ will be $\mathbf{G} = [\mathbf{I}|\mathbf{G}^1]$ where $\mathbf{G}^1$ is achieved by extending it from $\mathbf{G}^0$ with Theorem 2. It can be interpreted to be $[[2m-1, 1, 3]]$ QECC.

Example 8: We construct the new $[[11, 1]]$ QECC starting from $\mathbf{G}^0$ with the right part of $\mathbf{G}$ in (10):

$$\mathbf{G}^0 = \begin{bmatrix} 1 & 0 & \omega^2 & \omega^2 \\ 0 & 1 & \omega^2 & \omega^2 \\ \omega & \omega & 1 & 0 \\ \omega & \omega & 0 & 1 \end{bmatrix}.$$

Then, from $\mathbf{G}^0$, an even length, we extend $\mathbf{G}^0$ to $\mathbf{G}^1$ with Theorem 2, for example with $x = [1\ \ \omega\ \ 1\ \ \omega]$. We have the following generator matrix:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \omega & 1 & \omega \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & \omega^2 \\ 0 & 0 & 1 & 0 & 0 & \omega & \omega & 0 & 1 & \omega^2 & \omega^2 \\ 0 & 0 & 0 & 1 & 0 & \omega & \omega & \omega & \omega & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \omega & \omega & 0 & 1 \end{bmatrix}. \quad (13)$$

The generator in (13) corresponds to $[11, 5, 4]$ Hermitian linear code and $[[11, 1, 3]]$ quantum stabilizer code.

IV. CONCLUSION

In this paper, a new approach to constructing additive codes over GF(4), which are self-orthogonal with respect to Hermitian product, is proposed for even lengths and odd lengths, and the minimum distance is proven to be four. Moreover, the transformation to quantum stabilizer code is also considered. Six optimal quantum stabilizer codes $[[5, 1, 3]]$, $[[7, 1, 3]]$, $[[9, 1, 3]]$, $[[6, 0, 4]]$, $[[8, 0, 4]]$, and $[[10, 0, 4]]$ have been interpreted from corresponding linear codes with the standard form to show their practicality in quantum stabilizer codes. This code construction method can be applied for the code, can correct at least one error in quantum information theory, and can have a good quantum state.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation discrete logarithms and factoring," in *Proc. IEEE Symposium on FOCS*, Santa Fe New Mexico, 1994.

[2] L. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.* vol. 79, no. 2, pp. 325–328, July 1997.

[3] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A.* vol. 52, no. 4, pp. 2493–2496, Oct. 1995.

[4] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A.* vol. 54, pp. 1098–1106, Aug. 1996.

[5] D. Gottesman, *Ph.D. Dissertation,* California Institute of Technology, 1997.

[6] R. Penrose, *Quantum Error Correction and Fault Tolerant Quantum Computing.* CRC Press. Inc. BocaRaton. FL. USA, 2007.

[7] A. R. Calderbank and P. W. Shor, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory* vol. 53, no. 3, pp. 1183–1188, 2007.

[8] C. Dong and S. Yaoliang, "Novel class of entanglement-assisted quantum codes with minimal ebits," *J. Comm. Netw.* vol. 15, no. 2, April 2013.

[9] M. Grassl, W. Geiselmann, and T. Beth, "Quantum reed-solomon codes," *App. Alge. Algorm. Error-Correcting Codes,* vol. 1719, pp. 231–244, 1996.

[10] D. M. Nguyen and S. Kim, "Minimal-entanglement entanglement-assisted quantum error correction codes from modified circulant matrices," *Symmetry*, vol. 9, pp. 122, July 2017.

[11] S. M. Zhao, Y. Xiao, Y. Zhu, X. L. Zhu, and M. H. Hsieh, "New class of quantum codes constructed from cyclic difference set," *Int. J. Quantum Inform.,* vol. 10, no. 1, pp. 1250015, 2012.

[12] Y. Xie, J. Yuan, and Q. Sun, "On design of quantum stabilizer codes from quadratic residues sets," [Online]. Available: https://arxiv.org/pdf/1407.8249v1.pdf

[13] A. Naghipour, M. A. Jafarizadeh, and S. Shahmorad, "Quantum stabilizer codes from abelian and non-abelian groups association schemes," *Int. J. Quantum Inf.,* vol. 13, no. 3, pp. 1550021, 2015.

[14] A. R. Calderbank, E. M. Rains, P. W. 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, July 1998.

[15] J. L. Kim *et al*., "New self-dual codes over GF(4) with the highest known minimum weights," *IEEE Trans. Inf. Theory,* vol. 47, no. 4, pp. 1575–1580, May 2001.

[16] A. Thangaraj and S. W. McLaughlin, "Quantum codes from cyclic codes over GF(4^m)," *IEEE Trans. Inf. Theory,* vol. 47, no. 3, pp. 1176–1178, Mar. 2001.

[17] M. Grassl, *Bounds on the Minimum Distance of Linear Codes and Quantum Codes.* [Online]. Available: http://www.codetables.de

[18] L. E. Danielsen, *M.S. thesis,* University of Bergen, 2005.

[19] R. Penrose, *Quantum Computing for Computer Scientists.* Cambridge University Press New York, NY, USA, 2008.

Duc Manh Nguyen was born in Hai Duong City, Viet Nam in 1989. He received the bachelor degree in Electronic and Telecommunication from HaNoi University of Science and Technology in 2012. He was software engineer at Samsung Electronic Viet Nam from 2012 till 2014. He is currently studying for the Ph.D. degree at Coding and Information Theory Lab, University of Ulsan, Korea. His research interests include quantum information theory, quantum error correction code, and quantum cryptography.

Sunghwan Kim received his B.S., M.S., and Ph.D. degrees from Seoul National University, Korea, in 1999, 2001, and 2005, respectively. He was a Postdoctoral Visitor at the Georgia Institute of Technology (GeorgiaTech) from 2005 till 2007 and a Senior Engineer at Samsung Electronics from 2007 till 2011. He is currently an Associate Professor at the School of Electrical Engineering, University of Ulsan, Korea. His main research interests are 5G communication, information theory, visible light communication, and security.