International Journal of Modern Physics B
Vol. 33, No. 24 (2019) 1950274 (16 pages)

DOI: 10.1142/S0217979219502746

New construction of binary and nonbinary quantum stabilizer codes based on symmetric matrices

Duc Manh Nguyen* and Sunghwan Kim†

School of Electrical Engineering,
University of Ulsan, Ulsan 44610, Korea
**nguyenmanhduc18@gmail.com*
†*sungkim@ulsan.ac.kr*

Received 24 June 2019
Revised 31 July 2019
Accepted 31 July 2019
Published 4 October 2019

In this paper, we propose two construction methods for binary and nonbinary quantum stabilizer codes based on symmetric matrices. In the first construction, we use the identity and symmetric matrices to generate parity-check matrices that satisfy the symplectic inner product (SIP) for the construction of quantum stabilizer codes. In the second construction, we modify the first construction to generate parity-check matrices based on the Calderbank–Shor–Stean structure for the construction of quantum stabilizer codes. The binary and nonbinary quantum stabilizer codes whose parameters achieve equality of the quantum singleton bound are investigated with the code lengths ranging from 4 to 12.

Keywords: Quantum stabilizer code; Calderbank–Shor–Stean codes; symmetric matrix; symplectic inner product.

PACS numbers: 03.67.-a, 03.67.Pp

1. Introduction

Quantum mechanisms utilize two degrees of freedom of photons, allowing for various probabilities of possible measurement outcomes of a physical system.[1] Quantum processing devices are based on quantum mechanisms, which give us the ability to deal with the various tasks such as factoring a large integer number in polynomial time,[2] searching from un-ordered sets,[3] and improving the security of cryptography.[4,5] However, the effects of the noisy and imperfect environments of a quantum channel can reduce these performance advantages. Therefore, quantum error correcting codes (QECCs) have been proposed to protect quantum information from noisy environments. The first QECCs were proposed in the 1990s by

†Corresponding author.

Shor[6] and Steane,[7] and the general theory for QECCs, i.e., the stabilizer formalism, was introduced in 1997 by Daniel Gottesman.[8] In 1996, two independent research groups, Calderbank and Shor[9] and Stean[7] adopted the relationship between quantum codes and self-orthogonal codes. Therefore, quantum codes can be constructed using two classical linear error correction codes, i.e., the Calderbank–Shor–Stean (CSS) structure. The advantage of the CSS structure is that we can obtain the parameters of quantum codes directly from the parameters of two classical codes. Therefore, the CSS structure has been used by numerous researchers to construct quantum binary codes, such as BCH codes,[10] Reed Solomon codes,[11] quasi-cyclic LDPC codes[12] and SPC codes.[13] Quantum computations are performed based on the quantum circuit model using two different techniques, the first technique was provided by Deutsch, Deutsch–Jozsa, Grover, Shor and so on.[2,3,14,15] In this technique, a set of unitary transformations is applied on a quantum system and then the problem is solved according to the state of one qubit, or more, after measurement process to solve the problem at hand. The second is called Zidan's technique that solves the problem at hand by applying some unitary transformation(s) on a system of size n qubits, then measures the degree of entanglement (by concurrence measure) between two ancillary qubits. Hence, the solution of the problem at hand is obtained based on the concurrence value.[16] Recently, with the development of quantum information theory, more applications for QECCs in quantum information have been demonstrated, such as quantum algorithms,[16,17] quantum simulations,[18] and quantum network coding.[19]

The high-dimensional degrees of freedom of photons can encode more quantum information than their two-dimensional counterparts, and this increased information capacity has advantages in quantum applications, such as quantum communication, quantum cryptography and quantum algorithm. However, controlling and manipulating these systems have many challenges; QECCs form one solution that aims to solve these issues.[20] Additionally, QECCs for high-dimensional quantum systems must be considered in nonbinary cases by using "nonbinary quantum stabilizer codes." The CSS structure has been considered for nonbinary quantum codes for qudits, where the classical codes are over the Galois field.[21] Since the self-orthogonal codes over a finite field that satisfy the conditions of the CSS structure-based quantum code and self-orthogonal codes can be constructed effectively by combinatoric design, cyclic codes and constacyclic codes, many quantum codes have been constructed in recent years; these are based on the CSS structure via a finite field.[22–24] In addition, the stabilizer formalism allows quantum codes to be presented by binary matrices, i.e., parity-check matrices with symplectic inner product (SIP) constraints.[25–27] Hence, we can consider the construction of quantum codes based on the CSS structure to be in the form of matrices. For example, in Ref. 13, the authors used a permutation-based technique for this construction, and in Ref. 28 the authors searched for a suitable monomial matrix for the construction. The papers[13,28] provided some good quantum nonbinary codes with the singleton bound; however, many constructions remain to be discovered.

In this paper, we propose the new construction of quantum codes from symmetric matrices that are based on the CSS structure. The parity-check matrices are first generated from two constructions and proven to satisfy the SIP for the construction of binary and nonbinary quantum stabilizer codes. Then, the parameters of these codes are calculated and explained in detail. Some quantum codes are proven to achieve equality of the quantum singleton bound. The organization of this paper is as follows. In Sec. 2, we review some basic concepts related to quantum information theory, such as qubits, qupits and QECC. In Sec. 3, two methods of constructing quantum codes for binary and nonbinary cases from the symmetric matrices based on the CSS structure are proposed. Some quantum codes with good parameters are constructed to show the practicality of our construction.

2. Preliminaries

2.1. *Quantum information theory*

Bits or binary digits are the basic units of information that are used in classical computing and digital communication. The basic unit of quantum information is called a quantum bit (*qubit*). If a bit has two basic states of zero or one, a qubit uses the superposition principle of the two basic states. Hence, we use the two-dimensional Hilbert space (H_2) of complex number to model the quantum information. The Hilbert space is spanned by two basic states $H_2 = \text{span}\{|0\rangle, |1\rangle\}$ where the mathematical expressions are $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Therefore, the superposition state of a quantum system is denoted as $|\psi\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = a_1|0\rangle + a_2|1\rangle$, where a_1 and a_2 are complex numbers that satisfy the equation: $|a_1|^2 + |a_2|^2 = 1$. In a quantum system, if quantum states are used n times in a single qubit (n-qubits) physical system, the system consists of n-times tensor product of two-dimensional Hilbert space (${H_2}^{\otimes n}$). Since the quantum system requires unitary transformations of the quantum states, Pauli matrices that includes the identity matrix $\mathbf{I}$, $\mathbf{X}$ (bit flip), $\mathbf{Z}$ (phase flip), and $\mathbf{Y}$ (the combination of bit and phase flips)[4,5] with the size 2×2 are considered as the bases generators of all unitary transformations. The Pauli group P_1 for one qubit, i.e., $P_1 = \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$, is closed under multiplication. Generally, the n-qubit Pauli group P_n is n-times the tensor product of Pauli group P_1. P_n has the most important property in that any two elements in P_n are either commutative or anti-commutative.

The proposals for the first generation of quantum systems make use of two-level systems as the basis elements. However, recent innovations in QECC, quantum cryptography and quantum algorithms demonstrate that there are advantages in using high-level quantum systems over qubit analogues. To describe the high-level quantum system, we use the Galois field for the basic elements. Let p be a prime number and the Galois field GF_p be the finite field of p elements $\{0, 1, 2, \ldots, p-1\}$ that is closed under addition and multiplication modulo p. Additionally, assume a qupit (p-level quantum bit) whose Hilbert space (H_p) is represented by orthogonal bases $H_p = \mathrm{span}\{|0\rangle, |1\rangle, \ldots, |p-1\rangle\}$, where the mathematical expression is

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{p\times 1}, |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}_{p\times 1}, \ldots, |p-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}_{p\times 1}.$$

Let ω be the pth root of unity, $\omega = e^{\frac{2\pi i}{p}}$. Additionally, we define the generalized Pauli matrix[33,35] such that the generalization of the bit-flip matrix is

$$\mathbf{X}(p) = \sum_{j=0}^{p-1} |j+1\rangle\langle j| = \begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix}.$$

Then, we have $\mathbf{X}(p)|r\rangle = |r+1\rangle$ and $\mathbf{X}(p)^p = \mathbf{X}(p)^0 = \mathbf{I}(p)$. The generalization of the phase-flip matrix[33,35] is

$$\mathbf{Z}(p) = \sum_{j=0}^{p-1} \omega^j |j\rangle\langle j| = \begin{bmatrix} \omega^0 & 0 & \ldots & 0 \\ 0 & \omega^1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \omega^{p-1} \end{bmatrix}.$$

Then, we have $\mathbf{Z}(p)\,|r\rangle = \omega^r\,|r\rangle$ and $\mathbf{Z}(p)^p = \mathbf{Z}(p)^0 = \mathbf{I}(p)$. We note that here $\mathbf{X}(p)$, $\mathbf{Z}(p)$, $\mathbf{Y}(p)$, and $\mathbf{I}(p)$ are the generalized Pauli matrices over GF_p with the size $p \times p$.

2.2. *QECC*

The quantum code for the binary case with parameter $[[n, k, d_{\min}]]$ encodes k information qubits into the system of n qubits, and it can correct the $\lfloor \frac{d_{\min}-1}{2} \rfloor$ error. The first quantum code is the Shor code with parameters [[9,1,3]]; this is based on repetition codes. The second quantum code is [[7,1,3]], which is based on the classical hamming code [7,1,3] with a CSS structure. Next, the stabilizer formalism is used to express the quantum codes. With the stabilizer formalism, quantum codes are viewed via the group theory of the quantum stabilizer operator; thus, we are working with quantum operators rather than with quantum states. Let $H^{\otimes n}$ be the state space of n-qubits. The quantum stabilizer group S is an Abelian subgroup of P_n and is closed under multiplication. Further, there is no trivial subspace $C_S \subset H^{\otimes n}$ that is fixed (or stabilized) by S. The stabilized C_S defines a codeword such that $C_S = \{|\psi\rangle \in H^{\otimes n} : \mathbf{g}|\psi\rangle = |\psi\rangle, \forall \mathbf{g} \in S\}$. The quantum code with parameter $[[n, k, d_{\min}]]$ corresponds to the group S with its generators,

$g = \{\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_{n-k}\}$. The constraints for the generators in g are such that any two elements in g must commute with each other. Since the number of generators $(n-k)$ is less than or equal to n, $(n-k)$ is a well-defined quantity; it is called the rank of the stabilizer. If the stabilizer has the rank n $(k = 0)$, the stabilizer will be referred to as the full rank stabilizer and the corresponding quantum code is denoted as $[[n, 0, d_{\min}]]$. The codewords, or the stabilizer state of the full rank stabilizers group, will be called the graph state; this has many applications in one-way quantum computers, secure state distribution, secret sharing, etc.[29] It is known that, for a quantum code $[[n, k, d_{\min}]]_p$, the quantum singleton bound or Knill–Laflamme bound is $n - k \geq 2(d_{\min} - 1)$.[30] Then, the quantum codes whose parameters satisfy $d_{\min} = \lfloor \frac{n+2}{2} \rfloor$ will be maximum distance separable codes, which are referred to as the optimal quantum codes.[31] Since we can express the generator of the quantum stabilizer code as a binary field, due to the fact that any n-qubit Pauli operator can be expressed as a multiplication of an $\mathbf{X}$-containing operator and an $\mathbf{Z}$-containing operator, we define the mapping between Pauli operators and binary vectors as $\mathbf{I} \leftrightarrow (0, 0)$, $\mathbf{X} \leftrightarrow (1, 0)$, $\mathbf{Z} \leftrightarrow (0, 1)$ and $\mathbf{Y} \leftrightarrow (1, 1)$. As a consequence, $(n-k)$ generators of an $[[n, k]]$ code are formed in a binary field as $\mathbf{H} = [\mathbf{H_X}|\mathbf{H_Z}]$ where $\mathbf{H_X}, \mathbf{H_Z}$ are $(n-k) \times n$ binary matrices and "|" denotes the row concatenation. Hence, $\mathbf{H}$ represents binary matrices with the size $(n-k) \times 2n$. The commutative constraint between generators must change to the symplectic product constraint as

$$\mathbf{H_Z} \times \mathbf{H_X}^T + \mathbf{H_X} \times \mathbf{H_Z}^T = \mathbf{0}_m, \tag{1}$$

where $\mathbf{0}_m$ is the matrix of all zero elements with size $m \times m$.

Above, we considered quantum stabilizer codes with a binary form over $\{0, 1\}^{2n}$. Since these codes are defined over $\{0, 1\}^{2n}$, we call them "quantum binary codes." Generally, we denote quantum nonbinary codes with parameters $[[n, k, d_{\min}]]_p$, which are defined over GF_p^n (the *qupits* case). The quantum code for this case corresponds to the commutative group of generalized Pauli operators. Based on the generalized Pauli matrices $\mathbf{X}(p)$ and $\mathbf{Z}(p)$ in Sec. 2.1, we have $\mathbf{Z}(p)^{\mathbf{b}}\mathbf{X}(p)^{\mathbf{a}} = \omega^{\mathbf{a}\bullet\mathbf{b}}\mathbf{X}(p)^{\mathbf{a}}\mathbf{Z}(p)^{\mathbf{b}}$ with the following notations:

(1) $\mathbf{a} \bullet \mathbf{b} = \sum_{i=1}^{n} a_i \ldots b_i$ where $\mathbf{a} = (a_1 a_2 \ldots a_n)$ and $\mathbf{b} = (b_1 b_2 \ldots b_n)$,
(2) $\mathbf{X}(p)^{\mathbf{a}} = \mathbf{X}(p)^{a_1} \otimes \mathbf{X}(p)^{a_2} \otimes \cdots \otimes \mathbf{X}(p)^{a_n}$,
(3) $\mathbf{Z}(p)^{\mathbf{b}} = \mathbf{Z}(p)^{b_1} \otimes \mathbf{Z}(p)^{b_2} \otimes \cdots \otimes \mathbf{Z}(p)^{b_n}$.

We consider the commutative property between $\mathbf{X}(p)^{\mathbf{u}_1}\mathbf{Z}(p)^{\mathbf{v}_1}$ and $\mathbf{X}(p)^{\mathbf{u}_2}\mathbf{Z}(p)^{\mathbf{v}_2}$. Since

(1) $(\mathbf{X}(p)^{\mathbf{u}_1}\mathbf{Z}(p)^{\mathbf{v}_1})(\mathbf{X}(p)^{\mathbf{u}_2}\mathbf{Z}(p)^{\mathbf{v}_2}) = (\mathbf{X}(p)^{\mathbf{u}_1}\omega^{\mathbf{u}_2\cdot\mathbf{v}_1}\mathbf{X}(p)^{\mathbf{u}_2})(\mathbf{Z}(p)^{\mathbf{v}_1}\mathbf{Z}(p)^{\mathbf{v}_2}) = \omega^{\mathbf{u}_2\cdot\mathbf{v}_1}(\mathbf{X}(p)^{\mathbf{u}_1}\mathbf{X}(p)^{\mathbf{u}_2})(\mathbf{Z}(p)^{\mathbf{v}_1}\mathbf{Z}(p)^{\mathbf{v}_2}$,
(2) $(\mathbf{X}(p)^{\mathbf{u}_2}\mathbf{Z}(p)^{\mathbf{v}_2})(\mathbf{X}(p)^{\mathbf{u}_1}\mathbf{Z}(p)^{\mathbf{v}_1}) = (\mathbf{X}(p)^{\mathbf{u}_2}\omega^{\mathbf{u}_1\cdot\mathbf{v}_2}\mathbf{X}(p)^{\mathbf{u}_1})(\mathbf{Z}(p)^{\mathbf{v}_2}\mathbf{Z}(p)^{\mathbf{v}_1}) = \omega^{\mathbf{u}_1\cdot\mathbf{v}_2}(\mathbf{X}(p)^{\mathbf{u}_2}\mathbf{X}(p)^{\mathbf{u}_1})(\mathbf{Z}(p)^{\mathbf{v}_2}\mathbf{Z}(p)^{\mathbf{v}_1}$,

$\mathbf{X}(p)^{\mathbf{u}_1}\mathbf{Z}(p)^{\mathbf{v}_1}$ and $\mathbf{X}(p)^{\mathbf{v}_2}\mathbf{Z}(p)^{\mathbf{v}_2}$ are commutative if and only if $\omega^{\mathbf{u}_1\bullet\mathbf{v}_2} = \omega^{\mathbf{u}_2\bullet\mathbf{v}_1}$, hence $\mathbf{u}_1 \bullet \mathbf{v}_2 = \mathbf{u}_2 \bullet \mathbf{v}_1$. Then, the representation of the quantum stabilizer code for the qupits case is $\mathbf{H} = [\mathbf{H_{X(\mathit{p})}} \ \mathbf{H_{Z(\mathit{p})}}]$, where $\mathbf{H_{X(\mathit{p})}}, \mathbf{H_{Z(\mathit{p})}}$ are the matrices over the Galois field and the SIP, which is satisfies

$$\mathbf{H_{X(\mathit{p})}} \otimes \mathbf{H_{Z(\mathit{p})}}^T = \mathbf{H_{Z(\mathit{p})}} \otimes \mathbf{H_{X(\mathit{p})}}^T. \tag{2}$$

Here, the multiplication ($\otimes$) and summation ($\oplus$) operators are over the GF_p.

The CSS structure is an advantageous construction for quantum codes since the quantum codes can be investigated using the best classical codes based on the CSS structure. In addition, both quantum binary codes and quantum nonbinary codes can be constructed by the CSS structure. Hence, we summarize the generalized CSS structure for the construction of binary and nonbinary quantum codes in the following Lemma.

Lemma 1 (Quantum CSS structure). *Let C_1 and C_2 be two linear codes with parameters $[[n, k_1, d_1]]_p$ and $[[n, k_2, d_2]]_p$, respectively. If ${C_2}^{\perp} \subseteq C_1$, then there exists a quantum code with the parameter $[[n, k_1 + k_2 - n, d \geq min\{d_1, d_2\}]]_p$.*

As with the stabilizer formalism, the parity-check matrix of quantum codes based on the CSS structure can be expressed as follows:

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}(C_2) & \mathbf{0} \\ \mathbf{0} & \mathbf{H}(C_1) \end{bmatrix}.$$

The SIP for the above matrix is given as $\mathbf{H}(C_2) \times \mathbf{H}(C_1)^T = \mathbf{0}$.

3. Proposed Quantum Stabilizer Code Construction

3.1. *Quantum stabilizer codes for the binary case*

In this subsection, we propose the construction of quantum stabilizer codes for the binary case. Construction 1a considers the construction of a parity-check matrix based on identity and symmetric matrices. In another case, the parity-check matrix in construction 2a is based on the CSS structure.

Construction 1a. Let $\mathbf{I}$ be the identity binary matrix with size $n \times n$. Let $\mathbf{A}$ be the symmetric matrix ($\mathbf{A}^T = \mathbf{A}$) over binary with size $n \times n$. The proposed parity-check matrix has the following form:

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{A} \end{bmatrix}. \tag{3}$$

This corresponds to the quantum stabilizer code with parameter $[[n, 0]]$.

Proof. Based on the properties of symmetric matrices, we have:

$$\mathbf{I}\mathbf{A}^T + \mathbf{A}\mathbf{I}^T = \mathbf{A}^T + \mathbf{A} = \mathbf{0}.$$

The SIP equation (1) for the parity-check matrix in Eq. (3) is satisfied. Since $\mathbf{H}$ has the size $n \times 2n$, we get the quantum stabilizer code with parameter $[[n, 0]]$. □

Construction 2a. Let $\mathbf{I}$ be the identity binary matrix with size $n \times n$. Let $\mathbf{A}$ be the symmetric matrix ($\mathbf{A}^T = \mathbf{A}$) over binary with size $n \times n$. The proposed parity-check matrix has the following form:

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} \mathbf{I} & \mathbf{A} \end{bmatrix} & \mathbf{0} \\ \mathbf{0} & \begin{bmatrix} \mathbf{A} & \mathbf{I} \end{bmatrix} \end{bmatrix}. \tag{4}$$

This corresponds to the quantum stabilizer code with parameter $[[2n, 0, d]]$.

Proof. Based on the definition in Eq. (4), we have the following formulation:

$$\begin{aligned} \mathbf{H}_1 \times {\mathbf{G}_2}^T &= \begin{bmatrix} \mathbf{I} & \mathbf{A} \end{bmatrix} \times \begin{bmatrix} \mathbf{A} & \mathbf{I} \end{bmatrix}^T = \begin{bmatrix} \mathbf{I} & \mathbf{A} \end{bmatrix} \times \begin{bmatrix} \mathbf{A}^T \\ \mathbf{I}^T \end{bmatrix}, \\ &= \mathbf{I} \times \mathbf{A}^T + \mathbf{A} \times \mathbf{I}^T = \mathbf{A}^T + \mathbf{A} = \mathbf{0}. \end{aligned}$$

In addition, we also have:

$$\begin{aligned} \mathbf{G}_2 \times {\mathbf{H}_1}^T &= \begin{bmatrix} \mathbf{A} & \mathbf{I} \end{bmatrix} \times \begin{bmatrix} \mathbf{I} & \mathbf{A} \end{bmatrix}^T = \begin{bmatrix} \mathbf{A} & \mathbf{I} \end{bmatrix} \times \begin{bmatrix} \mathbf{I}^T \\ \mathbf{A}^T \end{bmatrix}, \\ &= \mathbf{A} \times \mathbf{I}^T + \mathbf{I} \times \mathbf{A}^T = \mathbf{A} + \mathbf{A}^T = \mathbf{0}. \end{aligned}$$

Then, the SIP for the parity-check matrix in (4) is

$$\begin{aligned} \mathbf{H_X} \times {\mathbf{H_Z}}^T + \mathbf{H_Z} \times {\mathbf{H_X}}^T &= \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{0} \\ \mathbf{G}_2 \end{bmatrix}^T + \begin{bmatrix} \mathbf{0} \\ \mathbf{G}_2 \end{bmatrix} \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{0} \end{bmatrix}^T, \\ &= \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{0}^T & {\mathbf{G}_2}^T \end{bmatrix} + \begin{bmatrix} \mathbf{0} \\ \mathbf{G}_2 \end{bmatrix} \begin{bmatrix} {\mathbf{H}_1}^T & \mathbf{0} \end{bmatrix}, \\ &= \begin{bmatrix} \mathbf{H}_1 \times \mathbf{0}^T & \mathbf{H}_1 \times {\mathbf{G}_2}^T \\ \mathbf{0} \times \mathbf{0}^T & \mathbf{0} \times {\mathbf{G}_2}^T \end{bmatrix} + \begin{bmatrix} \mathbf{0} \times {\mathbf{H}_1}^T & \mathbf{0} \times \mathbf{0}^T \\ \mathbf{G}_2 \times {\mathbf{H}_1}^T & \mathbf{G}_2 \times \mathbf{0}^T \end{bmatrix}, \\ &= \begin{bmatrix} \mathbf{0} & \mathbf{H}_1 \times {\mathbf{G}_2}^T \\ \mathbf{G}_2 \times {\mathbf{H}_1}^T & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}, \end{aligned}$$

Since $\mathbf{H}$ has the size $2n \times 4n$, we get the quantum stabilizer code with parameter $[[2n, 0]]$. □

In the following examples, the quantum stabilizer codes for the qubits case are given. In Examples 1–3, we consider the quantum stabilizer codes for the qubit case based on construction 1a where the code lengths are 5, 6, and 7. In the examples, we first give the construction of the parity-check matrices, and then the parameter of the code is calculated by the Magma tool's function *QuantumCode*, *MinimumWeight*.[32] Since any symmetric matrix satisfies our construction, there are many candidates for the parity-check matrices. Therefore, for each code length, we give the quantum stabilizer code with a largest minimum distance, which we calculated by the Magma tool's function.

Example 1. We consider the following parity-check matrix with the size 5×10:

$$\mathbf{H} = \begin{bmatrix} 1,0,0,0,0 & 1,1,0,1,1 \\ 0,1,0,0,0 & 1,0,1,1,0 \\ 0,0,1,0,0 & 0,1,1,0,1 \\ 0,0,0,1,0 & 1,1,0,1,0 \\ 0,0,0,0,1 & 1,0,1,0,1 \end{bmatrix}.$$

It corresponds to the quantum stabilizer code with parameter $[[5, 0, 3]]$.

Example 2. We consider the following parity-check matrix with the size 6×12:

$$\mathbf{H} = \begin{bmatrix} 1,0,0,0,0,0 & 1,0,1,1,0,1 \\ 0,1,0,0,0,0 & 0,0,1,0,1,1 \\ 0,0,1,0,0,0 & 1,1,0,0,0,1 \\ 0,0,0,1,0,0 & 1,0,0,1,1,1 \\ 0,0,0,0,1,0 & 0,1,0,1,0,1 \\ 0,0,0,0,0,1 & 1,1,1,1,1,0 \end{bmatrix}.$$

This corresponds to the quantum stabilizer code with parameter $[[6, 0, 4]]$.

Example 3. We consider the following parity-check matrix with the size 7×14:

$$\mathbf{H} = \begin{bmatrix} 1,0,0,0,0,0,0 & 1,0,1,0,1,0,1 \\ 0,1,0,0,0,0,0 & 0,1,0,0,1,0,1 \\ 0,0,1,0,0,0,0 & 1,0,1,1,0,1,1 \\ 0,0,0,1,0,0,0 & 0,0,1,0,1,1,0 \\ 0,0,0,0,1,0,0 & 1,1,0,1,1,0,1 \\ 0,0,0,0,0,1,0 & 0,0,1,1,0,1,0 \\ 0,0,0,0,0,0,1 & 1,1,1,0,1,0,1 \end{bmatrix}.$$

This corresponds to the quantum stabilizer code with parameter $[[7, 0, 3]]$.

In the following examples (from Examples 4–8), we consider the quantum stabilizer codes for the qubit case based on the construction 2a with the code lengths upto 12. As construction 2a requires the symmetric matrices to construct the parity-check matrix, there are many candidates for the symmetric matrices. By using the CSS structure, we can determine the parameter of the corresponding quantum stabilizer code via the parameters of two classical codes. Then, we choose the symmetric matrices with large maximum distances to get quantum stabilizer codes with large maximum distances.

Example 4. We consider two classical codes with the parity-check matrices and the generators matrices as follows:

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,1,0 \\ 0,1,0,1 \end{bmatrix}$$

(classical $[4,2,2]$ code) and

$$\mathbf{G}_2 = \begin{bmatrix} 1,0,1,0 \\ 0,1,0,1 \end{bmatrix}$$

(classical $[4,2,2]$ code).

This corresponds to the quantum stabilizer code with parameter $[[4,0,2]]$.

Example 5. We consider two classical codes with the parity-check matrices and the generators matrices as follows:

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,0,1,1,1 \\ 0,1,0,1,1,0 \\ 0,0,1,1,0,1 \end{bmatrix}$$

(classical $[6,3,3]$ code) and

$$\mathbf{G}_2 = \begin{bmatrix} 1,1,1,1,0,0 \\ 1,1,0,0,1,0 \\ 1,0,1,0,0,1 \end{bmatrix}$$

(classical $[6,3,3]$ code).

This corresponds to the quantum stabilizer code with parameter $[[6,0,3]]$.

Example 6. We consider two classical codes with the parity-check matrices and the generators matrices as follows:

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,0,0,0,0,1,1,1,1 \\ 0,1,0,0,0,1,1,0,1,1 \\ 0,0,1,0,0,1,0,1,1,1 \\ 0,0,0,1,0,1,1,1,1,0 \\ 0,0,0,0,1,1,1,1,0,1 \end{bmatrix}$$

($[8,4,4]$ code) and

$$\mathbf{G_2} = \begin{bmatrix} 0,1,1,1,1,1,0,0,0,0 \\ 1,1,0,1,1,0,1,0,0,0 \\ 1,0,1,1,1,0,0,1,0,0 \\ 1,1,1,1,0,0,0,0,1,0 \\ 1,1,1,0,1,0,0,0,0,1 \end{bmatrix}$$

($[8,4,4]$ code).

This corresponds to the quantum stabilizer code with parameter $[[8,0,4]]$.

Example 7. We consider two classical codes with the parity-check matrices and the generators matrices as follows:

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,0,0,0,0,1,1,1,1 \\ 0,1,0,0,0,1,1,0,1,1 \\ 0,0,1,0,0,1,0,1,1,1 \\ 0,0,0,1,0,1,1,1,1,0 \\ 0,0,0,0,1,1,1,1,0,1 \end{bmatrix}$$

([10,5,4] code) and

$$\mathbf{G}_2 = \begin{bmatrix} 0,1,1,1,1,1,0,0,0,0 \\ 1,1,0,1,1,0,1,0,0,0 \\ 1,0,1,1,1,0,0,1,0,0 \\ 1,1,1,1,0,0,0,0,1,0 \\ 1,1,1,0,1,0,0,0,0,1 \end{bmatrix}$$

([10,5,4] code).

This corresponds to the quantum stabilizer code with parameter [[10,0,4]].

Example 8. We consider two classical codes with the parity-check matrices and the generators matrices as follows:

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,0,0,0,0,1,0,1,0,1,0 \\ 0,1,0,0,0,0,0,0,1,1,1,1 \\ 0,0,1,0,0,0,1,1,1,0,1,1 \\ 0,0,0,1,0,0,0,1,0,1,1,1 \\ 0,0,0,0,1,0,1,1,1,1,1,0 \\ 0,0,0,0,0,1,0,1,1,1,0,1 \end{bmatrix}$$

([12,6,4] code) and

$$\mathbf{G}_2 = \begin{bmatrix} 1,0,1,0,1,0,1,0,0,0,0,0 \\ 0,0,1,1,1,1,0,1,0,0,0,0 \\ 1,1,1,0,1,1,0,0,1,0,0,0 \\ 0,1,0,1,1,1,0,0,0,1,0,0 \\ 1,1,1,1,1,0,0,0,0,0,1,0 \\ 0,1,1,1,0,1,0,0,0,0,0,1 \end{bmatrix}$$

([12,6,4] code).

This corresponds to the quantum stabilizer code with parameter [[12,0,4]].

3.2. *Quantum stabilizer codes for the nonbinary case*

In this subsection, we propose the construction of quantum stabilizer codes for the nonbinary case. Construction 1b considers the construction of the parity-check matrix over GF_p, which is based on identity and symmetric matrices over GF_p. In construction 2b, the parity-check matrices over GF_p are based on the CSS structure.

Construction 1b. Let $\mathbf{I}$ be a matrix with size $n \times n$ over GF_p, where all the elements are zeros except for those on the main diagonal, which are one. Additionally, the matrix $\mathbf{A}$ is a symmetric matrix with size $n \times n$ over GF_p, $\mathbf{A}^T = \mathbf{A}$. The proposed parity-check matrix has the following form:

$$\mathbf{H} = \begin{bmatrix}\mathbf{I} & \mathbf{A}\end{bmatrix}, \tag{5}$$

which corresponds to the quantum stabilizer code with parameter $[[n, 0]]_p$.

Proof. Based on the properties of $\mathbf{A}$ and $\mathbf{I}$, we have

$$\mathbf{I} \times \mathbf{A}^T = \mathbf{A}^T = \mathbf{A} = \mathbf{A} \times \mathbf{I}^T.$$

The SIP Eq. (2) for the parity-check matrix in Eq. (5) is satisfied. Since $\mathbf{H}$ has the size $n \times 2n$, we get the quantum stabilizer code with parameter $[[n, 0]]_p$. $\square$

Construction 2b. Let $\mathbf{I}$ be the matrix with size $n \times n$ over GF_p, where all the elements are zeros except for those on the main diagonal, which are one. Additionally, the matrix $\mathbf{A}$ is the symmetric matrix ($\mathbf{A}^T = \mathbf{A}$) with size $n \times n$ over GF_p, and $-\mathbf{A}$ denotes the matrix where its elements are the minus modulo p for corresponding elements of $\mathbf{A}$. The proposed parity-check matrix has the following form:

$$\mathbf{H} = \begin{bmatrix}\begin{bmatrix}\mathbf{I} & \mathbf{A}\end{bmatrix} & \mathbf{0} \\ \mathbf{0} & \begin{bmatrix}-\mathbf{A} & \mathbf{I}\end{bmatrix}\end{bmatrix}, \tag{6}$$

which corresponds to the quantum stabilizer code with parameter $[[2n, 0]]_p$.

Proof. Based on the definition in Eq. (6), we have the following formula:

$$\begin{aligned}\mathbf{H}_1 \times {\mathbf{G}_2}^T &= \begin{bmatrix}\mathbf{I} & \mathbf{A}\end{bmatrix} \times \begin{bmatrix}-\mathbf{A} & \mathbf{I}\end{bmatrix}^T = \begin{bmatrix}\mathbf{I} & \mathbf{A}\end{bmatrix} \times \begin{bmatrix}-\mathbf{A}^T \\ \mathbf{I}^T\end{bmatrix}, \\ &= \mathbf{I} \times (-\mathbf{A}^T) + \mathbf{A} \times \mathbf{I}^T = -\mathbf{A} + \mathbf{A} = \mathbf{0}.\end{aligned}$$

Then, we have

$$\begin{aligned}\mathbf{H_X} \times {\mathbf{H_Z}}^T &= \begin{bmatrix}\mathbf{H}_1 \\ \mathbf{0}\end{bmatrix} \times \begin{bmatrix}\mathbf{0} \\ \mathbf{G}_2\end{bmatrix}^T = \begin{bmatrix}\mathbf{H}_1 \\ \mathbf{0}\end{bmatrix} \times \begin{bmatrix}\mathbf{0}^T & {\mathbf{G}_2}^T\end{bmatrix}, \\ &= \begin{bmatrix}\mathbf{H}_1 \times \mathbf{0}^T & \mathbf{H}_1 \times {\mathbf{G}_2}^T \\ \mathbf{0} \times \mathbf{0}^T & \mathbf{0} \times {\mathbf{G}_2}^T\end{bmatrix} = \begin{bmatrix}\mathbf{0} & \mathbf{H}_1 \times {\mathbf{G}_2}^T \\ \mathbf{0} & \mathbf{0}\end{bmatrix}.\end{aligned}$$

In addition, we also have the following formula:

$$\mathbf{H_Z} \times \mathbf{H_X}^T = \begin{bmatrix} \mathbf{0} \\ \mathbf{G}_2 \end{bmatrix} \times \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{0} \end{bmatrix}^T = \begin{bmatrix} \mathbf{0} \\ \mathbf{G}_2 \end{bmatrix} \times \begin{bmatrix} \mathbf{H}_1{}^T & \mathbf{0} \end{bmatrix},$$

$$= \begin{bmatrix} \mathbf{0} \times \mathbf{H}_1{}^T & \mathbf{0} \times \mathbf{0}^T \\ \mathbf{G}_2 \times \mathbf{H}_1{}^T & \mathbf{G}_2 \times \mathbf{0}^T \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{G}_2 \times \mathbf{H}_1{}^T & \mathbf{0} \end{bmatrix}.$$

Thus, $\mathbf{H_X} \times \mathbf{H_Z}^T = \mathbf{H_Z} \times \mathbf{H_X}^T$ $(= [\mathbf{0}])$ and the parity-check matrix in Eq. (6) is satisfied by the SIP equation (2). Since $\mathbf{H}$ has the size $2n \times 4n$, we get the quantum stabilizer code with parameter $[[2n, 0]]_p$. □

In the following examples, we consider the quantum stabilizer codes over GF_3 and GF_5 that are based on construction 1b, where the code lengths are 4, 5 and 6. Using the same process as Sec. 3.1, we choose the candidates and then calculate the parameters of quantum stabilizer codes by using the Magma tool's function *QuantumCode*, *MinimumWeight*. Quantum stabilizer codes with large minimum distances are given in the examples.

Example 9. We consider the following parity-check matrix with the size 4×8:

$$\mathbf{H} = \begin{bmatrix} 1,0,0,0 & 2,1,1,1 \\ 0,1,0,0 & 1,0,1,1 \\ 0,0,1,0 & 1,1,2,0 \\ 0,0,0,1 & 1,1,0,2 \end{bmatrix}.$$

This corresponds to the quantum stabilizer code with parameter $[[4, 0, 2]]_3$.

Example 10. We consider the following parity-check matrix with the size 5×10:

$$\mathbf{H} = \begin{bmatrix} 1,0,0,0,0 & 2,1,0,0,2 \\ 0,1,0,0,0 & 1,2,0,2,2 \\ 0,0,1,0,0 & 0,0,1,1,1 \\ 0,0,0,1,0 & 0,2,1,1,0 \\ 0,0,0,0,1 & 2,2,1,0,1 \end{bmatrix}$$

This corresponds to quantum stabilizer code with parameter $[[5, 0, 3]]_3$.

Example 11. We consider the following parity-check matrix with the size 6×12:

$$\mathbf{H} = \begin{bmatrix} 1,0,0,0,0,0 & 4,0,2,1,0,1 \\ 0,1,0,0,0,0 & 0,0,1,0,1,1 \\ 0,0,1,0,0,0 & 2,1,0,0,0,1 \\ 0,0,0,1,0,0 & 1,0,0,3,1,1 \\ 0,0,0,0,1,0 & 0,1,0,1,0,1 \\ 0,0,0,0,0,1 & 1,1,1,1,1,0 \end{bmatrix}.$$

This corresponds to quantum stabilizer code with parameter $[[6,0,4]]_5$.

In the following examples (from Examples 12–15), we consider the quantum stabilizer codes over GF_3 and GF_7 based on construction 2b with code length up to 12. By using the CSS structure, we can determine the parameter of the corresponding quantum stabilizer code via the parameters of two classical codes. Then, we choose the symmetric matrices with large maximum distances to get quantum stabilizer codes with large maximum distances.

Example 12. We consider two classical codes with parity-check matrices and generators matrices as follows: $[4,2,2]_3$ code, where

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,2,0 \\ 0,1,0,2 \end{bmatrix}$$

and $[4,2,2]_3$ code, where

$$\mathbf{G}_2 = \begin{bmatrix} 1,0,1,0 \\ 0,1,0,1 \end{bmatrix}.$$

This corresponds to the quantum stabilizer code with parameter $[[4,0,2]]_3$.

Example 13. We consider two classical codes with parity-check matrices and generators matrices as follows: $[6,3,3]_7$ code where

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,0,0,1,1 \\ 0,1,0,1,2,0 \\ 0,0,1,1,0,3 \end{bmatrix}$$

and $[6,3,3]_7$ code where

$$\mathbf{G}_2 = \begin{bmatrix} 0,6,6,1,0,0 \\ 6,5,0,0,1,0 \\ 6,0,4,0,0,1 \end{bmatrix}.$$

This corresponds to the quantum stabilizer code with parameter $[[6,0,3]]_7$.

Example 14. We consider two classical codes with parity-check matrices and generators matrices as follows: $[8,4,4]_3$ code, where

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,0,0,2,1,1,1 \\ 0,1,0,0,1,0,1,1 \\ 0,0,1,0,1,1,2,0 \\ 0,0,0,1,1,1,0,2 \end{bmatrix}$$

and $[8,4,4]_3$ code, where

$$\mathbf{G}_2 = \begin{bmatrix} 1,2,2,2,1,0,0,0 \\ 2,0,2,2,0,1,0,0 \\ 2,2,1,0,0,0,1,0 \\ 2,2,0,1,0,0,0,1 \end{bmatrix}.$$

This corresponds to the quantum stabilizer code with parameter $[[8,0,4]]_3$.

Example 15. We consider two classical codes with parity-check matrices and generators matrices as follows: $[10,5,4]_3$ code, where

$$\mathbf{H}_1 = \begin{bmatrix} 1,0,0,0,0,2,1,0,0,2 \\ 0,1,0,0,0,1,2,0,2,2 \\ 0,0,1,0,0,0,0,1,1,1 \\ 0,0,0,1,0,0,2,1,1,0 \\ 0,0,0,0,1,2,2,1,0,1 \end{bmatrix}$$

and $[10,5,4]_3$ code, where

$$\mathbf{G_2} = \begin{bmatrix} 1,2,0,0,1,1,0,0,0,0 \\ 2,1,0,1,1,0,1,0,0,0 \\ 0,0,2,2,2,0,0,1,0,0 \\ 0,1,2,2,0,0,0,0,1,0 \\ 1,1,2,0,2,0,0,0,0,1 \end{bmatrix}.$$

This corresponds to the quantum stabilizer code with parameter $[[10,0,4]]_3$. In Table 1, we summarize some quantum binary and nonbinary codes with lengths ranging from 4 to 12 over two proposed constructions. The optimal quantum stabilizer codes are defined as the codes where the parameters equalize the equation

Table 1. Binary and nonbinary quantum stabilizer codes from proposed construction.

Construction	Code length	Code parameters	Note
2a	4	[[4,0,2]]	Optimal quantum stabilizer code
1b	4	$[[4, 0, 2]]_3$	Optimal quantum stabilizer code
2b	4	$[[4, 0, 2]]_3$	Optimal quantum stabilizer code
1a	5	[[5,0,3]]	Optimal quantum stabilizer code
1b	5	$[[5, 0, 3]]_3$	Optimal quantum stabilizer code
1a	6	[[6,0,4]]	Optimal quantum stabilizer code
2a	6	[[6,0,3]]	
1b	6	$[[6, 0, 4]]_5$	Optimal quantum stabilizer code
2b	6	$[[6, 0, 3]]_7$	
1a	7	[[7,0,3]]	Optimal quantum stabilizer code
2a	8	[[8,0,4]]	Optimal quantum stabilizer code
2b	8	$[[8, 0, 4]]_3$	Optimal quantum stabilizer code
2a	10	[[10,0,4]]	Optimal quantum stabilizer code
2b	10	$[[10, 0, 4]]_3$	Optimal quantum stabilizer code
2a	12	[[12,0,4]]	

of the Knill–Laflamme bound; detail discussion in Sec. 2. The proposed construction aims to provide quantum stabilizer codes with the full rank quantum stabilizer group ($[[n, 0, d]]_p$). As was previously discussed, the full rank quantum stabilizer codes can provide a perfect graph state, which has many applications in one-way quantum computers, secure state distribution, secret sharing and quantum algorithm.[34,35]

4. Conclusion

In this paper, we studied the quantum stabilizer code constructions based on the symmetric matrices for binary and nonbinary cases. The quantum stabilizer codes based on the two proposed constructions whose parameters achieved equality of the quantum singleton bound are explained in detail. These optimal quantum stabilizer codes are candidates for use in quantum applications such as quantum cryptography, quantum communication and quantum entanglement based on the graph state.

Acknowledgments

This work was supported by the Research Program through the National Research Foundation of Korea (NRF-2016R1D1A1B03934653, NRF-2019R1A2C1005920).

References

1. R. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).
2. P. W. Shor, in *Proc. 35th Annual Symp. Foundations of Computer Science* (IEEE Computer Society Press, 1994).
3. L. K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
4. D. M. Nguyen and S. Kim, *Int. J. Theor. Phys.* **58**, 2043 (2019).
5. D. M. Nguyen and S. Kim, *Int. J. Theor. Phys.* **58**, 71 (2019).

6. P. W. Shor, *Phys. Rev. A* **52**, 2493 (1995).
7. A. M. Steane, *Phys. Rev. A* **54**, 4741 (1996).
8. D. Gottesman, Stabilizer codes and quantum error correction, Caltech Ph.D. thesis (1997), arXiv:quant-ph/9705052.
9. A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54**, 1098 (1996).
10. M. Grassl and T. Beth, in *Int. Symp. Theoretical Electrical Engineering* (Magdeburg, 1999), pp. 207–212.
11. M. Grassl, W. Geiselmann and T. Beth, in *Proc. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (*AAECC*-13) (Springer, 1999).
12. M. Hagiwara and H. Imai, in *IEEE Int. Symp. Information Theory* (2017).
13. M. Hivadi, *Quantum Inf. Proc.* **17**, 324 (2018).
14. D. Deutsch and R. Jozsa, in *Proc. R. Soc. Lond. A* (1992).
15. K. Nagata *et al.*, *Asian J. Math. Phys.* **2**, 6 (2018).
16. M. Zidan *et al.*, *Appl. Math. Inf. Sci.* **12**, 265 (2018).
17. H. J. Garcia and I. L. Markov, *IEEE Trans. Comput.* **64** (2015).
18. M. Steudtner and S. Wehner, *Phys. Rev. A* **99**, 022308 (2019).
19. M. Epping, H. Kampermann and D. Bruf, *New J. Phys.* **18**, 103052 (2016).
20. X. Gao *et al.*, *Phys. Rev. A* **99**, 023825 (2019).
21. A. Ketkar *et al.*, *IEEE Trans. Inform. Theory* **52**, 4892 (2006).
22. G. Xu *et al.*, *Int. J. Mod. Phys. B* **31** (2017).
23. D. M. Nguyen and S. Kim, *J. Commun. Netw.* **20**, 309 (2018).
24. F. Li and Q. Yue, *Mod. Phys. Lett. B* **29** (2015).
25. D. M. Nguyen and S. Kim, *Symmetry* **10**, 655 (2018).
26. D. M. Nguyen and S. Kim, *Symmetry* **9**, 122 (2017).
27. D. M. Nguyen and S. Kim, in *Proc. Eighth Int. Conf. Ubiquitous and Future Networks* (*ICUFN*) (Austria, 2016).
28. J. Gao and Y. Wang, *IEEE Access* **7**, 26418 (2019).
29. M. Hein *et al.*, in *Proc. Int. School of Physics Enrico Fermi on Quantum Computers, Algorithms and Chaos* (Italy, 2005).
30. I. Djordjevic, *Quantum Information Processing and Quantum Error Correction: An Engineering Approach* (2012).
31. E. Knill and R. Laflamme, *Phys. Rev. A* **55**, 900 (1997).
32. MAGMA. Computer and Algebra calculation tool, http://magma.maths.usyd.edu.au/calc/.
33. S. Y. Looi *et al.*, *Phys. Rev. A* **78**, 042303 (2008).
34. A. Keet *et al.*, *Phys. Rev. A* **82**, 062315 (2010).
35. T.-A. Isdraila, *Sci. Rep.* **9**, 6337 (2019).