symmetry

MDPI

Article

Minimal-Entanglement Entanglement-Assisted Quantum Error Correction Codes from Modified Circulant Matrices

Duc Manh Nguyen and Sunghwan Kim *

School of Electrical Engineering, University of Ulsan, Ulsan 44610, Korea; nguyenmanhduc18@gmail.com
* Correspondence: sungkim@ulsan.ac.kr; Tel.: +82-052-259-1401

Academic Editor: Takeshi Koshiba
Received: 22 May 2017; Accepted: 13 July 2017; Published: 18 July 2017

Abstract: In this paper, new construction methods of entanglement-assisted quantum error correction code (EAQECC) from circulant matrices are proposed. We first construct the matrices from two vectors of constraint size, and determine the isotropic subgroup. Then, we also propose a method for calculation of the entanglement subgroup based on standard forms of binary matrices to satisfy the constraint conditions of EAQECC. With isotropic and entanglement subgroups, we determine all the parameters and the minimum distance of the EAQECC. The proposed EAQECC with small lengths are presented to explain the practicality of this construction of EAQECC. Comparison with some earlier constructions of EAQECC shows that the proposed EAQECC is better.

Keywords: entanglement quantum error correction code; circulant matrices; cyclic matrices; symplectic inner product

1. Introduction

The theory of quantum information is a result of the effort to generalize classical information theory. However, an aspect that is commonly tacitly referred to the background, is the reversible character of the quantum mechanical processes, underlying the computations [1]. An important milestone in quantum computations occurred in 1994 when Shor published computationally efficient quantum algorithms for factoring integers and for evaluating discrete logarithms [2]. With these algorithms, the owner of a quantum computer could crack popular, highly utilized public key cryptosystems. In addition, Grover [3] discovered a quantum algorithm for the important problem of searching an unstructured database, which yields a substantial speed-up over classical search algorithms. 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 [4]. To deal with the problems, the theory of quantum error correction codes was developed to protect quantum states against noise. Discoveries of 9-qubit codes by Shor [5] and 7-qubit codes by Steane [6] showed how data could be protected by containing more redundancy after encoding by quantum systems; these were the first examples of quantum error correction code (QECC). The purpose of QECC 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 [7], have become an important class of QECC, since these codes are useful for building quantum fault-tolerant circuits [8]. 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 from stabilizer operators, rather than from the quantum state itself. In addition, the stabilizer formalism allows us to construct quantum stabilizer codes from binary matrices over binary in the constraint referred to as the symplectic inner product (SIP) [7].

With Calderbank-Shor-Steane (CSS)-based construction [9], the problem turned out to be utilizing self-orthogonal classical codes. However, self-orthogonal codes with high error-correcting capacity are restricted, and therefore, further investigation was required to generate good stabilizer codes. Introduction of entanglement-assisted quantum error correction code (EAQECC) by Brun et al. [10] is one answer to this problem. More precisely, it enables us to construct the quantum error-correction codes not only from self-orthogonal classical codes, but also from arbitrary classical codes with the help of copies of maximally entangled quantum states shared between encoder and decoder. To design efficient EAQECC, however, it is desirable to use the fewest entangled states possible, because the cost to prepare those states is relatively high. Hence, the construction of EAQECC with small amounts of entangled states is a much more attractive issue [10,11]. Therefore, several constructions of EAQECC have been proposed, such as construction from arbitrary matrices where the number of ebits is determined by parameters of classical codes [12], from low-density parity-check (LDPC) codes [11], from generalized quadrangles [13], from circulant permutation matrices [14], and from shortened Hamming codes [15]. Almost all existing constructions consider classical codes to calculate the number of ebits. To do so, the problem of transforming the classical form to basic form of EAQECC was proposed in the Gram–Schmidt procedure. This aims to classify the classical form into isotropic and entanglement subgroups, but the complexity of the Gram–Schmidt procedure also increases in proportion to the length of the codes [16]. Furthermore, the encoding transforms the non-commuting set of generators into its canonical form [17]. Then, quantum circuits composed of *CNOT*, *H*, and *S* gates can be derived directly with complexity $O(n^2)$. The canonical form gives the relationship between EAQECC and quantum stabilizer codes, even though we can use the property of the stabilizer code that is useful for fault-tolerant computation [18].

The key result of this paper is to propose novel approaches to construction of EAQECC. First, we propose a new method for the construction of the isotropic subgroup based on circulant matrices. Then, the entanglement subgroup can be determined from a method of transforming the isotropic group into standard form; hence, the parameters of codes are found, and for effective preparation of the entangled state, the number of ebits should be as few as possible. To explain the practical construction of the quantum codes, design of the proposed EAQECC with lengths up to 12 are shown. In addition, the minimum distance is calculated and explained to show that the proposed construction has good correctable capability, in comparison with recent EAQECC. The organization of this paper is as follows. In Section 2, we review the theory of quantum mechanics, the role of quantum stabilizer codes in quantum error correction, and the constraints on the construction of EAQECC. In Section 3, we propose the construction of two new types of circulant matrices. Following that, we construct the isotropic subgroup, and the calculation for entanglement subgroups is proposed. From the subgroup of isotropic and entanglement, parameters and minimum distances of EAQECC have been determined. Finally, conclusions are presented in Section 4.

2. Background

In this section, we give some preliminary explanations about quantum mechanics, quantum error correction codes, and the entanglement-assisted quantum stabilizer codes used throughout the paper.

2.1. Introduction to Quantum Mechanics

The *bit* is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum *bit*, or *qubit* for short [4]. Then, just as the classical bit has a state (either 0 or 1), the state in a quantum system is instead a vector over the complex number $\boldsymbol{C}$; the state denoted as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be considered to have both values of $|0\rangle$ and $|1\rangle$ at the same time, where the probability of value $|0\rangle$ and $|1\rangle$ are $|\alpha|^2$ and $|\beta|^2$ respectively. This concept, known as superposition, is 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 is infinite. A qubit can be represented in vector form:

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

According to the probability, the condition $|\alpha|^2 + |\beta|^2 = 1$ must be satisfied. A quantum memory register is a physical system composed of n qubits, that is, multiples of the tensor product of some qubits. Generally, the n-qubit state is denoted as:

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

where $i = \sum_{k=1}^{n} 2^{n-k} i_k$. Hence, a state vector of an n-qubit quantum system is considered a superposition of the states that make up a base in a 2^n dimensional complex Hilbert space, $\mathrm{H}^{\otimes n}$.

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. For example, Pauli operators are one of the unitary transformations. The single Pauli operators (matrices) **I**, **X**, **Y**, and **Z** are represented as

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

where $j = \sqrt{-1}$. The Pauli operation acts on the qubit as follows:

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

Thus, the 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.

$$\begin{aligned}
&\mathbf{X}^2 = \mathbf{Y}^2 = \mathbf{Z}^2 = \mathbf{I};\\
&\mathbf{X} \times \mathbf{Y} = j\mathbf{Z}; \mathbf{Y} \times \mathbf{X} = -j\mathbf{Z} \rightarrow \mathbf{X} \times \mathbf{Y} = -\mathbf{Y} \times \mathbf{X};\\
&\mathbf{Y} \times \mathbf{Z} = j\mathbf{X}; \mathbf{Z} \times \mathbf{Y} = -j\mathbf{X} \rightarrow \mathbf{Y} \times \mathbf{Z} = -\mathbf{Z} \times \mathbf{Y};\\
&\mathbf{Z} \times \mathbf{X} = j\mathbf{Y}; \mathbf{X} \times \mathbf{Z} = -j\mathbf{Y} \rightarrow \mathbf{Z} \times \mathbf{X} = -\mathbf{X} \times \mathbf{Z}.
\end{aligned}$$

The single Pauli group P_1 is a group formed by the Pauli operators, which is closed under multiplication. Therefore, the Pauli group consists of all the Pauli matrices, together with the multiplicative factors ± 1, $\pm j$. We have: $P_1 = \pm\{\mathrm{I}, j\mathbf{I}, \mathbf{X}, j\mathbf{X}, \mathbf{Y}, j\mathbf{Y}, \mathbf{Z}, j\mathbf{Z}\}$. 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 anti-commute. For n-qubit Pauli operators $\mathbf{A}, \mathbf{B} \in P_n$, the operator $\circ$ for commutativity is defined as

$$\mathbf{A} \circ \mathbf{B} = \prod_{i=1}^{n} \mathbf{A}_i \bullet \mathbf{B}_i, \text{ where } \mathbf{A}_i \bullet \mathbf{B}_i = \begin{cases} +1, & \text{if } \mathbf{A}_i \times \mathbf{B}_i = \mathbf{B}_i \times \mathbf{A}_i \\ -1, & \text{if } \mathbf{A}_i \times \mathbf{B}_i = -\mathbf{B}_i \times \mathbf{A}_i \end{cases}$$

The 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 described in the next section.

2.2. Standard QECC: Stabilizers Code

Let $H^{\otimes n} = \{|\psi\rangle\}$ be the quantum state space of n qubits. A stabilizer group, $\boldsymbol{S}$, closed under multiplication, is an Abelian subgroup of P_n, such that a non-trivial subspace, $C_{\boldsymbol{S}}$ of $H^{\otimes n}$, is fixed (or stabilized) by $\boldsymbol{S}$. The stabilized $C_{\boldsymbol{S}}$ defines a quantum code space such that

$$C_{\boldsymbol{S}} = \left\{|\psi\rangle \in H^{\otimes n} \,\middle|\, \mathbf{g}|\psi\rangle = |\psi\rangle,\ \forall \mathbf{g} \in \boldsymbol{S}\right\}.$$

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

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

Then, it is enough to check the commutative property of the generators of $C_{\boldsymbol{S}}$: $\mathbf{g} = \{\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_m\}$; every two elements must be commutative to each other. Considering a set of error operators, $\{\} \subset P_n$, 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 anti-commutes with each stabilizer $\boldsymbol{S}_i$. Then, the corrupted state $\mathbf{E}|\psi\rangle$ is diagnosed by elements $\boldsymbol{S}_i$ of the set $\boldsymbol{S}$. The outcome of the diagnostic procedure is a vector, $\{+1, -1\}$, indicating whether $\mathbf{E}$ can be detected or not. The indication for the error detection is expressed as follows:

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

The condition for quantum error correction is that $\mathbf{E}$ is a set of correctable error operators for $C_{\boldsymbol{S}}$ if

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

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

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

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

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

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

Quantum stabilizer codes can be expressed in the binary field, since any given Pauli operator on n qubits can be composed into an $\mathbf{X}$–containing operator and a $\mathbf{Z}$–containing operator, as well as a phase factor, $\{\pm 1, \pm j\}$. This is achieved by mapping $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$ as follows: $\mathbf{I} \to (0,0)$; $\mathbf{X} \to (1,0)$ and $\mathbf{Y} \to (1,1)$; $\mathbf{Z} \to (0,1)$. 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

$$\mathbf{H} = [\mathbf{H_X}|\mathbf{H_Z}]. \tag{1}$$

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 m-th row, $\mathbf{r}_m$, is expressed as $\mathbf{r}_m = [\mathbf{x}_m \mid \mathbf{z}_m]$, where $\mathbf{z}_m$ and $\mathbf{x}_m$ are binary strings for $\mathbf{Z}$ and $\mathbf{X}$, respectively, then the symplectic product of the m_1 row and m_2 row in the parity-check matrix $\mathbf{H}$ in (1) is expressed as

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

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 $\mathbf{X}$ and $\mathbf{Z}$ is even. This condition is also needed to satisfy the commutativity property. In other words, for a binary matrix, size $(n-k) \times 2n$, $\mathbf{H} = [\mathbf{H_X} \mid \mathbf{H_Z}]$, the symplectic product is satisfied for all rows if and only if

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

where $\mathbf{0}_a$ is the $a \times a$ zero matrix. (2) is the SIP condition, which can be used to determine generators of stabilizer codes.

2.3. Entanglement-Assisted Quantum Error Correction Code

An EAQECC is an extension of quantum stabilizer codes with parameter $[[n, k, d_{\min}; c]]$. Like classical coding theory, it also encodes k logical qubits into n physical qubits but with the help of c copies of maximally entangled Bell states. It has been shown that EAQECCs have considerable advantages over standard quantum stabilizer codes from pre-existing entanglement between transmitter and receiver to improve the reliability of transmission. In addition, while quantum stabilizer codes based on CSS can use dual-containing classical linear binary or quaternary code, non-self-orthogonal codes can be transformed into an EAQECCs.

Let a size of a group be the number of elements in the group. If $\boldsymbol{S}$ is the non-Abelian in Pauli group P_n of size m, then there exists a set of generators for $\boldsymbol{S}$ of the form $\{\mathbf{Z}_1, \mathbf{Z}_2, \ldots, \mathbf{Z}_{s+c}, \mathbf{X}_{s+1}, \mathbf{X}_{s+2}, \ldots, \mathbf{X}_{s+c}\}$ (where $s + c = m$) with the following commutation properties:

$$\begin{cases} [\mathbf{Z}_i, \mathbf{Z}_j] = 0 \text{ and } [\mathbf{X}_i, \mathbf{X}_j] = 0 \text{ for all } i, j; \\ [\mathbf{X}_i, \mathbf{Z}_j] = 0 \text{ for all } i \neq j; \\ \{\mathbf{X}_i, \mathbf{Z}_i\} = 0 \text{ for all } i, \end{cases} \tag{3}$$

where $[\mathbf{A}, \mathbf{B}]$ and $\{\mathbf{A}, \mathbf{B}\}$ are a commutator and a anti-commutator of generator $\mathbf{A}$ and $\mathbf{B}$, respectively. The $[\mathbf{A}, \mathbf{B}]$ and $\{\mathbf{A}, \mathbf{B}\}$ of generator $\mathbf{A}$ and $\mathbf{B}$ can be expressed as $\mathbf{A} \times \mathbf{B} - \mathbf{B} \times \mathbf{A}$ and $\mathbf{A} \times \mathbf{B} + \mathbf{B} \times \mathbf{A}$, respectively. Then, the non-Abelian group can be partitioned into:

1. a commuting subgroup, the isotropic group $\boldsymbol{S}_{\mathrm{I}} = \{\mathbf{Z}_{c+1}, \mathbf{Z}_{c+2}, \ldots, \mathbf{Z}_{c+s}\}$.
2. entanglement subgroup pairs $\boldsymbol{S}_{\mathrm{E}} = \{\mathbf{Z}_1, \mathbf{Z}_2, \ldots, \mathbf{Z}_c, \mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_c\}$ with anti-commuting pairs; the anti-commuting pairs $(\mathbf{Z}_i, \mathbf{X}_i)$ being shared between source and receiver.

The Gram–Schmidt procedure to drop the non-Abelian group into the partitions of operators with the above properties (called the isotropic and entanglement subgroup) was introduced and discussed [10]. From the isotropic and entanglement subgroup, EAQECC code C_{EA} are defined as $[[n, k; c]]$ that encodes $k = n - s - c$ qubits into n physical qubits with the help of $s = n - k - c$ ancillas qubits and c ebits shared between the sender and receiver, that can correct any error from the following set of errors, N:

$$N = \left\{ \mathbf{E}_m \;\middle|\; \forall \mathbf{E}_1, \mathbf{E}_2 \;\Rightarrow\; \mathbf{E}_2{}^{\dagger}\mathbf{E}_1 \;\in\; \boldsymbol{S}_{\mathbf{I}} \cup (\mathrm{P}_n \;-\; N(\boldsymbol{S})) \right\}.$$

Code space C_{EA} is a simultaneous eigenspace of the Abelian extension of $\boldsymbol{S}$ [16]. The Abelian extension is Galois extension by using ancilla operators. From N, we can determine $d_{\min}$, and it tells us the detectable and correctable EAQECCs.

From the isotropic and entanglement subgroup, the operation of EAQECC can be considered. For example, the following state shared between A (Alice) and B (Bob) is an entanglement state:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

The first half of the entanglement pair belongs to Alice and the second half to Bob. Then, the operating principle is illustrated in Figure 1 [16]. The Sender A encodes the quantum information state $|\psi\rangle$ with the

help of local ancillary qubits $|0\rangle$ and her half of shared ebits, $|\Phi\rangle$, and then shares the encoded qubits over a noisy quantum channel. The Receiver B performs multi-qubit measurement on all qubits to diagnose the channel error and perform recovery unitary operation R to reserve the action of the channel.

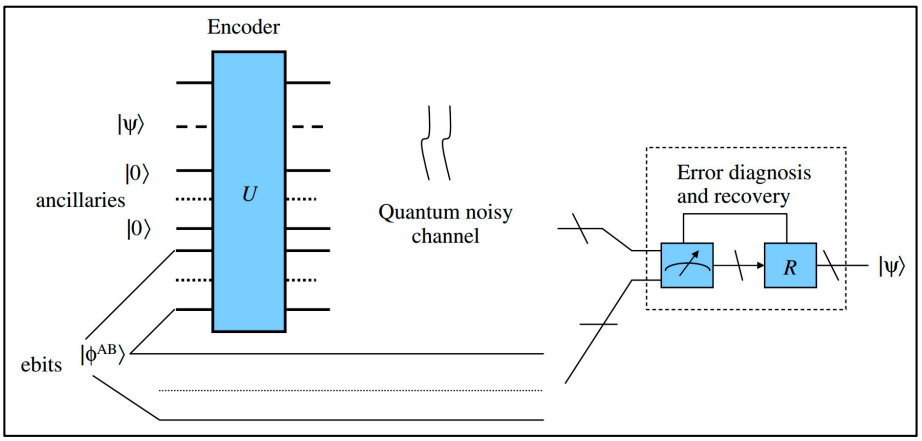

Figure 1. Entanglement-assisted (EA) quantum error correction operating principle.

The most important relationship between EAQECCs and classical codes is given in the following theorem [10,12]:

Theorem 1. *Let C be a binary classical code [n, k, d] with parity check matrix* **H**. *We can obtain a corresponding [[n, 2k − n + c, d; c]]* EAQECC, *where* $c = rank\{\mathbf{H}\mathbf{H}^T\}$ *is the number of ebits needed.*

As a consequence, there are lots of papers using this theorem for EAQECC construction. From binary code C with parameter $[n, k, d]$ and the generator matrix $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{A}_{kx(n-k)}]$, the EAQECC with $[[2n - k, k, d'; c]]$ can be made [12], where $c = 2n - 2k$ and $d' \geq$ d. Tomas [13] used the generalized quadrangle GQ(*s*,1) for the construction of classical binary code and proved the number of ebits is 2. The circulant matrix $\mathbf{P}_m = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}$, and $\mathbf{A}_m{}^{(i)}$ $(i = 0, 1, 2, \ldots, m - 1)$ is an $m \times m$ binary matrix where the $(i + 1)$ row is **1** and other rows are **0**, and defines classical binary codes [14]. Then, the number of ebits is proven to be 1 for some conditions. Qian and Zhang [15] used shortened Hamming codes with parameter $\left[\frac{m(m-1)}{2}, \frac{(m-1)(m-2)}{2}, 3\right]$, and proved EAQECCs with parameter $\left[\left[\frac{m(m-1)}{2}, \frac{(m-1)(m-4)}{2} + 1, 3; 1\right]\right]$ exist if m is even.

3. Construction Method of the Proposed EAQECC

In this section, general properties of cyclic matrices and circulant matrices are introduced first. Then, we discuss the construction of the isotropic subgroup from the proposed modified circulant matrix, and then the calculation for an entanglement group is given. As a consequence, the parameters for EAQECC are obtained.

3.1. Cyclic Matrices

Definition 1. ***(Cyclic Matrix)*** *Let* $\mathbf{I}_n$ *be the* $n \times n$ *identity matrix. A cyclic matrix* $\mathbf{I}_n(x)$ *is a shifted identity matrix with the rows of* $\mathbf{I}_n$ *circularly shifted to the right by x positions, where* $x \in \{0, 1, ..., n - 1\}$ *is the offset.*

In general, it is known that $\mathbf{I}_n(0) = \mathbf{I}_n$ and $\mathbf{I}_n(x \pm kn) = \mathbf{I}_n(x)$ for any integer k. The multiplication of $\mathbf{I}_n(1)$ and $\mathbf{I}_n(1)$ is $\mathbf{I}_n(2)$. Therefore, if $\mathbf{I}_n(1)^c$ is denoted as c times the multiplication of $\mathbf{I}_n(1)$, then $\mathbf{I}_n(1)^c = \mathbf{I}_n(c)$.

Example 1. *For n = 4, the cyclic matrix and relations are given as follows:*

$$\mathbf{I}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \mathbf{I}_4(1) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \text{and } \mathbf{I}_4(1)^2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \mathbf{I}_4(2).$$

Definition 2. *(**Left-cyclic Matrix**) Let $\mathbf{J}_n$ be the $n \times n$ binary matrix made from the π-rotation of identity matrix $\mathbf{I}_n$. A cyclic matrix $\mathbf{J}_n(x)$ is a shifted $\mathbf{J}_n$ with the rows of $\mathbf{J}_n$ circularly shifted to the right by x positions, where $x \in \{0, 1, ..., n-1\}$ is the offset.*

In general, it is known that the transpose matrix of any **Left-**cyclic matrix is equal to itself. Therefore, any **Left-**cyclic matrix is a symmetric matrix.

Example 2. *For n = 4, the following **Left-**cyclic matrix and relations are given:*

$$\mathbf{J}_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \mathbf{J}_4(1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{and } \mathbf{J}_4(1)^T = \mathbf{J}_4(1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

3.2. Circulant Matrices

Definition 3. *(**Circulant Matrix-CM**) An $n \times n$ binary matrix $\mathbf{Q}_1$ is called a CM if it is expressed as*

$$\mathbf{Q}_1 = \begin{bmatrix} i_0 & i_1 & i_2 & \cdots & i_{n-1} \\ i_{n-1} & i_0 & i_1 & \cdots & i_{n-2} \\ i_{n-2} & i_{n-1} & i_0 & \cdots & i_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ i_1 & i_2 & i_3 & \cdots & i_0 \end{bmatrix},$$

where the entries $\{i_0, i_1, \ldots, i_{n-1}\}$ of matrix $\mathbf{Q}_1$ are the binary values.

Circulant matrix $\mathbf{Q}_1$ can be expressed by using a cyclic matrix as follows:

$$\mathbf{Q}_1 = i_0 \times \mathbf{I}_n(0) + i_1 \times \mathbf{I}_n(1) + i_2 \times \mathbf{I}_n(2) + ... + i_{n-1} \times \mathbf{I}_n(n-1) = \begin{bmatrix} \mathbf{u} \times \mathbf{I}_n(0) \\ \mathbf{u} \times \mathbf{I}_n(1) \\ \vdots \\ \mathbf{u} \times \mathbf{I}_n(n-1) \end{bmatrix},$$

where $\mathbf{u} = [i_0\ i_1\ \ldots\ i_{n-1}]$. Therefore, we can denote $\mathbf{Q}_1$ as the function of vector $\mathbf{u}$ and variable n. Hereafter, we denote $\mathbf{Q}_1$ as $\mathbf{P}_1(\mathbf{u}, n)$.

Definition 4. *(**Left-circulant Matrix—Left-CM**) An $n \times n$ binary matrix $\mathbf{Q}_2$ is called a Left-CM if it is expressed as*

$$\mathbf{Q}_2 = \begin{bmatrix} j_0 & j_1 & j_2 & \cdots & j_{n-1} \\ j_1 & j_2 & j_3 & \cdots & j_0 \\ j_2 & j_3 & j_4 & \cdots & j_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ j_{n-1} & j_0 & j_1 & \cdots & j_{n-2} \end{bmatrix},$$

where the entries $\{j_0, j_1, \ldots, j_{n-1}\}$ of matrix $\mathbf{Q}_2$ are the binary values.

Circulant matrix $\mathbf{Q}_2$ can be expressed by using a left-cyclic matrix, such as

$$\mathbf{Q}_2 = j_0 \times \mathbf{J}_n(1) + j_1 \times \mathbf{J}_n(2) + j_2 \times \mathbf{J}_n(3) + ... + j_{n-2} \times \mathbf{J}_n(n-1) + j_{n-1} \times \mathbf{J}_n(0) = \begin{bmatrix} \mathbf{v} \times \mathbf{I}_n(0) \\ \mathbf{v} \times \mathbf{I}_n(n-1) \\ \vdots \\ \mathbf{v} \times \mathbf{I}_n(1) \end{bmatrix},$$

where $\mathbf{v} = [j_0\ j_1\ \ldots\ j_{n\text{-}1}]$. Therefore, we can denote $\mathbf{Q}_2$ as the function of vector $\mathbf{v}$ and variable n. Hereafter, we denote $\mathbf{Q}_2$ as $\mathbf{P}_2(\mathbf{v}, n)$.

3.3. Construction of Parity Check Matrices of EAQECC Based on Modified Circulant Matrices

From the combination of circulant matrices and the left-circulant matrices, the parity check matrix that corresponds to isotropic subgroup have been formed in Theorem 2, then the anti-commuting subgroup are determined as logical operators of the parity check matrix as Theorem 3. Finally, the EAQECCs $[[n, k, d_{\min}; 1]]$ are found as the Corollary 1.

Theorem 2. *For any two binary vectors $\mathbf{u}$, $\mathbf{v}$ of size n, two circulant matrices are $\mathbf{P}_1(\mathbf{u}, n)$ and $\mathbf{P}_2(\mathbf{v}, n)$. Then, the parity-check matrix $\mathbf{H} = [\mathbf{H_X} \mid \mathbf{H_Z}]$, where $\mathbf{H_X}$ and $\mathbf{H_Z}$ correspond to $\mathbf{P}_1(\mathbf{u}, n)$ and $\mathbf{P}_2(\mathbf{v}, n)$, respectively, satisfies the SIP condition in* (2).

Proof. From Definitions 3 and 4, $\mathbf{P}_1(\mathbf{u}, n)$ and $\mathbf{P}_2(\mathbf{v}, n)$ can be written as

$$\mathbf{P}_1(\mathbf{u}, n) = \mathbf{I}_n(i_{\mathbf{u}_1}) + \mathbf{I}_n(i_{\mathbf{u}_2}) + ... + \mathbf{I}_n(i_{\mathbf{u}_k}) \Leftrightarrow \mathbf{H_X} = \mathbf{I}_n(i_{\mathbf{u}_1}) + \mathbf{I}_n(i_{\mathbf{u}_2}) + ... + \mathbf{I}_n(i_{\mathbf{u}_k}),$$

$$\mathbf{P}_2(\mathbf{v}, n) = \mathbf{J}_n(i_{\mathbf{v}_1}) + \mathbf{J}_n(i_{\mathbf{v}_2}) + ... + \mathbf{J}_n(i_{\mathbf{v}_h}) \Leftrightarrow \mathbf{H_Z} = \mathbf{J}_n(i_{\mathbf{v}_1}) + \mathbf{J}_n(i_{\mathbf{v}_2}) + ... + \mathbf{J}_n(i_{\mathbf{v}_h}),$$

where $\{u_1, u_2, \ldots, u_k\}$ and $\{v_1, v_2, \ldots, v_k\}$ are the positions of 1 at vectors $\mathbf{u}$ and $\mathbf{v}$, respectively.

From the properties of circulant matrices, we get following equation for any $0 < m, l \ll n$:

$$\begin{cases} \mathbf{J}_n(m) = \mathbf{J}_n(0) \times \mathbf{I}_n(m), \\ \mathbf{I}_n(l) \times \mathbf{J}_n(0) = \mathbf{J}_n(0) \times \mathbf{I}_n(n-l), \\ \mathbf{I}_n(l)^T = \mathbf{I}_n(n-l). \end{cases}$$

In addition, any left-cyclic matrix is a symmetric matrix. So, the following equation is always true:

$$\mathbf{I}_n(l) \times \mathbf{J}_n(m) = \mathbf{J}_n(m) \times \mathbf{I}_n(l)^T \Leftrightarrow \mathbf{I}_n(l) \times \mathbf{J}_n(m)^T = \mathbf{J}_n(m) \times \mathbf{I}_n(l)^T. \quad (4)$$

From (4), we get:

$$(\mathbf{I}_n(i_{\mathbf{u}_1}) + \mathbf{I}_n(i_{\mathbf{u}_2}) + ... + \mathbf{I}_n(i_{\mathbf{u}_k}))(\mathbf{J}_n(i_{\mathbf{v}_1}) + \mathbf{J}_n(i_{\mathbf{v}_2}) + ... + \mathbf{J}_n(i_{\mathbf{v}_h}))^T = (\mathbf{J}_n(i_{\mathbf{v}_1}) + \mathbf{J}_n(i_{\mathbf{v}_2}) + ... + \mathbf{J}_n(i_{\mathbf{v}_h}))(\mathbf{I}_n(i_{\mathbf{u}_1}) + \mathbf{I}_n(i_{\mathbf{u}_2}) + ... + \mathbf{I}_n(i_{\mathbf{u}_k}))^T.$$

$$\Leftrightarrow \mathbf{H_X} \times \mathbf{H_Z}^T = \mathbf{H_Z} \times \mathbf{H_X}^T \Leftrightarrow \mathbf{H_X} \times \mathbf{H_Z}^T + \mathbf{H_Z} \times \mathbf{H_X}^T = \mathbf{0}_n \text{ modulo } 2.$$

Therefore, the matrix $\mathbf{H} = [\mathbf{H_X} \mid \mathbf{H_Z}]$ satisfies the SIP condition in (2), and Theorem 2 is proven. □

Since the parity-check matrices constructed from Theorem 2 satisfy the SIP condition in (2), we can choose the independent vectors from $\mathbf{H}$ to create corresponding isotropic subgroup S_I. To have the entanglement subgroup, the following theorem can be considered to satisfy the conditions.

Theorem 3. *Given that parity-check matrix* $\mathbf{H}$ *of size* $(n-k) \times 2n$ *and its vectors are an independent relationship, we can transform* $\mathbf{H}$ *into the standard form* $\mathbf{H}_{st}$ *in the following form:*

$$\mathbf{H}_{st} = \begin{bmatrix} \overbrace{\mathbf{I}}^{r} & \overbrace{\mathbf{A}_1}^{n-k-r} & \overbrace{\mathbf{A}_2}^{k} & \overbrace{\mathbf{B}}^{r} & \overbrace{\mathbf{C}_1}^{n-k-r} & \overbrace{\mathbf{C}_2}^{k} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{D} & \mathbf{I} & \mathbf{E} \end{bmatrix} \begin{matrix} \} \ r \\ \} \ n-k-r \end{matrix} \tag{5}$$

Then, the pairs of anti-commuting can be determined as

$$\begin{cases} \mathbf{X}_E = [\ \mathbf{0} & \mathbf{E}^T & \mathbf{I} & (\mathbf{E}^T\mathbf{C}_1 + \mathbf{C}_2{}^T) & \mathbf{0} & \mathbf{0}\ ] \\ \mathbf{Z}_E = [\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{A}_2{}^T & \mathbf{0} & \mathbf{I}\ ] \end{cases} \tag{6}$$

where the rank of matrix $\mathbf{X}_E$ and $\mathbf{Z}_E$ are k.

Proof.

(1) To transform the parity-check matrix to standard form, we use the Gauss-Jordan elimination, swap the qubits, and add one row to another. The codewords and stabilizer are invariant to these changes. So, step by step, the standard form can be obtained with (5).

(2) From the standard form, $\mathbf{H}_{st}$, we calculate the encoded Pauli operators $\overline{\mathbf{X}}$ and $\overline{\mathbf{Z}}$ that satisfy the following conditions:

$$\begin{cases} [\overline{\mathbf{X}_i}, \overline{\mathbf{X}_j}] = 0, \\ [\overline{\mathbf{Z}_i}, \overline{\mathbf{Z}_j}] = 0, \\ [\overline{\mathbf{X}_i}, \overline{\mathbf{Z}_j}] = 0 \text{ for } i \neq j, \\ \{\overline{\mathbf{X}_i}, \overline{\mathbf{Z}_j}\} = 0 \text{ for } i = j. \end{cases}$$

Consequently, encoded Pauli operators $\overline{\mathbf{X}}$ and $\overline{\mathbf{Z}}$ can be used as $\mathbf{X}_E$ and $\mathbf{Z}_E$. Theorem 3 is proven. □

EAQECCs use pre-existing entanglement between transmitter and receiver to improve the reliability of transmission. Hence, before transmission we must manufacture the entanglement state between transmitter and receiver. It will be difficult to set up if the number of ebits becomes larger. So, an EAQECC design to minimize the numbers of ebits is an important constraint. In following Corollary, we will consider the result of the Theorem 2 when the number of ebits is 1.

Corollary 1. *From the Theorem 3, firstly we choose one pair of anti-commuting from* S_E*, it denotes as* $\{X_1, Z_1\}$*. Then, we choose* $n-k-1$ *generators* $\{\mathbf{Z}_2, \mathbf{Z}_3, \ldots, \mathbf{Z}_{n-k}\}$ *from parity check matrix that satisfy the commutation property of isotropic sub-group* S_I*. The minimum distance* d_{min} *is calculated from the generators of* S_E *and* S_I*. The EAQECCs with parameter* $[[n, k, d_{min};1]]$ *is constructed.*

Proof.

As the definition of EAQECC in Section 2.3, the non-Abelian group can be partitioned into:

1. a commuting subgroup, the isotropic group $\boldsymbol{S}_I = \{\mathbf{Z}_{c+1}, \mathbf{Z}_{c+2}, \ldots, \mathbf{Z}_{c+s}\}$.
2. entanglement subgroup pairs $\boldsymbol{S}_E = \{\mathbf{Z}_1, \mathbf{Z}_2, \ldots, \mathbf{Z}_c, \mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_c\}$ with anti-commuting pairs; the anti-commuting pairs $(\mathbf{Z}_i, \mathbf{X}_i)$ being shared between source and receiver.

Then, from the isotropic and entanglement subgroup, EAQECC code C_{EA} are defined as $[[n, k; c]]$ that encodes $k = n - s - c$ qubits into n physical qubits with the help of $s = n - k - c$ ancillas qubits and c ebits shared between the sender and receiver. As the expectation to get the minimum distance, one entanglement pair is chosen, hence $c = 1$, the operators are chosen above, the minimum distance is determined by the minimum weights of operators in the error set N:

$$N = \left\{ \mathbf{E}_m \;\middle|\; \forall \mathbf{E}_1,\ \mathbf{E}_2 \ \Rightarrow \mathbf{E}_2{}^{\dagger}\mathbf{E}_1 \ \in \ \boldsymbol{S}_{\mathbf{I}} \cup (\mathrm{P}_n \ - \ N(\boldsymbol{S})) \right\}.$$

Finally, the parameter of EAQECC $[[n, k, d_{\min};1]]$ are determined and the Corollary is proven. □

Following examples show the outputs of Corollary 1 where the minimum distance $d_{\min} \geq 3$, we search vectors which make codes with various minimum distance. Then, among many candidates of the vectors, to achieve largest minimum distance that has the error correctable ability the number of error $t = \lfloor (d_{\min} - 1)/2 \rfloor \geq 1$ when the length of code up to 12.

Example 3. *For n = 7, let us consider the EAQECC when* **u** *= [1 1 0 0 1 0 1] and* **v** *= [1 0 0 1 0 1 1]. We have a code with the minimum number of ebits and good minimum distance, as in the following explanations.*

Per **Theorem 2**, we have the corresponding parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{7}$$

The six generators are chosen from the first six rows of matrix **H**, which satisfy the independent condition to generate all elements of an inotropic subgroup. By using Gaussian elimination and interchanges of columns, matrix **H** in (7) takes the standard form:

$$\mathbf{H}_{\mathrm{st}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{8}$$

And the corresponding entanglement subgroup pair is calculated as:

$$\begin{aligned} \mathbf{X}_1 &= \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \\ \mathbf{Z}_1 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \end{aligned} \tag{9}$$

Then, from vectors in (8) and (9) we have the generators for EAQECC as follows: $\boldsymbol{S}_{\mathrm{E}} = \{\mathbf{X}_1, \mathbf{Z}_1\}$ and $\boldsymbol{S}_{\mathrm{I}} = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6\}$ where

$$\begin{aligned} \mathbf{Z}_2 &= [1\,1\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,1\,1], \\ \mathbf{Z}_3 &= [1\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,1\,1\,1], \\ \mathbf{Z}_4 &= [0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0], \\ \mathbf{Z}_5 &= [1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0], \\ \mathbf{Z}_6 &= [0\,0\,1\,0\,1\,1\,1\,1\,1\,1\,0\,0\,1\,0]. \end{aligned}$$

The generators $S = <S_I, S_E>$ correspond to EAQECC [[7,1,3;1]] that encodes **one** information qubit into **seven** physical qubits with the help of $s = 6$ ancilla qubits and only one pair entanglement -assisted ebit, and they can correct one error.

Example 4. *For n = 9, let us consider the EAQECC where* $\mathbf{u} = [0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1]$ *and* $\mathbf{v} = [1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0]$*. We have a code with the minimum number of ebits and good minimum distance, as in the following explanations.*

From Theorem 2, we have the corresponding parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1\,0 \\ 1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0 \\ 1\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1 \\ 0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0 \\ 1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0 \\ 1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,0\,1 \end{bmatrix} \tag{10}$$

The eight generators are chosen from the first eight rows of matrix **H,** which satisfies the independent condition to generate all elements of an inotropic subgroup. By using Gaussian elimination and interchange of columns, matrix **H** in (10) takes the standard form:

$$\mathbf{H}_{st} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,1\,1 \\ 0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0\,1 \\ 0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,1\,1\,1\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1 \end{bmatrix} \tag{11}$$

And the corresponding entanglement subgroup pair is calculated as:

$$\begin{aligned} \mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0], \\ \mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1]. \end{aligned} \tag{12}$$

Then, from vectors in (11) and (12), we have the generators for EAQECC as follows: $S_E = \{\mathbf{X}_1, \mathbf{Z}_1\}$ and $S_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8\}$, where

$$\begin{aligned} \mathbf{Z}_2 &= [0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1\,0], \\ \mathbf{Z}_3 &= [1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1], \\ \mathbf{Z}_4 &= [0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,1\,1], \\ \mathbf{Z}_5 &= [0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0], \\ \mathbf{Z}_6 &= [0\,1\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1], \\ \mathbf{Z}_7 &= [0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0], \\ \mathbf{Z}_8 &= [1\,0\,0\,1\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0]. \end{aligned}$$

The generators $S = < S_I, S_E >$ correspond to EAQECC [[9,1,3;1]] that encodes **one** information qubit into **nine** physical qubits with the help of $s = 7$ ancilla qubits and one pair entanglement -assisted ebit, and they can also correct one error.

Example 5. *For n = 10, let us consider the EAQECC when* **u** *= [0 1 1 1 0 1 1 0 1 0] and* **v** *= [1 1 1 0 1 1 0 1 0 0]. We have a code with the minimum number of ebits and good minimum distance as in the following explanations.*

Per Theorem 2, we have the corresponding parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1 \\ 1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1 \\ 0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1 \\ 1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0 \\ 1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1 \\ 0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1 \\ 1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0 \\ 1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1 \end{bmatrix} \tag{13}$$

The nine rows of matrix **H** satisfy the independent condition to generate all elements of an inotropic subgroup. By using Gaussian elimination and interchange of columns, matrix **H** in (13) takes the standard form:

$$\mathbf{H}_{\text{st}} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,0\,1\,0\,0\,1\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,1\,0\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,0\,1\,0\,0\,1 \end{bmatrix} \tag{14}$$

And the corresponding entanglement subgroup pair is calculated as:

$$\begin{aligned} \mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0], \\ \mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1]. \end{aligned} \tag{15}$$

a/ Then, from vectors in (14) and (15) we have the generators for EAQECC as follows: $\mathbf{S}_{\text{E}} = \{\mathbf{X}_1, \mathbf{Z}_1\}$ and $\mathbf{S}_{\text{I}} = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8, \mathbf{Z}_9\}$ where

$$\begin{aligned} \mathbf{Z}_2 &= [0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0], \\ \mathbf{Z}_3 &= [0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1], \\ \mathbf{Z}_4 &= [1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1], \\ \mathbf{Z}_5 &= [0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1], \\ \mathbf{Z}_6 &= [1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0], \\ \mathbf{Z}_7 &= [1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1], \\ \mathbf{Z}_8 &= [0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1], \\ \mathbf{Z}_9 &= [1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0]. \end{aligned}$$

The generators $\mathbf{S} = < \mathbf{S}_{\text{I}}, \mathbf{S}_{\text{E}} >$ correspond to EAQECC [[10,1,3;1]] that encodes **one** information qubit into **10** physical qubits with the help of $s = 8$ ancilla qubits and only one pair entanglement-assisted ebit, and they can correct one error.

b/ When we calculate with $\mathbf{S}_{\text{E}} = \{\mathbf{X}_1, \mathbf{Z}_1\}$ where

$$\begin{aligned} \mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0], \\ \mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1]. \end{aligned}$$

and $S_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8\}$ where

$$\begin{aligned}
\mathbf{Z}_2 &= [0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0], \\
\mathbf{Z}_3 &= [0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1], \\
\mathbf{Z}_4 &= [0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1], \\
\mathbf{Z}_5 &= [1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0], \\
\mathbf{Z}_6 &= [0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1], \\
\mathbf{Z}_7 &= [1\,0\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0], \\
\mathbf{Z}_8 &= [1\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1].
\end{aligned}$$

The generator $S = < S_I, S_E >$ correspond to EAQECC [[10,2,3;1]] that encodes **two** information qubits into **10** physical qubits with the help of $s = 7$ ancilla qubits and only one pair entanglement-assisted ebit, and they can correct one error.

Example 6. *For n = 11, let us consider the EAQECC when* $\mathbf{u}$ *= [1 1 1 0 0 1 1 0 0 0 1], *$\mathbf{v}$* *= [1 1 0 0 1 1 0 0 0 1 1]. We have a code with the minimum number of ebits and good minimum distance as in the following explanations.*

Per Theorem 2, we have the corresponding parity-check matrix:

$$\mathbf{H} = \begin{bmatrix}
1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1 \\
1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1 \\
0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1 \\
0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0 \\
0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0 \\
1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1 \\
1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1 \\
0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0 \\
0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0 \\
1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0
\end{bmatrix} \tag{16}$$

The ten rows of matrix $\mathbf{H}$ satisfy the independent condition to generate all elements of an inotropic subgroup. By using Gaussian elimination and interchange of columns, matrix $\mathbf{H}$ in (16) takes the standard form:

$$\mathbf{H}_{st} = \begin{bmatrix}
1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1 \\
0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1 \\
0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,1\,0\,1\,0\,0 \\
0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1 \\
0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,1 \\
0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1 \\
0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,1\,0\,0\,0\,1\,1\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1\,1\,0\,1\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,1
\end{bmatrix} \tag{17}$$

And the corresponding entanglement subgroup pair is calculated as:

$$\begin{aligned}
\mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0], \\
\mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1].
\end{aligned} \tag{18}$$

a/ Then, from vectors in (14) and (15), we have the generators for EAQECC as follows: $S_E = \{\mathbf{X}_1, \mathbf{Z}_1\}$ and $S_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8, \mathbf{Z}_9, \mathbf{Z}_{10}\}$ where

$$\begin{aligned}
\mathbf{Z}_2 &= [1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1], \\
\mathbf{Z}_3 &= [1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1], \\
\mathbf{Z}_4 &= [0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0], \\
\mathbf{Z}_5 &= [0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0], \\
\mathbf{Z}_6 &= [1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1], \\
\mathbf{Z}_7 &= [1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1], \\
\mathbf{Z}_8 &= [0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0], \\
\mathbf{Z}_9 &= [0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0], \\
\mathbf{Z}_{10} &= [1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0].
\end{aligned}$$

The generators $S = < S_I, S_E >$ correspond to EAQECC [[11,1,4;1]] that encodes **one** information qubit into **11** physical qubits with the help of $s = 9$ ancilla qubits and only one entanglement-assisted ebit, and the minimum distance is four.

b/ When we calculate with $S_E = \{\mathbf{X}_1, \mathbf{Z}_1\}$ where

$$\begin{aligned}
\mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0], \\
\mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1].
\end{aligned}$$

and $S_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8, \mathbf{Z}_9\}$ where

$$\begin{aligned}
\mathbf{Z}_2 &= [1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1], \\
\mathbf{Z}_3 &= [0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0], \\
\mathbf{Z}_4 &= [0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0], \\
\mathbf{Z}_5 &= [1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1], \\
\mathbf{Z}_6 &= [1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1], \\
\mathbf{Z}_7 &= [0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0], \\
\mathbf{Z}_8 &= [0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0], \\
\mathbf{Z}_9 &= [1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0].
\end{aligned}$$

The generator $S = < S_I, S_E >$ correspond to EAQECC [[11,2,3;1]] that encodes **two** information qubits into **11** physical qubits with the help of $s = 8$ ancilla qubits and only one pair entanglement-assisted ebit, and they can correct one error.

c/ When we calculate with $S_E = \{\mathbf{X}_1, \mathbf{Z}_1\}$ where

$$\begin{aligned}
\mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0], \\
\mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1].
\end{aligned}$$

and $S_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8\}$ where

$$\begin{aligned}
\mathbf{Z}_2 &= [1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1], \\
\mathbf{Z}_3 &= [0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0], \\
\mathbf{Z}_4 &= [1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1], \\
\mathbf{Z}_5 &= [1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1], \\
\mathbf{Z}_6 &= [0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0], \\
\mathbf{Z}_7 &= [0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0], \\
\mathbf{Z}_8 &= [1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0].
\end{aligned}$$

The generator $\boldsymbol{S} = <\boldsymbol{S}_I, \boldsymbol{S}_E>$ correspond to EAQECC [[11,3,3;1]] that encodes **three** information qubits into **11** physical qubits with the help of $s = 7$ ancilla qubits and only one pair entanglement-assisted ebit, and they can correct one error.

d/ When we calculate with $\boldsymbol{S}_E = \{\mathbf{X}_1, \mathbf{Z}_1\}$ where

$$\begin{aligned}\mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,0],\\ \mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1].\end{aligned}$$

and $\boldsymbol{S}_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7\}$ where

$$\begin{aligned}\mathbf{Z}_2 &= [1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1],\\ \mathbf{Z}_3 &= [0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0],\\ \mathbf{Z}_4 &= [1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1],\\ \mathbf{Z}_5 &= [1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1],\\ \mathbf{Z}_6 &= [0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0],\\ \mathbf{Z}_7 &= [0\,0\,1\,1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0].\end{aligned}$$

The generator $\boldsymbol{S} = <\boldsymbol{S}_I, \boldsymbol{S}_E>$ correspond to EAQECC [[11,4,3;1]] that encodes **four** information qubits into **11** physical qubits with the help of $s = 6$ ancilla qubits and only one pair entanglement-assisted ebit, and they can correct one error.

Example 7. *For n = 12, let us consider the EAQECC where* $\mathbf{u}$ *= [1 1 1 0 0 1 0 1 0 1 0 1],* $\mathbf{v}$ *= [1 1 0 0 1 0 1 0 1 0 1 1]. We have a code with the minimum number of ebits and good minimum distance, as in the following explanations.*

Per Theorem 2, we have the corresponding parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\\ 1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\\ 0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\\ 1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\\ 0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\\ 1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,1\\ 0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\\ 1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\\ 0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\\ 0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\\ 1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0 \end{bmatrix} \tag{19}$$

The eleven rows of matrix $\mathbf{H}$ satisfy the independent condition to generate all elements of an inotropic subgroup. By using Gaussian elimination and interchange of columns, matrix $\mathbf{H}$ in (19) takes the standard form:

$$\mathbf{H}_{st} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\\ 0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1\,0\\ 0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,0\\ 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,0\,0\\ 0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,0\,1\,1\,1\,1\\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0\\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1\,1\,1\\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1 \end{bmatrix} \tag{20}$$

And the corresponding entanglement subgroup pair is calculated as:

$$\begin{aligned}\mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0],\\ \mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1].\end{aligned} \tag{21}$$

a/ Then, from vectors in (14) and (15) we have the generators for EAQECC as follows: $S_E = \{\mathbf{X}_1, \mathbf{Z}_1\}$ and $S_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8, \mathbf{Z}_9, \mathbf{Z}_{10}, \mathbf{Z}_{11}\}$ where

$$\begin{aligned}\mathbf{Z}_2 &= [1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1],\\ \mathbf{Z}_3 &= [1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1],\\ \mathbf{Z}_4 &= [0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1],\\ \mathbf{Z}_5 &= [1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0],\\ \mathbf{Z}_6 &= [0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0],\\ \mathbf{Z}_7 &= [1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1],\\ \mathbf{Z}_8 &= [0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0],\\ \mathbf{Z}_9 &= [1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1],\\ \mathbf{Z}_{10} &= [0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0],\\ \mathbf{Z}_{11} &= [0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1].\end{aligned}$$

The generators $S = <S_I, S_E>$ correspond to EAQECC [[12,1,4;1]] that encodes **one** information qubit into **12** physical qubits with the help of $s = 10$ ancilla qubits and only one pair entanglement -assisted ebit and the minimum distance is four.

b/ When we calculate with $S_E = \{\mathbf{X}_1, \mathbf{Z}_1\}$ where

$$\begin{aligned}\mathbf{X}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0],\\ \mathbf{Z}_1 &= [0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1].\end{aligned}$$

and $S_I = \{\mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_8, \mathbf{Z}_9, \mathbf{Z}_{10}\}$ where

$$\begin{aligned}\mathbf{Z}_2 &= [1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1],\\ \mathbf{Z}_3 &= [0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1],\\ \mathbf{Z}_4 &= [1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0],\\ \mathbf{Z}_5 &= [0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0],\\ \mathbf{Z}_6 &= [1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1],\\ \mathbf{Z}_7 &= [0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0],\\ \mathbf{Z}_8 &= [1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1],\\ \mathbf{Z}_9 &= [0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0],\\ \mathbf{Z}_{10} &= [0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1].\end{aligned}$$

The generator $S = <S_I, S_E>$ correspond to EAQECC [[12,2,4;1]] that encodes **two** information qubits into **12** physical qubits with the help of $s = 9$ ancilla qubits and only one pair entanglement-assisted ebit, and they can correct one error.

The results of the proposed EAQECC with lengths up to 12 are listed in Table 1. The detailed values of the operators are calculated in Examples 3–7.

In comparison with the results of referenced studies [12–15], the proposed EAQECC shows outperform as a smaller number of ebits and larger minimum distance. As the construction of EAQECC by generalized quadrangles in [13] and circulant matrix in [14], the two main things are clearly to conclude the advances of proposed methods that are code lengths and the classification of generators. Firstly, in [13,14], the code lengths are limited as the conditions to construct the parity check matrix, in contrast the proposed method can find the corresponding EAQECCs for any length. In addition, proposed codes are expressed as the standard form transformation to classify subgroups $\boldsymbol{S_I}$ and $\boldsymbol{S_E}$; hence, the operators of subgroups are clearly determined, instead of knowing the numbers and

operators not being determined, as seen in elsewhere, hence the minimum distance of outputs are not calculated in [13,14], furthermore the determined generators also open the effective way to implement the quantum system in future works. For more details, the comparisons are listed in Table 2.

Table 1. Entanglement-assisted quantum error correction code (EAQECC) [[n, k, d; c]] from proposed method with $c = 1$ and $d \geq 3$.

n	k	d
7	1	3
8	1	3
9	1	3
10	1	3
10	2	3
11	1	4
11	2	3
11	3	3
11	4	3
12	1	4
12	2	4
12	3	3
12	4	3
12	5	3

Table 2. Comparison of this proposed paper to other research.

EAQECC Based on	Number of Ebits	To Classify Subgroups	Minimum Distance
Arbitrary binary linear code [12]	$2n - 2k$	Gram-Schmidt procedure	≥ 3
Generalized quadrangles [13]	2	Gram-Schmidt procedure	Not mentioned
Circulant permutation [14]	1	Gram-Schmidt procedure	Not mentioned
Shortened Hamming code [15]	1	Gram-Schmidt procedure	3
The proposed method	1	Standard form transformation of matrix	3, ≥ 4

4. Conclusions

In this paper, the construction of EAQECC-based on circulant matrices has been studied. Not using the Gram-Schmidt procedure to classify the subgroups of EAQECC, we first propose the construction and calculation for each subgroup. This work aims to reduce the complexity in the classification and determination of ebits. Some EAQECCs with a minimum number of ebits, and the capability to correct errors were showed clearly, with generators of each subgroup. This promises effective codes in comparison with other results.

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

Author Contributions: All authors discussed the contents of the manuscript and contributed to its presentation. Duc Manh Nguyen designed and implemented the proposed scheme, analyzed the simulation data and wrote the paper under the supervision of Sunghwan Kim.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. DeVos, A.; Baerdemacker, S.D. Symmetry groups for the decomposition of reversible computers, quantum computers, and computers in between. *Symmetry* **2011**, *3*, 305–324.
2. Shor, P.W. Algorithms for quantum computation discrete logarithms and factoring. In Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994.
3. Grover, L. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [CrossRef]

4. Gaitan, F. *Quantum Error Correction and Fault Tolerant Quantum Computing*; CRC Press Inc.: Boca Raton, FL, USA, 2007.
5. Shor, P.W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **1995**, *52*, 2493. [CrossRef]
6. Steane, A.M. Error correcting codes in quantum theory. *Phys. Rev. Lett.* **1996**, *77*, 793. [CrossRef] [PubMed]
7. Gottesman, D. Stabilizer Codes and Quantum Error Correction. Ph.D. Thesis, California Institute of Technology, Pasadena, CA, USA, 1997.
8. Gottesman, D. Theory of fault-tolerant quantum computation. *Phys. Rev. A.* **1998**, *57*, 127. [CrossRef]
9. Calderbank, A.R.; Shor, P.W. Good quantum error correcting codes exist. *Phys. Rev. A.* **1996**, *54*, 1098–1105. [CrossRef] [PubMed]
10. Brun, T.A.; Devetak, I.; Hsieh, M.H. Correcting quantum errors with entanglement. *Science* **2006**, *314*, 436. [CrossRef] [PubMed]
11. Hsieh, M.H.; Yen, W.T.; Hsu, L.Y. High performance entanglement-assisted quantum LDPC codes need little entanglement. *IEEE Trans. Inf. Theory* **2011**, *57*, 1761–1769. [CrossRef]
12. Quian, J.; Zhang, L. Entanglement-assisted quantum codes from arbitrary binary linear codes. *Des. Codes Cryptogr.* **2015**, *77*, 193–202. [CrossRef]
13. Thomas, W. Entanglement-assisted quantum error-correcting codes from generalized quadrangles. *Rose-Hulman Undergrad. Math. J.* **2013**, *14*, 2.
14. Wada, M.; Kodaira, K.; Shibuya, T. Entanglement-assisted quantum error-correcting codes based on the circulant permutation matrix. *Int. Symp. Inf. Theory Appl.* **2014**, *26–29*, 158–162.
15. Qian, J.; Zhang, L. Two class of entanglement-assisted quantum codes from shortened hamming codes. In Proceedings of the IEEE International Conference on Signal and Image Processing (ICSIP), Beijing, China, 3–15 August 2016; pp. 347–351.
16. Djordjevic, I. *Quantum Information Processing and Quantum Error Correction: An Engineering Approach*; Academic Press: Oxford, UK, 2012.
17. Yun-Jiang, W. Encoding entanglement-assisted quantum stabilizer codes. *Chin. Phys. B* **2012**, *21*, 2.
18. Shaw, B.; Wilde, M.M.; Oreshkov, O.; Kremsky, I.; Lidar, D.A. Encoding one logical qubit into six physical qubits. *Phys. Rev. A* **2008**, *78*, 012337. [CrossRef]