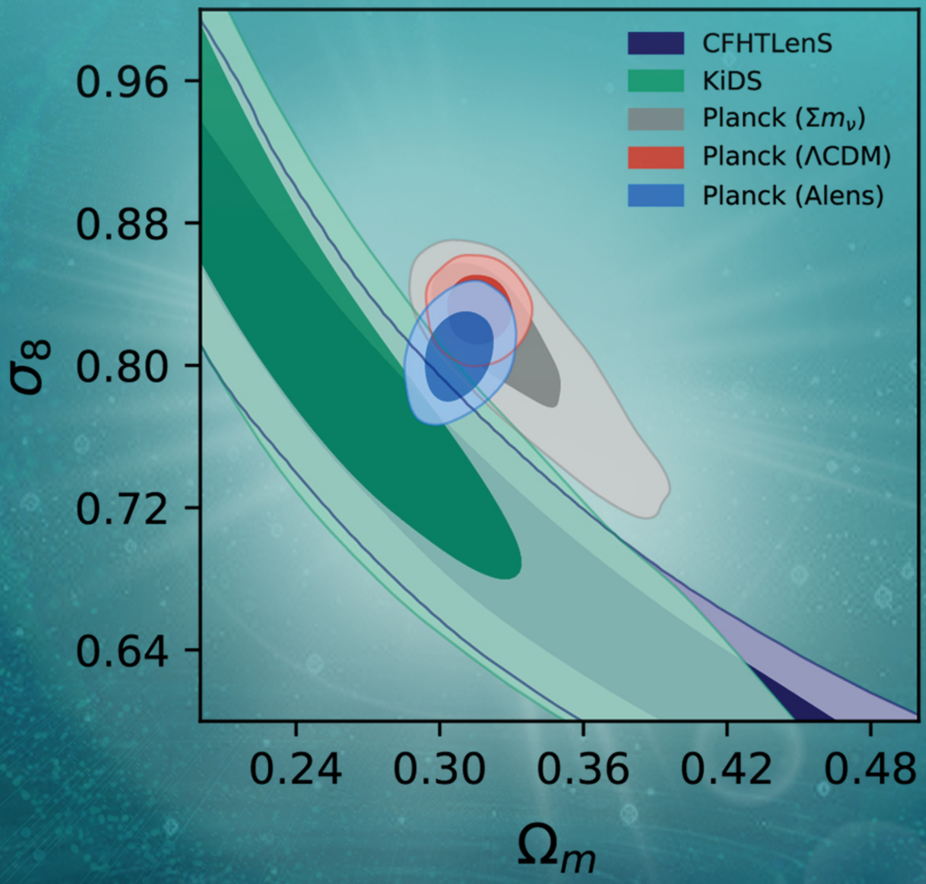
symmetry

IMPACT FACTOR 1.256



Exploring the Tension between Current Cosmic Microwave Background and Cosmic Shear Data

Volume 10 · Issue 11 | November 2018

MDPI

mdpi.com/journal/symmetry
ISSN 2073-8994

symmetry

MDPI

Article

New Constructions of Quantum Stabilizer Codes Based on Difference Sets

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

Received: 19 October 2018; Accepted: 15 November 2018; Published: 19 November 2018

Abstract: In this paper, new conditions on parameters in difference sets are derived to satisfy symplectic inner product, and new constructions of quantum stabilizer codes are proposed from the conditions. The conversion of the difference sets into parity-check matrices is first explained. Then, the proposed code construction is composed of three steps, which are to choose the generators of quantum stabilizer code, to determine the quantum stabilizer groups, and to determine subspace codewords with large minimum distance. The quantum stabilizer codes with various length are also presented to explain the practicality of the code construction. The proposed design can be applied to quantum stabilizer code construction based on combinatorial design.

Keywords: quantum information; quantum error correction codes; quantum stabilizer codes; difference sets; symplectic inner-product

1. Introduction

Quantum theory gives the probability of the possible outcomes for a measurement on a physical system [1]. Quantum computers which are based on quantum theory give us the possibility deal on the various tasks such as factoring the large integer number that shows the substantial speed-up in polynomial time over the best classical algorithm [2,3]. However, the effects of noisy and imperfect environments of the quantum channel would reduce the performance advantages. Therefore, quantum error correcting codes (QECCs) have been proposed to protect quantum information from noisy environments. Since the first QECCs were proposed in the 1990s by Shor [4] and Steane [5], the general theory of QECCs has been introduced [6].

After establishment in 1997 [7], quantum stabilizer codes have played a prominent role in QECCs. A stabilizer code appends ancilla qubits to qubits to be protected. The most consequential advantage of stabilizer code is that the errors can be detected and removed from the stabilizer operators [4]. Hence, stabilizer codes had been constructed to enhance the application of stabilizer formalism in quantum mechanics. In addition, the stabilizer theory allows the transfer of classical binary and quaternary codes to corresponding quantum stabilizer codes. Consequently, the various constructions of quantum stabilizer codes based on classical codes have been proposed [3,5,8,9]. The key idea of development of quantum stabilizer code is that the quantum stabilizer code can be established as a parity-check matrix whose binary or quaternary elements satisfy the constraint of *symplectic inner product* (SIP). Therefore, in [8,9], the authors considered the circulant matrix to construct the parity-check matrix. The modified circulant matrix has been proposed to construct the parity-check matrix and the results for entanglement-assisted quantum error correction codes are explained [8]. In [9], two sub-matrices are proposed to satisfy the constraint of parity-check matrix for quantum stabilizer codes with length seven.

Low-density parity-check (LDPC) codes were first introduced by Gallager [10]. Then, an excellent performance close to Shannon channel capacity was obtained according to large block size of binary parity-check matrix in classical communication [11]. Innovative designs of the parity-check matrix have been proposed for LDPC codes with better performances or with easy implementation. The application of combinatoric design on LDPC codes was proposed to increase the girth of the parity-check matrices [12]. Adaptive selection of quasi-cyclic LDPC (QC-LDPC) codes suitable for visible light communication had been studied to adjust the dimming control [13]. New quantum codes have been proposed based on LDPC codes with the Calderbank-Shor-Steane (CSS) form in [14,15] and quantum LDPC with the non-CSS form in [16,17].

A difference set (DS) in combinatorics [18–20] is defined as a subset in which each difference of two elements occurs in the group. Perfect DSs have been used to build up cyclic codes which have remarkable performance in classical channels. Hence, the new trial using DSs on quantum code was first studied in [21] where DSs are used to construct dual-containing sparse-graph codes for QECCs. Further, one-time DSs were used to construct entanglement-assisted quantum LDPC codes in [22] and these quantum codes have shown a significant improvement in the error probability performance. The quantum QC-LDPC codes based on the DSs in [23], where the set of DSs is easily generated by only a single parameter; however, a lot of the DSs cannot be defined except for prime numbers of the form $n = 4k - 1$, where k is even number.

In this paper, new constructions of quantum stabilizer codes based on DSs are proposed. From the suitable DSs, the circulant matrices are designed and used to construct the parity-check matrix. Then, the generators of the stabilizer should first be chosen to make independent rows of parity-check matrix. Finally, the codeword and minimum distance are determined. Two quantum stabilizer codes with lengths of seven and 15 from the proposed design are shown to express the practical application. The organization of this paper is as follows. In Section 2, we introduce the importance of the stabilizer codes as well as the quantum theory and we explain the binary formalism of quantum stabilizer codes. In Section 3, the definition of difference sets and the circulant matrices are first explained. Then, an innovative approach to DS properties and how to use DSs to build up circulant permutation matrices which satisfy the condition are discussed. Finally, conclusions are listed in Section 4.

2. Quantum Stabilizer Code

2.1. Quantum Information Theory

Qubit is the simplest unit in quantum information and can be expressed as a two-state Hilbert space $\mathbf{H}^{\otimes 2}$ with dimension 2. Therefore, the two basis quantum states can be denoted as $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. The general quantum state of a qubit can be represented by a linear superposition of its two orthogonal basis states as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$. The state can be found at both of basis states $|0\rangle$ and $|1\rangle$ at the same time, where the probability of outcome $|0\rangle$ is $|\alpha|^2$ and the probability of outcome $|1\rangle$ is $|\beta|^2$. According to the norm condition for qubits, the condition $|\alpha|^2 + |\beta|^2 = 1$ must be satisfied. In general, n qubits are represented by 2^{n} dimensional Hilbert space $\mathbf{H}^{\otimes \mathrm{n}}$ 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 $i = \sum_{k=1}^{n} 2^{n-k} i_k$.

In classical computation, Boolean functions f: $\{0, 1\} \to \{0, 1\}$ are performed over a single bit. In the case of quantum computation, reversible operation represented by unitary matrices are performed over a qubit. Representative quantum operations are Pauli operators. Four Pauli operators (matrices) $\mathbf{I}$, $\sigma_{\mathbf{X}}$, $\sigma_{\mathbf{Y}}$, and $\sigma_{\mathbf{Z}}$ are

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

where $j = \sqrt{-1}$. The transformations of quantum states by Pauli operators is as

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

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

Therefore, operators $\sigma_{\mathbf{X}}$, $\sigma_{\mathbf{Z}}$, and $\sigma_{\mathbf{Y}}$ are regarded as a bit flip, a phase flip, and a combination of bit and phase flips, respectively. Multiplications between Pauli operators are defined as

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

The Pauli group P_1 on a qubit is a group composed of Pauli operators and their multiplications with the factor ± 1, $\pm j$. Then, $P_1 = \pm\{\mathbf{I}, \sigma_{\mathbf{X}}, j\sigma_{\mathbf{X}}, \sigma_{\mathbf{Y}}, j\sigma_{\mathbf{Y}}, \sigma_{\mathbf{Z}}, j\sigma_{\mathbf{Z}}\}$. The Pauli group on n qubits P_n is defined as n tensor product of the Pauli operators. Then, the elements of P_n are either commutative or anti-commutative. The commutative operator "$\circ$" for two operators $\mathbf{A}$ and $\mathbf{B}$ is defined as

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

Quotient group P_n/C where C = $\{\pm\mathbf{I}, \pm j\mathbf{I}\}$ is defined as the center of P_n [24]. Therefore, the notation $\mathbf{X} \leftrightarrow \sigma_{\mathbf{X}}$, $\mathbf{Y} \leftrightarrow -j\sigma_{\mathbf{Y}}$, $\mathbf{Z} \leftrightarrow \sigma_{\mathbf{Z}}$ [25] are used in the rest of the paper.

2.2. Quantum Error Correction Code

QECCs are used in quantum computing to protect quantum information from errors due to decoherence and other quantum noises. QECCs are essential to achieve fault-tolerant quantum computation [6]. In classical error correcting code, it is easy to make the copy of information. In contrast, it is impossible to make the copy of quantum information due to the non-cloning theorem [3]. Therefore, quantum information can be extended to highly entangled quantum state with the help of ancillary qubits and Unitary transforms. Classical error correcting codes use a syndrome measurement to diagnose errors which corrupt an encoded state. QECC also employs the syndrome detection with the help of quantum stabilizers operators. A block diagram of the QECC process is shown in Figure 1. The quantum information can be protected from noisy quantum channel with the help of ancillary qubits, the quantum stabilizer operators, and syndrome measurement.

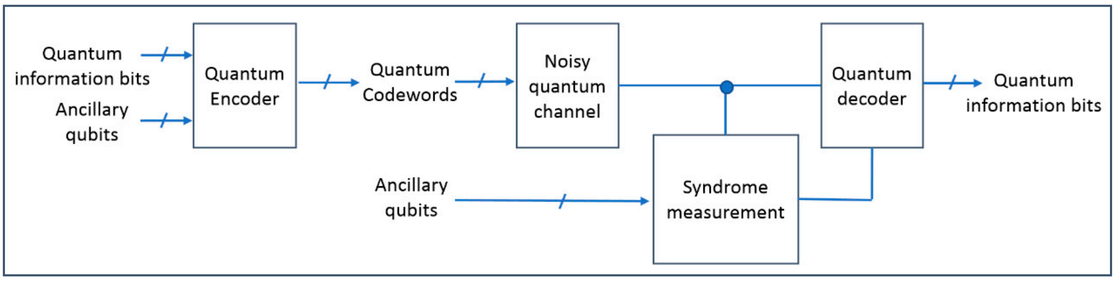


Figure 1. Quantum error correction operating process.

A quantum state $|\psi\rangle$ is stabilized by operator $\mathbf{g} \in P_n$ if $\mathbf{g}|\psi\rangle = |\psi\rangle$. The quantum states, which are stabilized by all elements of any subgroup S of the Pauli group P_n form a subspace C_S of $\mathbf{H}^{\otimes n}$. The subspace C_S is defined as,

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

If C_S is non-trivial subspace, S is an abelian subgroup which is closed under multiplication. The subgroup generated by elements $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_m$ is denoted as $S = \langle \mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_m \rangle$. Then, any two operators on S are commutative. Since $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_m$ are m (=$n-k$) independent Pauli operators, S forms subspace $C\boldsymbol{s}$ to be $[[n, k, d_{\text{min}}]]$ quantum stabilizer code [7] which encodes k logical qubits into n physical qubits and can correct $t = \lfloor (d_{\text{min}} - 1)/2 \rfloor$ errors [6]. For example, the quantum stabilizer code [[5,1,3]] can correct one error and four generators in Table 1 produce the full quantum stabilizer set $\boldsymbol{S}$.

Table 1. Generators of [[5,1,3]] quantum stabilizer code.

Generators	Operators
$\mathbf{g}_1$	**XZZXI**
$\mathbf{g}_2$	**IXZZX**
$\mathbf{g}_3$	**XIXZZ**
$\mathbf{g}_4$	**ZXIXZ**

Let $\{\mathbf{E}\} \subset P_n$ be the error set which makes the state $|\Psi\rangle$ to the corrupted state $\mathbf{E}|\Psi\rangle$. Since elements of Pauli operators are either commutative or anti-commutative, a vector on error set is either commutative or anti-commutative with elements of stabilizer group S. Therefore, the corrupted state $\mathbf{E}|\Psi\rangle$ is identified by the elements of stabilizer group S and the error detection is defined as

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

The operator $\mathbf{E}_\text{i}$ is correctable by stabilizer group S if the following condition is satisfied.

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

where $\mathbf{E}_i{}^{\dagger}$ is the conjugate transpose of $\mathbf{E}_\text{i}$ and $N(\boldsymbol{S})$ is the normalizer of S in P_n. Then, normalizer of S is defined as

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

$N(\boldsymbol{S})$ is the collection of all operators in Pauli group which is commutative with elements in $\boldsymbol{S}$. Therefore, the minimum distance d_{min} is determined as

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

where W($\mathbf{A}$) is defined as the number of positions not equal to Pauli operators $\mathbf{I}$ in $\mathbf{A}$ and min($\mathbf{x}$) is the minimum number in set $\mathbf{x}$.

2.3. Binary Formalism of Quantum Stabilizer Codes

In classical error correcting codes, the parity-check matrices give the constraint that the codewords must have vanishing scalar product with every vector of the parity-check matrices. In quantum error correcting codes, binary expression of quantum stabilizer operators also remains the parity-check constraint to quantum codeword.

Any Pauli operators can be expressed as the product of **X**-containing and **Z**-containing operators such as **XYYZI** = **XXXII** × **IZZZI**. Therefore, a simple but useful mapping exists between elements of Pauli operators and binary vector as **I** → (0, 0), **X** → (1, 0), **Z** → (0, 1), **Y** → (1, 1). Consequently, the $n-k$ generators of an $[[n, k]]$ quantum stabilizer code can be formed by a parity-check matrix $\mathbf{H}$ which is a concatenation of $\mathbf{H_X}$, $\mathbf{H_Z}$ as follows,

$$\mathbf{H} = [\mathbf{H_X}|\mathbf{H_Z}], \quad (1)$$

where $\mathbf{H_X}$, $\mathbf{H_Z}$ are the binary matrices of size $(n-k)\times n$. For example, the quantum stabilizer code [[5,1,3]] in Table 1 has corresponding parity-check matrices as

$$\mathbf{H}=\left[\begin{array}{cc} 10010 & 01100\\ 01001 & 00110\\ 10100 & 00011\\ 01010 & 10001 \end{array}\right]. \tag{2}$$

Since there exists the requirement that quantum stabilizer operators must be commutative, the constraint known as the symplectic inner product (SIP) is applied to **H**. We assume that m-th row of parity-check matric **H**, r_m is expressed as $\mathrm{r}_m = [\mathrm{x}_m \mid \mathrm{z}_m]$, where z_m and x_m are binary strings for **Z** and **X**, respectively. Hence, the symplectic product of the m_1-th row and m_2-th row is given as

$$\mathbf{r}_{m_1}\odot\mathbf{r}_{m_2}=[\mathbf{x}_{m_1}\big|\mathbf{z}_{m_1}]\odot[\mathbf{x}_{m_2}\big|\mathbf{z}_{m_2}]=\mathbf{x}_{m_1}*\mathbf{z}_{m_2}+\mathbf{x}_{m_2}*\mathbf{z}_{m_1}\ \text{modulo2},$$

where $\mathbf{x}_k*\mathbf{z}_l=\sum_{i=1}^{n}x_{ki}\times\mathbf{z}_{li}$. This product will give us zero if the number of different positions in **X** and **Z** are even. Hence, for a given parity-check matrix $\mathbf{H} = [\mathbf{H_X} \mid \mathbf{H_Z}]$ with size $(n-k)\times 2n$, the SIP formulation is defined as

$$\mathbf{H_X}\times\mathbf{H_Z}^T+\mathbf{H_Z}\times\mathbf{H_X}^T=0_{n-k}\,\text{modulo}\,2, \tag{3}$$

where $\mathbf{0}_\mathrm{a}$ is the a $\times$ a zero matrix. The constraint in (3) is called SIP constraint. For quantum stabilizer code [[5,1,3]] in Table 1, the formulation (3) is calculated as

$$\mathbf{H_X}\times\mathbf{H_Z}^T+\mathbf{H_Z}\times\mathbf{H_X}^T=\left[\begin{array}{c} 0\,2\,2\,2\\ 2\,0\,2\,2\\ 2\,2\,0\,2\\ 2\,2\,2\,0 \end{array}\right]=0_4\,\text{modulo}\,2.$$

The parity-check matrix in (1) has the rank $(n-k)$. Hence, the dual space of **H** has the dimension $2n-m$ (=$m+2k$). Then, the normalizer group $N(\mathbf{S})$ can be generated by an $(m+2k)\times 2n$ binary matrix. The first m rows are the parity-check matrix and the last $2k$ row are the logical operators denoted as $\overline{\mathbf{X}}$, $\overline{\mathbf{Z}}$. Logical operators satisfy the conditions as

$$\begin{cases} \overline{\mathbf{X}_i}\circ\overline{\mathbf{X}_j}=+1\\ \overline{\mathbf{Z}_i}\circ\overline{\mathbf{Z}_j}=+1\\ \overline{\mathbf{X}_i}\circ\overline{\mathbf{Z}_j}=+1\,\text{for}\,i\neq j\\ \overline{\mathbf{X}_i}\circ\overline{\mathbf{Z}_j}=-1\,\text{for}\,i=j \end{cases}.$$

Using Gaussian elimination, we can transform the parity check matrix into standard form as

$$\left[\begin{array}{cccccc} \overbrace{\mathbf{I}}^{r} & \overbrace{\mathbf{A}_1}^{n-k-r} & \overbrace{\mathbf{A}_2}^{k} & \overbrace{\mathbf{B}}^{r} & \overbrace{\mathbf{C}_1}^{n-k-r} & \overbrace{\mathbf{C}_2}^{k}\\ 0 & 0 & 0 & \mathbf{D} & \mathbf{I} & \mathbf{E} \end{array}\right]\begin{array}{l} \}\quad r\\ \}\quad n-k-r \end{array} \tag{4}$$

Therefore, logical operators are in standard form as

$$\begin{cases} \overline{\mathbf{X}}=\left[\begin{array}{cccccc} 0 & \mathbf{E}^T & \mathbf{I} & (\mathbf{E}^T\mathbf{C}_1+\mathbf{C}_2{}^T) & 0 & 0 \end{array}\right]\\ \overline{\mathbf{Z}}=\left[\begin{array}{cccccc} 0 & 0 & 0 & \mathbf{A}_2{}^T & 0 & \mathbf{I} \end{array}\right] \end{cases}. \tag{5}$$

Finally, the codewords of the quantum stabilizer code are given as

$$|c_1c_2\dots c_k\rangle = \frac{1}{\sqrt{2^m}} \times \left(\prod_{i=1}^{m}(I+g_i)\right) \times \overline{\mathbf{X}_1}^{c_1} \times \overline{\mathbf{X}_2}^{c_2} \times \dots \times \overline{\mathbf{X}_k}^{c_k}|00\dots0\rangle_n, \tag{6}$$

where $c_i \in \{0,1\}$. For the quantum stabilizer code [[5,1,3]] in Table 1, the standard form of parity-check matrix is investigated as,

$$\mathbf{H} = \left[\begin{array}{c} 1\,0\,0\,0\,1\,1\,1\,0\,1\,1 \\ 0\,1\,0\,0\,1\,0\,0\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1\,0\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1\,1\,1 \end{array}\right].$$

Therefore, its logical operators are in standard form as,

$$\begin{cases} \overline{\mathbf{X}} = & [0\,0\,0\,0\,1\,1\,0\,0\,1\,0] \Leftrightarrow \overline{\mathbf{X}} = \mathbf{ZIIZX} \\ \overline{\mathbf{Z}} = & [0\,0\,0\,0\,0\,1\,1\,1\,1\,1] \Leftrightarrow \overline{\mathbf{Z}} = \mathbf{ZZZZZ} \end{cases}.$$

3. Circulant Matrices Based on DS and QECC Construction

In this section, the definition, properties of DS, and circulant permutation matrices will be first introduced. Then, the QECC construction from circulant matrices based on parameters of DS are discussed with two examples.

3.1. Difference Sets and Shifted Difference Sets

A $(n,\, k, \lambda)$ difference set (DS) $D = \{d_1,\, d_2,\, \dots,\, d_k\}$ is defined as a collection of k residues ($\in \{0,\, 1,\, 2,\, \dots,\, n-1\}$). Then, for any residue $\alpha \neq 0$, the congruence $d_i - d_j = \alpha$ (modulo n) has exactly λ solution pairs (d_i, d_j) with $d_i, d_j \in D$. The necessary condition of the parameters (n, k, λ) is $k(k-1) = \lambda(n-1)$ [18]. Assume that the (n, k, λ) DS $D = \{d_1,\, d_2,\, \dots,\, d_k\}$ is given, then the shifted set $D(s) = \{d_1 + s,\, d_2 + s,\, \dots,\, d_k + s\}$ is also a new DS with the same parameters (n, k, λ). A DS with three elements and its shifted DS are shown in Example 1.

Example 1. *A perfect DS is (7, 3, 1) with D = {1, 2, 4},*

$$\begin{cases} 1-2 \equiv 6 & 2-1 \equiv 1 & 4-1 \equiv 3 \\ 1-4 \equiv 4 & 2-4 \equiv 5 & 4-2 \equiv 2 \end{cases} \text{modulo } 7.$$

The shifted (7, 3, 1) DS with offset 6 is D (6) = {0, 1, 3},

$$\begin{cases} 0-1 \equiv 6 & 1-0 \equiv 1 & 3-0 \equiv 3 \\ 0-3 \equiv 4 & 1-3 \equiv 5 & 3-1 \equiv 2 \end{cases} \text{modulo } 7.$$

The notation $D(s)$ stands for the shifted DS from D with the offset s.

3.2. Circulant Permutation Matrices

Let $\mathbf{I}_n$ be the identity matrix of size $n \times n$. Then, $\mathbf{I}_n(x)$ is the shift of $\mathbf{I}_n$ where the rows of $\mathbf{I}_n$ are circularly shifted to the right by x positions ($0 \le x \le n-1$). Generally, we notice that $\mathbf{I}_n(0) = \mathbf{I}_n$ and $\mathbf{I}_n(x \pm kn) = \mathbf{I}_n(x)$ for any integer k. Let $\mathbf{I}_n(1)^c$ be the c times of multiplying $\mathbf{I}_n(1)$, we have $\mathbf{I}_n(1)^c = \mathbf{I}_n(c)$ ($0 \le c \le n-1$).

Example 2. *With n = 4, we have:*

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

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

A $n \times n$ circulant permutation binary matrix $\mathbf{P}_n$ is defined as

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

where i_k is the binary value. $\mathbf{P}_n$ can be given as the linear combination of identity matrix and its shifted matrices.

$$\mathbf{P}_n = i_0 \times \mathbf{I}_n(0) + i_1 \times \mathbf{I}_n(1) + i_2 \times \mathbf{I}_n(2) + \ldots + i_{n-1} \times \mathbf{I}_n(n-1). \tag{7}$$

It is assumed that $i_0 + i_1 + \ldots + i_{n-1} = k$. Let t_0<$t_1 < \ldots < t_{k-1}$ be the position index of nonzero elements in the sequence set $\{i_0, i_1, \ldots, i_{n-1}\}$. For example, if the sequence set $\{i_0, i_1, \ldots, i_{n-1}\}$ is {1, 1, 0, 0, 1, 0, 1}, then t_0 = 0, t_1 = 1, t_2 = 4, and t_3= 6. The matrix $\mathbf{P}_n$ can also be expressed by using the Hall-polynomial form $p_n(x)$ [18] as

$$p_n(x) = x^{t_0} + x^{t_1} + \ldots + x^{t_{k-1}} \tag{8}$$

Let T be the transpose operator. Then, the transpose matrix of $\mathbf{P}_n$ is denoted as $\mathbf{P}_n{}^T$. Let $p_n(x)^T$ be the Hall-polynomial form of $\mathbf{P}_n{}^T$. Then, the polynomial $p_n(x)^T$ is expressed as

$$p_n(x)^T = x^{-t_0} + x^{-t_1} + \ldots + x^{-t_{k-1}}, \tag{9}$$

where $t_0, t_1, \ldots, t_{k-1}$ are the values in (8). For a (n, k, λ) DS $D = \{d_1, d_2, \ldots, d_k\}$, the circulant permutation matrix $\mathbf{P}_n$ in (7) is made where the element i_j is 1 if $j \in D$ and is 0 otherwise. Then, the Hall-polynomial form $p_n(x)^D$ for the DS D is expressed as

$$p_n(x)^D = x^{d_1} + x^{d_2} + \ldots + x^{d_k} \tag{10}$$

3.3. Construction of Quantum Stabilizer Code Based on DS

With difference sets (n, k, λ) D, the product of the two circulant permutation matrices can be expressed as a function of parameter of DS and the shift values in the following theorem.

Theorem 1. *Let $h_1(x)$ and $h_2(x)$ be the Hall-polynomials of $D(s_1)$ and $D(s_2)$, which are defined as $h_1(x) = p_n{}^{D(s_1)}$ and $h_2(x) = p_n{}^{D(s_2)}$, respectively. Let the circulant permutation matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ correspond to $h_1(x)$ and $h_2(x)$, respectively. Then, the product of the two polynomials $h_1(x)$, $h_2(x)^T$ and the product of the two matrices $\mathbf{H}_1$ and $\mathbf{H}_2{}^T$ are given as*

$$h_1(x)\times h_2(x)^T=(k-\lambda)\times x^{s_1-s_2}+\lambda\times\sum_{l=0}^{n-1}x^l \text{ and } \mathbf{H}_1\times\mathbf{H}_2{}^T=(k-\lambda)\times\mathbf{I}_n(s_1-s_2)+\lambda\times\mathbf{J}_n,$$

where the size of matrix $\mathbf{J}_n$ *is* $n\times n$ and whose entries are all one.

Proof. From the definition of the Hall-polynomial, $h_1(x)$ and $h_2(x)$ can be expressed as

$$h_1(x)=x^{d_1+s_1}+x^{d_2+s_1}+\ldots+x^{d_k+s_1} \text{ and } h_2(x)=x^{d_1+s_2}+x^{d_2+s_2}+\ldots+x^{d_k+s_2}.$$

Then, the Hall-polynomial $h_2(x)^T$ for (9) is given as $h_2(x)^T=x^{-d_1-s_2}+x^{-d_2-s_2}+\ldots+x^{-d_k-s_2}$. Therefore, the product of the two polynomials $h_1(x)$ and $h_2(x)^T$ is given as

$$\begin{aligned}h_1(x)\times h_2(x)^T &= (x^{d_1+s_1}+x^{d_2+s_1}+\ldots+x^{d_k+s_1})\times(x^{-d_1-s_2}+x^{-d_2-s_2}+\ldots+x^{-d_k-s_2})\\ &=\sum_{i=1}^{k}\left[x^{(d_i+s_1)-(d_1+s_2)}+x^{(d_i+s_1)-(d_2+s_2)}+\ldots+x^{(d_i+s_1)-(d_k+s_2)}\right]\\ &=\sum_{i=1}^{k}x^{s_1-s_2}\times\left[x^{d_i-d_1}+x^{d_i-d_2}+\ldots+x^{d_i-d_k}\right]\\ &=x^{s_1-s_2}\times\sum_{u=1}^{k}\sum_{v=1}^{k}x^{d_u-d_v}=x^{s_1-s_2}\times\left[k\times x^0+\sum_{u=1}^{k}\sum_{v=1,v\neq u}^{k}x^{d_u-d_v}\right].\end{aligned}\tag{11}$$

$\sum_{u=1}^{k}\sum_{v=1,v\neq u}^{k}x^{d_u-d_v}$ in (11) can be expressed as

$$\sum_{u=1}^{k}\sum_{v=1,v\neq u}^{k}x^{d_u-d_v}=\lambda\times\sum_{l=1}^{n-1}x^l=\lambda\times\sum_{l=0}^{n-1}x^l-\lambda\times x^0.$$

Hence, Equation (11) is expressed as

$$\begin{aligned}&x^{s_1-s_2}\times\left[k\times x^0+\sum_{u=1}^{k}\sum_{v=1,v\neq u}^{k}x^{d_u-d_v}\right]=x^{s_1-s_2}\times\left[k\times x^0+\lambda\times\sum_{l=0}^{n-1}x^l-\lambda\times x^0\right]\\ &=(k-\lambda)\times x^{s_1-s_2}+\lambda\times x^{s_1-s_2}\times\sum_{l=0}^{n-1}x^l=(k-\lambda)\times x^{s_1-s_2}+\lambda\times\sum_{l=0}^{n-1}x^l.\end{aligned}\tag{12}$$

Since the circulant permutation matrices corresponding to the polynomials $x^{s_1-s_2}$ and $\sum_{l=0}^{n-1}x^l$ are $\mathbf{I}_n(s_1-s_2)$ and $\mathbf{J}_n$, respectively, the product of $\mathbf{H}_1$ and $\mathbf{H}_2{}^T$ is expressed as

$$\mathbf{H}_1\times\mathbf{H}_2{}^T=(k-\lambda)\times\mathbf{I}_n(s_1-s_2)+\lambda\times\mathbf{J}_n\tag{13}$$

Therefore, the expressions in (12) and (13) prove Theorem 1. □

Since the product of $\mathbf{H}_1$ and $\mathbf{H}_2{}^T$ in Theorem 1 is expressed as the function of k, λ, s_1, and s_2, the constraint on parameter of DSs to satisfy the SIP condition of parity-check matrix is explained in the following theorem.

Theorem 2. *For any* (n,k,λ) *DS D where* $k\equiv\lambda$ *modulo 2 and any integers* $s_1\neq s_2$ *where* $s_1,s_2\in\{0,1,\ldots,n-1\}$*, parity-check matrix* $\mathbf{H}=[\mathbf{H}_1|\mathbf{H}_2]$ *where* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *corresponding to* $h_1(x)=p_n{}^{D(s_1)}$ *and* $h_2(x)=p_n{}^{D(s_2)}$*, respectively, satisfies the SIP condition (2).*

Proof. From Theorem 1, we have:

$$\mathbf{H}_1\times\mathbf{H}_2{}^T=(k-\lambda)\times\mathbf{I}_n(s_1-s_2)+\lambda\times\mathbf{J}_n\tag{14}$$

$$\mathbf{H}_2 \times \mathbf{H}_1{}^T = (k-\lambda) \times \mathbf{I}_n(s_2 - s_1) + \lambda \times \mathbf{J}_n \tag{15}$$

The summation of (14) and (15) is

$$\begin{aligned} \mathbf{H}_1 \times \mathbf{H}_2{}^T + \mathbf{H}_2 \times \mathbf{H}_1{}^T &= (k-\lambda) \times \mathbf{I}_n(s_1 - s_2) + \lambda \times \mathbf{J}_n + (k-\lambda) \times \mathbf{I}_n(s_2 - s_1) + \lambda \times \mathbf{J}_n \\ &= (k-\lambda) \times [\mathbf{I}_n(s_1 - s_2) + \mathbf{I}_n(s_2 - s_1)] + 2\lambda \times \mathbf{J}_n. \end{aligned} \tag{16}$$

If $k - \lambda$ is even, all elements of the matrix $(k-\lambda) \times [\mathbf{I}_n(s_1 - s_2) + \mathbf{I}_n(s_2 - s_1)]$ in (16) are even. Moreover, all elements of the matrix $2\lambda \times \mathbf{J}_n$ in (16) are also even. Then, all elements of the matrix $(k-\lambda) \times [\mathbf{I}_n(s_1 - s_2) + \mathbf{I}_n(s_2 - s_1)] + 2\lambda \times \mathbf{J}_n$ in (16) are even. Therefore, if $k \equiv \lambda$ modulo 2, the equation $\mathbf{H}_1 \times \mathbf{H}_2{}^T + \mathbf{H}_2 \times \mathbf{H}_1{}^T = 0_n$ is always true. Therefore, the parity-check matrix $\mathbf{H}$ of $\mathbf{H}_1$ and $\mathbf{H}_2$ which is made from the parameter of DS with the constraint $k \equiv \lambda$ modulo 2 satisfies the SIP condition. □

In Table 2, eight DSs with the constraint $k \equiv \lambda$ modulo 2 are listed among the DSs in [18,19]. For the practical applications of proposed construction, two DSs with parameters (7, 4, 2) and (15, 7, 3) are considered in Examples 3 and 4.

Table 2. Difference sets (DSs) with parameters $k \equiv \lambda$ modulo 2.

No	n, k, λ	Difference Set
1	7, 3, 1	1 2 4.
2	7, 4, 2	0 3 5 6.
3	15, 7, 3	0 1 2 4 5 8 10.
4	21, 5, 1	3 6 7 12 14.
5	23, 11, 5	1 2 3 4 6 8 9 12 13 16 18.
6	31, 15, 7	1 2 3 4 6 8 12 15 16 17 23 24 27 29 30.
7	47, 23, 11	1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27. 28 32 34 36 37 42.

8	199, 99, 49	1 2 4 5 7 8 9 10 13 14 16 18 20 23 25 26 28 29 31 32 33 35 36 40 43 45 46 47 49 50 51 52
		53 56 57 58 61 62 63 64 65 66 70 72 79 80 81 86 89 90 91 92 94 98 100 102 103 104 106
		111 112 114 115 116 117 121 122 123 124 125 126 128 130 131 132 139 140 144 145 151
		155 157 158 160 161 162 165 169 172 175 177 178 180 182 184 187 188 193 196.

Example 3. *For the DS D = {0, 3, 5, 6} with parameter (7, 4, 2), two shifted DSs are considered as D(1) = {0 + 1, 3 + 1, 5 + 1, 6 + 1} = {0, 1, 4, 6}, D(4) = {0 + 4, 3 + 4, 5 + 4, 6 + 4} = {0, 2, 3, 4}. Then, the Hall-polynomials for D(1) and D(4) are* $h_1(x) = p_7{}^{D(1)}$ *and* $h_2(x) = p_7{}^{D(4)}$*, respectively. Therefore, the corresponding binary matrices for the Hall-polynomials are given as*

$$\mathbf{H}_1 = \begin{bmatrix} 1\,1\,0\,0\,1\,0\,1 \\ 1\,1\,1\,0\,0\,1\,0 \\ 0\,1\,1\,1\,0\,0\,1 \\ 1\,0\,1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \\ 1\,0\,0\,1\,0\,1\,1 \end{bmatrix}, \mathbf{H}_2 = \begin{bmatrix} 1\,0\,1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \\ 1\,0\,0\,1\,0\,1\,1 \\ 1\,1\,0\,0\,1\,0\,1 \\ 1\,1\,1\,0\,0\,1\,0 \\ 0\,1\,1\,1\,0\,0\,1 \end{bmatrix}, \mathbf{H} = [\mathbf{H}_1 | \mathbf{H}_2]. \tag{17}$$

It follows that two products $\mathbf{H}_1 \times \mathbf{H}_2{}^T$ *and* $\mathbf{H}_2 \times \mathbf{H}_1{}^T$ *are given by:*

$$\mathbf{H}_1 \times \mathbf{H}_2{}^T = \begin{bmatrix} 2\,2\,2\,2\,4\,2\,2 \\ 2\,2\,2\,2\,2\,4\,2 \\ 2\,2\,2\,2\,2\,2\,4 \\ 4\,2\,2\,2\,2\,2\,2 \\ 2\,4\,2\,2\,2\,2\,2 \\ 2\,2\,4\,2\,2\,2\,2 \\ 2\,2\,2\,4\,2\,2\,2 \end{bmatrix} = (4-2) \times \mathbf{I}_7(1-4) + 2 \times \mathbf{J}_7,\ \mathbf{H}_2 \times \mathbf{H}_1{}^T = \begin{bmatrix} 2\,2\,2\,4\,2\,2\,2 \\ 2\,2\,2\,2\,4\,2\,2 \\ 2\,2\,2\,2\,2\,4\,2 \\ 2\,2\,2\,2\,2\,2\,4 \\ 4\,2\,2\,2\,2\,2\,2 \\ 2\,4\,2\,2\,2\,2\,2 \\ 2\,2\,4\,2\,2\,2\,2 \end{bmatrix} = (4-2) \times \mathbf{I}_7(4-1) + 2 \times \mathbf{J}_7.$$

$$\textit{Then, the SIP product is } \mathbf{H}_1 \times {\mathbf{H}_2}^T + \mathbf{H}_2 \times {\mathbf{H}_1}^T = \begin{bmatrix} 2\ 2\ 2\ 6\ 6\ 2\ 2 \\ 2\ 2\ 2\ 2\ 6\ 6\ 2 \\ 2\ 2\ 2\ 2\ 2\ 6\ 6 \\ 6\ 2\ 2\ 2\ 2\ 2\ 6 \\ 6\ 6\ 2\ 2\ 2\ 2\ 2 \\ 2\ 6\ 6\ 2\ 2\ 2\ 2 \\ 2\ 2\ 6\ 6\ 2\ 2\ 2 \end{bmatrix} = 0_7 \textit{ modulo 2.}$$

The seven quantum stabilizer operators corresponding to the seven rows in **H***(17) are given as*

$$\mathbf{g}_1 = \mathbf{YXZZYIX};\ \mathbf{g}_2 = \mathbf{XYXZZY\ I};\ \mathbf{g}_3 = \mathbf{I\ XYXZZY};$$
$$\mathbf{g}_4 = \mathbf{YIXYXZZ};\ \mathbf{g}_5 = \mathbf{ZYIXYXZ};\ \mathbf{g}_6 = \mathbf{ZZY\ IXYX};\ \mathbf{g}_7 = \mathbf{XZZYIXY}.$$

Among the seven operators, there are a maximum of three linearly independent operators. If $\mathbf{g}_1$, $\mathbf{g}_2$ *and* $\mathbf{g}_3$ *are chosen as the maximum of three linearly independent operators, the other operators are expressed as* $\mathbf{g}_4 = \mathbf{g}_1 \times \mathbf{g}_3$; $\mathbf{g}_5 = \mathbf{g}_1 \times \mathbf{g}_2 \times \mathbf{g}_3$; $\mathbf{g}_6 = \mathbf{g}_1 \times \mathbf{g}_2$; $\mathbf{g}_7 = \mathbf{g}_2 \times \mathbf{g}_3$. *With* $S = \langle \mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3 \rangle$, *a stabilizer subgroup is composed as*

$$S = \{\mathbf{YXZZYIX},\ \mathbf{XYXZZYI}, \mathbf{IXYXZZY}, \mathbf{YIXYXZZ}, \mathbf{ZYIXYXZ}, \mathbf{ZZYIXYX}, \mathbf{XZZYIXY}, \mathbf{I\ I\ I\ I\ I\ I\ I}\}.$$

Using Equation (4), we transform the **H** *matrix in (17) into its standard form as*

$$\begin{bmatrix} 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ \ 1\ 0\ 0\ 1 \\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1 \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \end{bmatrix}.$$

Then, as Equation (5), the logical operators $\overline{\mathbf{X}}$ *and* $\overline{\mathbf{Z}}$ *are calculated as*

$$\overline{\mathbf{X}} = \begin{bmatrix} 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0 \end{bmatrix} \text{and}\, \overline{\mathbf{Z}} = \begin{bmatrix} 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1 \end{bmatrix}$$
$$\Leftrightarrow \begin{cases} \overline{\mathbf{X}_1} = \mathbf{ZI\ IXI\ I\ I} \\ \overline{\mathbf{X}_2} = \ \mathbf{IZI\ IXI\ I} \\ \overline{\mathbf{X}_3} = \mathbf{I\ IZI\ IXI} \\ \overline{\mathbf{X}_4} = \mathbf{ZZI\ I\ I\ IX} \end{cases} \text{and} \begin{cases} \overline{\mathbf{Z}_1} = \mathbf{ZZIZ\ I\ I\ I} \\ \overline{\mathbf{Z}_2} = \mathbf{IZZIZI\ I} \\ \overline{\mathbf{Z}_3} = \mathbf{ZZZIIZI} \\ \overline{\mathbf{Z}_4} = \mathbf{Z\ IZI\ I\ IZ} \end{cases}.$$

The codewords of the quantum stabilizer code [[7,4]] are expressed as

$$\begin{aligned} |c_1c_2c_3c_4\rangle &= \tfrac{1}{\sqrt{2^3}} \times \left(\prod_{i=1}^{3} (I + g_i) \right) \times \overline{\mathbf{X}_1}^{c_1} \times \overline{\mathbf{X}_2}^{c_2} \times \overline{\mathbf{X}_3}^{c_3} \times \overline{\mathbf{X}_4}^{c_4} |0000000\rangle \\ &= \tfrac{1}{\sqrt{2^3}} \times \overline{\mathbf{X}_1}^{c_1} \times \overline{\mathbf{X}_2}^{c_2} \times \overline{\mathbf{X}_3}^{c_3} \times \overline{\mathbf{X}_4}^{c_4} \left(\sum_{s \in S} s|0000000\rangle \right), \end{aligned}$$

where $\prod_{i=1}^{3} (I + g_i) = \sum_{s \in S} s$ and $c_i \in \{0, 1\}$.

The minimum distance d_{min} *of the [[7,4]] code is determined by the smallest weight of N(***S***)\***S***. One of the smallest weights is* $\overline{\mathbf{X}_1} \times \mathbf{IIIIIII}$. *Since W(* $\overline{\mathbf{X}_1} \times \mathbf{IIIIIII}$*) = 2, the minimum distance* d_{min} *is 2. Therefore, the quantum stabilizer code from the DS with parameter (7, 4, 2) is [[7,4,2]].*

Example 4. *A DS D = {0 1 2 4 5 8 10} with parameters (15, 7, 3) is considered to construct a quantum stabilizer code with length 15. The parity-check matrix is given as* $\mathbf{H} = [\mathbf{H}_1\ \mathbf{H}_2]$ *where*

$$\mathbf{H}_1 = \begin{bmatrix} 0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1 \\ 1\,0\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0 \end{bmatrix}, \mathbf{H}_2 = \begin{bmatrix} 0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,1 \\ 1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1 \\ 1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1 \\ 1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0 \end{bmatrix}.$$

Five independent generators can be chosen as

$$\begin{cases} \mathbf{g}_1 = \ \mathbf{IYYX\ IYXZIX\ IXZZZ} \\ \mathbf{g}_2 = \mathbf{Z\ IYYXIYXZIX\ IXZZ} \\ \mathbf{g}_3 = \mathbf{ZZIYYXIYXZIXI\ XZ} \\ \mathbf{g}_4 = \mathbf{ZZZIYYXI\ YXZIXIX} \\ \mathbf{g}_5 = \mathbf{XZZZIYYXIYXZIX\ I} \end{cases}.$$

By using Gaussian elimination, the logical operators $\overline{\mathbf{X}}$ *and* $\overline{\mathbf{Z}}$ *can be written as*

$$\begin{aligned}
\overline{\mathbf{X}_1} &= \mathbf{Z\ I\ \ IZZX\ I\ I\ I\ I\ I\ I\ I\ I\ I}, & \overline{\mathbf{Z}_1} &= \mathbf{Z\ I\ Z\ I\ ZZ\ I\ I\ I\ I\ I\ I\ I\ I\ I} \\
\overline{\mathbf{X}_2} &= \mathbf{ZZZI\ I\ I\ \ X\ I\ I\ I\ I\ I\ I\ I\ I}, & \overline{\mathbf{Z}_2} &= \mathbf{ZZZZZ\ I\ Z\ I\ I\ I\ I\ I\ I\ I\ I} \\
\overline{\mathbf{X}_3} &= \mathbf{I\ ZZZ\ I\ I\ I\ X\ I\ I\ I\ I\ I\ I\ I}, & \overline{\mathbf{Z}_3} &= \mathbf{ZZ\ I\ Z\ I\ I\ I\ Z\ I\ I\ I\ I\ I\ I\ I} \\
\overline{\mathbf{X}_4} &= \mathbf{I\ IZZZ\ I\ I\ \ IX\ I\ I\ I\ I\ I\ I}, & \overline{\mathbf{Z}_4} &= \mathbf{I\ Z\ Z\ IZI\ I\ I\ Z\ I\ I\ I\ I\ I\ I} \\
\overline{\mathbf{X}_5} &= \mathbf{ZIZZ\ I\ \ I\ I\ I\ \ IX\ I\ I\ I\ I\ I}, & \overline{\mathbf{Z}_5} &= \mathbf{Z\ I\ I\ Z\ ZI\ I\ I\ I\ Z\ I\ I\ I\ I\ I} \\
\overline{\mathbf{X}_6} &= \ \mathbf{I\ ZIZZ\ I\ I\ I\ \ I\ IX\ I\ I\ I\ I}, & \overline{\mathbf{Z}_6} &= \mathbf{ZZZ\ I\ \ I\ \ I\ \ I\ I\ I\ I\ Z\ I\ I\ I\ I} \\
\overline{\mathbf{X}_7} &= \mathbf{Z\ I\ I\ I\ \ I\ I\ I\ I\ I\ \ I\ \ IX\ I\ I\ I}, & \overline{\mathbf{Z}_7} &= \ \mathbf{I\ ZZ\ Z\ I\ \ I\ I\ I\ I\ I\ I\ Z\ I\ I\ I} \\
\overline{\mathbf{X}_8} &= \ \ \mathbf{I\ ZI\ I\ \ I\ \ I\ I\ I\ I\ \ I\ I\ I\ XI\ I}, & \overline{\mathbf{Z}_8} &= \mathbf{I\ \ I\ Z\ ZZ\ I\ I\ I\ I\ I\ I\ I\ \ Z\ I\ I} \\
\overline{\mathbf{X}_9} &= \ \ \mathbf{I\ IZ\ I\ I\ \ I\ I\ I\ I\ I\ \ I\ I\ \ IX\ I}, & \overline{\mathbf{Z}_9} &= \mathbf{Z\ I\ Z\ Z\ I\ I\ I\ I\ I\ I\ I\ I\ I\ Z\ I} \\
\overline{\mathbf{X}_{10}} &= \mathbf{I\ I\ I\ Z\ I\ I\ I\ I\ I\ I\ \ I\ I\ I\ I\ X}, & \overline{\mathbf{Z}_{10}} &= \mathbf{IZ\ I\ Z\ Z\ I\ I\ I\ I\ I\ I\ I\ I\ I\ Z}
\end{aligned}$$

Therefore, the codewords for the [[15,10,2]] stabilizer code can be expressed as

$$\begin{aligned}
|c_1c_2\ldots c_{10}\rangle_L &= \frac{1}{\sqrt{2^5}} \times \left(\prod_{i=1}^{5}(I+g_i)\right) \times \overline{\mathbf{X}_1}^{c_1} \times \overline{\mathbf{X}_2}^{c_2} \times \ldots \times \overline{\mathbf{X}_{10}}^{c_{10}} |0_1 0_2 \ldots 0_{15}\rangle \\
&= \frac{1}{\sqrt{2^5}} \times \overline{\mathbf{X}_1}^{c_1} \times \overline{\mathbf{X}_2}^{c_2} \times \ldots \times \overline{\mathbf{X}_{10}}^{c_{10}} \left(\sum_{s\in S} s|0_1 0_2 \ldots 0_{15}\rangle\right).
\end{aligned}$$

As shown in Table 3, the parameter constraints for difference sets in proposed construction are different from the ones in [23]. Since $2p - 1 \equiv p - 1$ modulo 2 where p is an even number, DSs which are used in [23] can be also used in the proposed construction. In contrast, DSs in the proposed construction are not always used in [23] because $4p - 1$ must be a prime number. As a result, the proposed construction is more general than [23]'s construction and the proposed construction enlarges the results of using DSs for quantum stabilizer code construction. In addition, in comparison to the proposed codes with existing quantum codes, quantum codes with length 7 and 15 are discussed. It is known that existing quantum stabilizer codes with length 7 have code parameters [[7,3,2]] from quadratic residue sets in [26], or [[7,3,2]] and [[7,4,2]] constructed over the quaternary alphabet, listed in [27]. To compare to the proposed codes and codes in [26], the number of information bits of the proposed codes is 1 bit larger than the referenced code. As referenced in the list in [27], a stabilizer with length 15 and the same parameters of [[15,10,2]] that were constructed over quaternary alphabet are found.

Table 3. Comparison of our proposed method and [23]'s method.

Paper [23]'s Construction	Proposed Construction
Focus on the difference set with parameters: $(n, k, \lambda) = (4p - 1, 2p - 1, p - 1)$ where p is even number and $4p - 1$ is a prime number.	Focus on the difference set with parameters: (n, k, λ) where $k \equiv \lambda$(modulo 2)

4. Conclusions

In this paper, the conditions of a DS are examined to satisfy the SIP condition and a new construction method of quantum stabilizer codes from the DS is proposed. The condition of a DS to satisfy the SIP constraint is equivalent to determine a DS with $k \equiv \lambda$ modulo 2. Quantum stabilizer codes [[7,4,2]] and [[15,10,2]] are presented from the proposed construction with DS (7, 4, 2) and DS (15, 7, 3), respectively, for practical applications. Moreover, since there are many DSs with parameters that satisfy $k \equiv \lambda$ modulo 2, it is possible to produce new quantum stabilizer codes with greater length. In comparison with the referenced construction, the proposed construction provides more candidates for the quantum stabilizer code based on DSs.

Author Contributions: All authors discussed the contents of the manuscript and contributed to its presentation. D.M.N. designed and implemented the proposed scheme, analyzed the simulation data and wrote the paper under the supervision of S.K.

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

Acknowledgments: The authors are extremely thankful for the reviewers' comments and suggestions for improving this article.

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

References

1. Goyal, P.; Knuth, K.H. Quantum Theory and Probability Theory: Their Relationship and Origin in Symmetry. *Symmetry* **2011**, *3*, 171–206. [CrossRef]
2. Shor, P.W. Algorithms for quantum computation discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
3. Nguyen, D.M.; Kim, S. Quantum Key Distribution Protocol Based on Modified Generalization of Deutsch-Jozsa Algorithm in *d*-level Quantum System. *Int. J. Theor. Phys.* **2018**. [CrossRef]
4. Shor, P.W. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A* **1995**, *52*, 2493–2496. [CrossRef]
5. Steane, A.M. Error correcting codes in quantum theory. *Phys. Rev. Lett.* **1996**, *77*, 793–797. [CrossRef] [PubMed]
6. Calderbank, A.R.; Shor, P.W. Good quantum error-correcting codes exist. *Phys. Rev. A* **1996**, *54*, 1098–1105. [CrossRef] [PubMed]
7. Gottesman, D. Stabilizer Codes and Quantum Error Correction. Ph.D. Thesis, California Institute of Technology, Pasadena, CA, USA, 1997.
8. Nguyen, D.M.; Kim, S. Minimal-Entanglement Entanglement-Assisted Quantum Error Correction Codes from Modified Circulant Matrices. *Symmetry* **2017**, *9*, 122. [CrossRef]
9. Nguyen, D.M.; Kim, S. Construction and complement circuit of a quantum stabilizer code with length 7. In Proceedings of the Eighth International Conference on Ubiquitous and Future Networks, Vienna, Austria, 5–8 July 2016. [CrossRef]
10. Gallager, R.G. Low density parity check codes. *IRE Trans. Inf. Theory* **1962**, *8*, 21–28. [CrossRef]
11. Chung, S.Y.; Forney, G.D.; Richardson, T.J.; Urbanke, R. On the design of low-density parity check codes within 0.045 db of the shannon limit. *IEEE Comm. Lett.* **2001**, *45*, 58–60. [CrossRef]
12. Kim, S.; No, J.S.; Chung, H.; Shin, D.J. Quasi-cyclic low-density parity-check codes with girth larger than 12. *IEEE Trans. Inf. Theory* **2007**, *53*, 2885–2891.

13. Kim, S. Adaptive FEC codes suitable for variable dimming values in visible light communication. *IEEE Photonics Technol. Lett.* **2015**, *27*, 967–969.
14. Postol, M.S. A proposed quantum low density parity check code. *arXiv*, 2001; arXiv:quant-ph/010813.
15. Hagiwara, M.; Imai, H. Quantum quasi-cyclic LDPC codes. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Nice, France, 24–29 June 2007.
16. Hwang, Y.; Chung, Y.; Jeon, M. A class of quantum low-density parity check codes by combining seed graphs. *Quantum Inf. Process.* **2013**, *12*, 2219–2239. [CrossRef]
17. Tan, P.; Li, J. Efficient quantum stabilizer codes: LDPC and LDPC convolutional constructions. *IEEE Trans. Inf. Theory* **2010**, *56*, 476–491. [CrossRef]
18. Baumert, L.D. *Cyclic Difference Sets*; Springer: New York, NY, USA, 1971.
19. Anderson, I. *Combinatorial Designs: Construction Methods*; Ellis Horwood Limited: New York, NY, USA, 1990.
20. Beth, T.; Jungnickel, D.; Lenz, H. *Design Theory*; Cambridge University Press: New York, NY, USA, 1986.
21. MacKay, D.; Mitchison, G.; McFadden, P. Sparse-graph codes for quantum error correction. *IEEE Trans. Inf. Theory* **2004**, *50*, 2315–2330. [CrossRef]
22. Liu, Y.; Wang, Y.; Zhao, S.; Zheng, B. A construction of entanglement-assisted quantum LDPC codes from the cyclic difference set. In Proceedings of the IEEE 11th International Conference on Signal Processing (ICSP), Beijing, China, 21–25 October 2012.
23. Xie, Y.; Yuan, J.; Malaney, R. Quantum stabilizer codes from difference sets. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Istanbul, Turkey, 7–12 July 2013.
24. Vos, A.D.; Baerdemacker, S.D. Symmetry Groups for the Decomposition of Reversible Computers, Quantum Computers, and Computers in between. *Symmetry* **2011**, *3*, 305–324. [CrossRef]
25. Nguyen, D.M.; Kim, S. Quantum Stabilizer Codes Construction from Hermitian Self-Orthogonal Codes over GF (4). *J. Commun. Netw.* **2018**, *20*, 209–315. [CrossRef]
26. Xie, Y.; Yuan, J.; Sun, T.Q. On design of quantum stabilizer codes from quadratic residues sets. *IEEE Trans. Inf. Theory* **2014**, *66*, 3721–3735.
27. Grassl, M. Bounds on the Minimum Distance of Linear Codes and Quantum Codes. Available online: http://codetables.de/ (accessed on 7 November 2018).