Hindawi Publishing Corporation
Advances in Mathematical Physics
Volume 2010, Article ID 469124, 12 pages
doi:10.1155/2010/469124

Research Article

Fast Constructions of Quantum Codes Based on Residues Pauli Block Matrices

Ying Guo, Guihu Zeng, and MoonHo Lee

Institute of Information and Communication, Chonbuk National University, Chonju 561-756, South Korea

Correspondence should be addressed to MoonHo Lee, moonho@chonbuk.ac.kr

Received 21 July 2009; Accepted 20 December 2009

Academic Editor: Debashish Goswami

We demonstrate how to fast construct quantum error-correction codes based on quadratic residues Pauli block transforms. The present quantum codes have an advantage of being fast designed from Abelian groups on the basis of Pauli block matrices that can be yielded from quadratic residues with much efficiency.

1. Introduction

The applications of the Legendre symbol have been already suggested in signal processing, communication, image compression, cryptography, and so forth [1, 2].

Provided a finite field $GF(q)$, Euler's criterion $\mathcal{L}_q(x)$ for the Legendre symbol is defined by

$$\mathcal{L}_q(x) = x^{(q-1)/2} \mod q, \tag{1.1}$$

where q is a power of an odd prime number. Namely, $\mathcal{L}_q(0) = 0$, $\mathcal{L}_q(x) = 1$ if $x = y^2$ for some element $y \in GF(q)$, and $\mathcal{L}_q(x) = -1$ if $x \neq y^2$ for any element in $GF(q)$. Based on quadratic residues in $GF(q)$, one defines a matrix

$$Q_q = \left(a_{ij}\right)_{q\times q}, \tag{1.2}$$

with the elements $a_{ij} = \mathcal{L}_q(i-j)$.

Lemma 1.1. *Taking any two rows of Q_q, that is, $\overrightarrow{a}_i = (\mathcal{L}_q(x_0), \mathcal{L}_q(x_1), \ldots, \mathcal{L}_q(x_{q-1}))$and $\overrightarrow{a}_{i+s} = (\mathcal{L}_q(x_0 + s), \mathcal{L}_q(x_1 + s), \ldots, \mathcal{L}_q(x_{q-1} + s))$ for $s \neq 0$, it follows*

$$\overrightarrow{a}_i \cdot \overrightarrow{a}_{i+s} = \sum_{i=0}^{q-1} \mathcal{L}_q(x_i)\mathcal{L}_q(x_i + s) = q - 1 \mod q. \tag{1.3}$$

Currently, the striking development in quantum error-correction codes (QECCs) is the employment of the stabilizer formalism, whereby code words are subspaces in Hilbert space specified by Abelian groups. The problem of constructing QECCs was reduced to that of searching for the classical dual-containing (or self-orthogonal) codes [3–8]. The virtue of this approach is that QECCs can be directly constructed from classical codes with a certain property, rather than developing a completely new coding theory of QECCs from scratch. Unfortunately, the need for dual-containing codes presents a substantial obstacle to the quantum coding theory in its entirety, especially in the context of modern codes, such as low-density parity-check quantum codes [7]. To resolve this problem, we consider the construction of QECCs over the finite field $GF(q)$ by employing the matrix Q_n in (1.2). Namely, we first replace all entries of Q_n with Pauli matrices and obtain the Pauli block matrix $\mathcal{Q}_n$. After that, we extend this kind of block matrices for the large-size Pauli block matrices by using the recursive techniques with the fast matrix block transforms [9–12]. Since all row operations that are obtained from rows of $\mathcal{Q}_n$ are independent and commutative, an Abelian group can be generated elegantly. Therefore, a type of quantum code is generated structurally via the stabilizer formalism. This approach provides the great flexibility in designing quantum codes with large code length and hence allows for an advantage of being simply constructed with the low complexity.

This paper is organized as follows. In Section 2, three kinds of Pauli block matrices are constructed. In Section 3, according to the properties of Pauli block matrices, Abelian groups can be generated with efficiency. In Section 4, we investigate constructions of quantum codes based on the stabilizer formalism. Finally, conclusions are drawn in Section 5.

2. Pauli Block Matrices

Pauli matrices have been widely applied in signal processing [11], quantum information and quantum computing [3, 13], and so forth. In this section, we investigate constructions of several types of Pauli block matrices according to the structure of Hadamard transforms based on these Pauli matrices.

2.1. Pauli Matrices

Pauli matrices are defined by $\mathcal{P} = \{\sigma_j : 0 \leq j \leq 3\}$, where

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.1}$$

where $i = \sqrt{-1}$. For simplicity, we denote the 2×2 identity matrix σ_0 by a block matrix $\mathcal{I}$ throughout this paper.

Pauli matrices in $\mathcal{P}$ have the following basic properties:

$$\begin{gathered}\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \mathcal{I}, \\ \sigma_1\sigma_2 = i\sigma_3, \qquad \sigma_2\sigma_3 = i\sigma_1, \qquad \sigma_3\sigma_1 = i\sigma_2.\end{gathered} \tag{2.2}$$

2.2. Pauli Block Matrice

Definition 2.1. Denote $Q = ([a]_{ij})_{k\times t}$, then Q is a Pauli block matrix if and only if all entries $[a]_{ij}$ belong to $\mathcal{P}$, that is, $[a]_{ij} \in \mathcal{P}$.

Based on the matrix Q_q in (1.2), we propose several approaches for constructions of Pauli block matrices for any two entries $\sigma_i, \sigma_j \in \mathcal{P} \setminus \{\sigma_0\}$.

Construction 2.1

Taking a matrix Q_q in (1.2), it follows two kinds of Pauli block matrices:

(1) $Q_q^{(1)}$, which is constructed by replacing "0, 1" in Q_q with σ_i and "−1" with σ_j,

(2) $Q_q^{(2)}$, which is constructed by replacing "1" in Q_q with σ_i and "−1, 0" with σ_j.

Specially, one achieves two types of Pauli block matrices.

Construction 2.2

If $q = 4m + 3$ for any positive integer m, then the $(q+1) \times (q+1)$ matrix can be constructed as

$$Q_{q+1} = I + \begin{pmatrix} 0 & t^T \\ -t & Q_q \end{pmatrix}, \tag{2.3}$$

where t denotes the all-1 column vector of the length q and I is the $(q+1) \times (q+1)$ identity matrix. As a result, there are two types of Pauli block matrices:

(1) $Q_{q+1}^{(1)}$, which is constructed by replacing "0, 1" in Q_{q+1} with σ_i and "−1" with σ_j,

(2) $Q_{q+1}^{(2)}$, which is constructed by replacing "1" in Q_{q+1} with σ_i and "−1, 0" with σ_j.

Construction 2.3

If $q = 4m + 1$ for any positive integer m, then one constructs the $2(q+1) \times 2(q+1)$ matrix $Q_{2(q+1)}$ by replacing "0" in the matrix

$$\begin{pmatrix} 0 & t^T \\ t & Q_q \end{pmatrix} \tag{2.4}$$

with the block matrix $[R_0]$ and "±1" with the matrix $[R_{\pm 1}]$, where

$$[R_0] = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \qquad [R_{\pm 1}] = \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.5}$$

Then, there are two Pauli block matrices:

(1) $Q^{(1)}_{2(q+1)}$, which is constructed by replacing "0, 1" in $Q_{2(q+1)}$ with σ_i and "−1" with σ_j,

(2) $Q^{(2)}_{2(q+1)}$, which is constructed by replacing "1" in $Q_{2(q+1)}$ with σ_i and "−1, 0" with σ_j.

2.3. Fast Constructions of Pauli Block Matrices

To construct the large-order Pauli block matrices, we first introduce the Kronecker product of two matrices $A = (a_{ij})_{r\times l}$ and $B = (b_{ij})_{s\times t}$, that is,

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1l}B \\ a_{21}B & a_{22}B & \cdots & a_{2l}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1}B & a_{r2}B & \cdots & a_{rl}B \end{pmatrix}. \tag{2.6}$$

With a little abuse, we denote the Kronecker product by using the notation "⊗" throughout this paper.

Making use of the Kronecker product of Pauli block matrices [9–12], a family of Pauli block matrices may be extended.

Theorem 2.2. *Suppose that Q_q and Q_p are two Pauli block matrices. For any nonnegative integer numbers s and m, a large-order block Jacket matrix $Q_{q^s p^m}$ may be constructed (or decomposed) in the following way:*

$$\begin{aligned} Q_{q^s p^m} &= \left\{ \mathcal{I}_{q^s} \otimes \left(\prod_{i=0}^{m-1} \mathcal{I}_{p^{m-i-1}} \otimes Q_p \otimes \mathcal{I}_{p^i} \right) \right\} \times \left\{ \left(\prod_{i=0}^{s-1} \mathcal{I}_{q^{s-i-1}} \otimes Q_q \otimes \mathcal{I}_{q^i} \right) \otimes \mathcal{I}_{p^m} \right\} \\ &= \left\{ \mathcal{I}_{q^s} \otimes \left(\prod_{i=1}^{m} \mathcal{I}_{p^{m-i}} \otimes Q_p \otimes \mathcal{I}_{p^{i-1}} \right) \right\} \times \left\{ \left(\prod_{i=1}^{s} \mathcal{I}_{q^{s-i}} \otimes Q_q \otimes \mathcal{I}_{q^{i-1}} \right) \otimes \mathcal{I}_{p^m} \right\}. \end{aligned} \tag{2.7}$$

Proof. Based on an arbitrary Pauli block matrix Q_r, the large-order Pauli block matrices Q_{r^l} for $l \geq 2$ can be obtained by using the recursive relations:

$$Q_{r^l} = Q_{r^{l-1}} \otimes Q_r = \prod_{i=0}^{l-1} \mathcal{I}_{r^{l-i-1}} \otimes Q_r \otimes \mathcal{I}_{r^i} = \prod_{i=1}^{m} \mathcal{I}_{r^{l-i}} \otimes Q_r \otimes \mathcal{I}_{r^{i-1}}, \tag{2.8}$$

Table 1: Computation complexity of the fast algorithm based on Pauli block matrices. For simplicity, Add and Mul denote the number of additions and multiplications. The notations L_p^σ and L_q^σ express the number of nonidentity matrices σ_0 in Pauli block matrices Q_p and Q_q.

	Direct approach	Proposed algorithm	Proposed algorithm
Add	$(n-1)n$	$(p-1)nm$	$pn+qn-2n$
Mul	n^2	$L_p^\sigma nm$	$L_p^\sigma mn + L_q^\sigma sn$

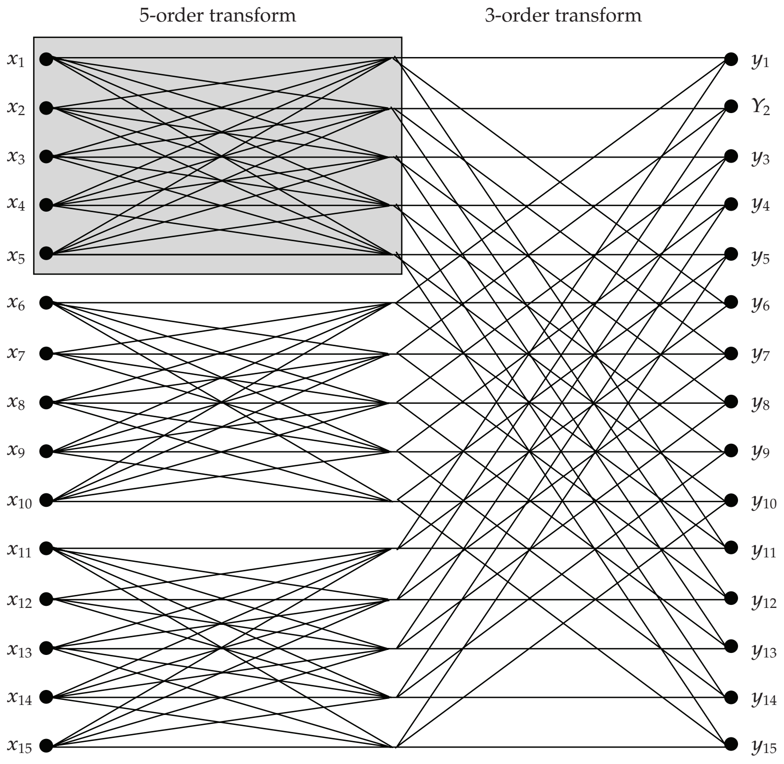

Figure 1: Signal flow graph for Pauli block transform for Q_{15}.

where $r \in \{p,q\}$ and $l \in \{s,m\}$. According to the properties of the Kronecker product, it is easy to calculate

$$Q_{q^s p^m} = Q_{q^s} \otimes Q_{p^m} = \left(\mathcal{I}_{q^s} \otimes Q_{p^m}\right) \cdot \left(Q_{q^s} \otimes \mathcal{I}_{p^m}\right), \tag{2.9}$$

and then this completes the proof of the theorem. □

Employing Pauli Block matrices Q_n in Constructions 2.1, 2.2, and 2.3 with respect to the Kronecker product in (2.7), any large-order Pauli block matrices can be constructed with the fast algorithm. The computational complexity of the proposed algorithm is shown in Table 1.

As an example, the construction of $Q_{15} = Q_3 \otimes Q_5$ is depicted in Figure 1. According to Table 1, the computation of the Pauli block matrix Q_{15} requires 26 additions and 34 multiplications. Compared with the directed computation, the proposed algorithm is obviously faster.

3. Abelian Group Based on Pauli Block Matrices

Let $\mathcal{P}^{\otimes n}$ denote the set of the n-fold tensor products (the Kronecker product) of Pauli operators (matrices) in $\mathcal{P}$ [13]. Then $\mathcal{P}^{\otimes n}$, together with possible multiplicative factors in $\{\pm i, \pm 1\}$, form a group of n-qubit operations, denoted by $\mathcal{G}_n$. An arbitrary operation $\alpha_u \in \mathcal{G}_n$ can be uniquely expressed by

$$\alpha_u = i^{\lambda}\left[\sigma_1^{x_{u1}}\sigma_2^{z_{u1}}\right] \otimes \cdots \otimes \left[\sigma_1^{x_{un}}\sigma_2^{z_{un}}\right], \tag{3.1}$$

where $x_{ut}, z_{ut} \in \{0,1\}$ for $1 \leq t \leq n$. Omitting factor i^{λ}, we denote α_u by a concatenated $2n$-dimensional vector $\overrightarrow{\alpha}_u$ [6]:

$$\overrightarrow{\alpha}_u = \left(\overrightarrow{x}_u \mid \overrightarrow{z}_u\right) = \left(x_{u1}, \ldots, x_{un} \mid z_{u1}, \ldots, z_{un}\right). \tag{3.2}$$

The Hamming weight of $\overrightarrow{\alpha}_u$ is the number of $(x_{uh} \mid z_{uh})$ $(1 \leq h \leq n)$ such that $(x_{uh} \mid z_{uh}) \neq (0 \mid 0)$. The symplectic inner product of any two vectors $\overrightarrow{\alpha}_u = (\overrightarrow{x}_u \mid \overrightarrow{z}_u)$ and $\overrightarrow{\alpha}_v = (\overrightarrow{x}_v \mid \overrightarrow{z}_v)$ is defined by

$$\overrightarrow{\alpha}_u \cdot \overrightarrow{\alpha}_v = \overrightarrow{x}_u \cdot \overrightarrow{z}_v + \overrightarrow{z}_u \cdot \overrightarrow{x}_v, \tag{3.3}$$

where $\overrightarrow{x}_u \cdot \overrightarrow{z}_v = \sum_{i=1}^{n} x_{ui} z_{vi}$ and $\overrightarrow{z}_u \cdot \overrightarrow{x}_v = \sum_{i=1}^{n} z_{ui} x_{vi}$. According to [6], two operations α_u and α_v commute if and only if

$$\overrightarrow{\alpha}_u \cdot \overrightarrow{\alpha}_v = 0. \tag{3.4}$$

The symplectic inner product of two vectors is important since it can be used conveniently to search for generators of an Abelian subgroup $\mathcal{S} \subseteq \mathcal{G}_n$.

Assume that each row of a Pauli block matrix Q_n is denoted by $(\sigma_{i_1}, \ldots, \sigma_{i_n})$ for $1 \leq i \leq n$, from which an n-qubit operation, called as the row operator, can be obtained as

$$\alpha_i = \sigma_{i_1} \otimes \cdots \otimes \sigma_{i_n}. \tag{3.5}$$

Based on properties of the Kronecker product [11, 14, 15], we achieve the commutativity of row operators for Pauli block matrices Q_n.

Theorem 3.1. *For Pauli block matrices Q_n proposed in Construction 2.1 (also for Constructions 2.2 and 2.3), all independent row operators of Q_n are commuting and hence generate an Abelian group.*

Proof. Employing Pauli block matrices Q_n that are constructed via substituting Pauli matrices for the entries of the Hadamard matrices, all row operators of Q_n can be expressed by the concatenated vectors in (3.2), from which the $n \times 2n$ matrices $(H_x \mid H_z)$ can hence be constructed. According to the properties of the Hadamard matrices, it is easy to calculate

$$H_x \cdot H_z^T + H_z \cdot H_x^T = 0 \mod 2, \tag{3.6}$$

which implies that all independent n-qubit row operators of Q_n are commuting [5]. □

Corollary 3.2. *Considering any two given Pauli block matrices Q_p and Q_q, all independent pq-qubit row operators of the Kronecker product $Q_{pq} = Q_p \otimes Q_q$ are commuting.*

Example 3.3. We consider $GF(3) = \{0, 1, 2\}$ with the nonzero squares $1^2 = 1 \bmod 3$ and $2^2 = 1 \bmod 3$, and hence $\mathcal{L}_3(0) = 0, \mathcal{L}_3(1) = 1$, and $\mathcal{L}_3(2) = -1$. With the rows and columns of a matrix Q_3 being indexed by $\{0, 1, 2\}$, one obtains

$$Q_3 = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}. \tag{3.7}$$

According to Construction 2.1, one gains the Pauli block matrix:

$$Q_3^{(1)} = \begin{pmatrix} \sigma_i & \sigma_i & \sigma_j \\ \sigma_j & \sigma_i & \sigma_i \\ \sigma_i & \sigma_j & \sigma_i \end{pmatrix}. \tag{3.8}$$

Taking $i = 1$ and $j = 3$, one has the concatenated matrix:

$$H_3 = \left(H_3^x \mid H_3^z\right) = \begin{array}{c|c} 110 & 001 \\ 011 & 100 \\ 101 & 100 \end{array}. \tag{3.9}$$

It is easy to check that $H_3^x \cdot H_3^{z^T} + H_3^z \cdot H_x^{3^T} = 0 \mod 2$, which means that three row operators of $Q_3^{(1)}$

$$\begin{aligned} \alpha_1 &= \sigma_1 \otimes \sigma_1 \otimes \sigma_3, \\ \alpha_2 &= \sigma_3 \otimes \sigma_1 \otimes \sigma_1, \\ \alpha_3 &= \sigma_1 \otimes \sigma_3 \otimes \sigma_1 \end{aligned} \tag{3.10}$$

are commuting.

For another, based on Construction 2.2, one obtains

$$Q_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{pmatrix}, \tag{3.11}$$

from which the Pauli block matrix $Q_4^{(1)}$ can be achieved:

$$Q_4^{(1)} = \begin{pmatrix} \sigma_i & \sigma_i & \sigma_i & \sigma_i \\ \sigma_j & \sigma_i & \sigma_i & \sigma_j \\ \sigma_j & \sigma_j & \sigma_i & \sigma_i \\ \sigma_j & \sigma_i & \sigma_j & \sigma_i \end{pmatrix}. \tag{3.12}$$

Taking $i = 1$ and $j = 3$, one has the concatenated matrix:

$$H_4 = \begin{array}{c|c} 1111 & 0000 \\ 0110 & 1001 \\ 0011 & 1100 \\ 0101 & 1010 \end{array}, \tag{3.13}$$

from which it is easy to check that all row operators of $Q_4^{(1)}$ are commuting.

Example 3.4. According to $GF(5)$ with $\mathcal{L}_5(1) = \mathcal{L}_5(4) = 1 \mod 5$ and $\mathcal{L}_5(2) = \mathcal{L}_5(3) = -1 \mod 5$, if the rows and columns of Q_5 are indexed by $GF(5)$, one gets

$$Q_5 = \begin{pmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{pmatrix}. \tag{3.14}$$

Employing Construction 2.1, we get the Pauli block matrix:

$$Q_5^{(1)} = \begin{pmatrix} \sigma_i & \sigma_i & \sigma_j & \sigma_j & \sigma_i \\ \sigma_i & \sigma_i & \sigma_i & \sigma_j & \sigma_j \\ \sigma_j & \sigma_i & \sigma_i & \sigma_i & \sigma_j \\ \sigma_j & \sigma_j & \sigma_i & \sigma_i & \sigma_i \\ \sigma_i & \sigma_j & \sigma_j & \sigma_i & \sigma_i \end{pmatrix}. \tag{3.15}$$

Taking $i = 1$ and $j = 3$, one has

$$H_5 = \begin{array}{c|c} 11001 & 00110 \\ 11100 & 00011 \\ 01110 & 10001 \\ 00111 & 11000 \\ 10011 & 01100 \end{array}, \tag{3.16}$$

which means that five row operators of $\mathcal{Q}_5^{(1)}$ for $i = 1$ and $j = 3$ are commuting.

Furthermore, according to Construction 2.3 with respective Q_5 in (3.14), one obtains a Pauli block matrix $\mathcal{Q}_{10}^{(1)}$ for $i = 1$ and $j = 3$ with the concatenated matrix H_{10} expressed as

$$H_{10} = \begin{array}{c|c} 1011000011 & 0100111100 \\ 0010010110 & 1101101001 \\ 1110110000 & 0001001111 \\ 1000100101 & 0111011010 \\ 0011101100 & 1100010011 \\ 0110001001 & 1001110110 \\ 0000111011 & 1111000100 \\ 0101100010 & 1010011101 \\ 1100001110 & 0011110001 \\ 1001011000 & 0110100111 \end{array}. \tag{3.17}$$

It is obvious that all row operators of $\mathcal{Q}_{10}^{(1)}$ are commuting.

4. The Stabilizer Quantum Codes

In this section, we construct quantum codes $C(\mathcal{S})$ by using Pauli block matrices $\mathcal{Q}_n$ with commutative row operators, from which $n - k$ independent row operators can be selected as generators of an Abelian group $\mathcal{S}$.

Given an Abelian subgroup $\mathcal{S}$ of $\mathcal{G}_n$, the stabilizer quantum code $C(\mathcal{S})$ is a set of n-qubit quantum states $\{|\psi\rangle\}$ associated with $\mathcal{S}$, that is,

$$C(\mathcal{S}) = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle, \ \forall M \in \mathcal{S}\}, \tag{4.1}$$

which is the subspace fixed by $\mathcal{S}$ (called as the stabilizer). For an $[[n, k, d]]$ stabilizer quantum code, which encodes k logical qubits into n physics qubits, $C(\mathcal{S})$ has dimension 2^k and $\mathcal{S}$ has 2^{n-k} independent operators.

To construct such a quantum code, the sticking point is to search for an Abelian group, the stabilizer $\mathcal{S}$, from which the code $C(\mathcal{S})$ can be structurally generated through (4.1).

Theorem 4.1. *Given a Pauli block matrix $\mathcal{Q}_n$ with commutative row operators, the stabilizer quantum code $C(\mathcal{S})$ can be constructed with parameters $[[n, k, d]]$ where the stabilizer $\mathcal{S}$ is a set of n-qubit operators generated from $n - k$ independent row operators of Pauli block matrix $\mathcal{Q}_n$.*

Proof. Suppose that there are r ($r \geq n - k$) independent rows of $\mathcal{Q}_n$. Then $n - k$ generators of the stabilizer $\mathcal{S}$ can be generated by selecting $n - k$ rows from these r independent rows of $\mathcal{Q}_n$ provided $n - k \leq r$. Namely, any $n - k$ operators $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{n-k}}$ can be selected to generate an Abelian group:

$$\mathcal{S} = \langle \alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{n-k}} \rangle, \tag{4.2}$$

which is a stabilizer in essence. By making use of (4.1), a stabilizer quantum code $[[n, k, d]]$ can be generated from $\mathcal{S}$. According to the quantum Singleton bound proposed in [6], it follows that $k \leq n - 2d + 2$. This completes the proof of the theorem. □

Example 4.2. We consider the Pauli block matrix $\mathcal{Q}_5$ in (3.15) with the concatenated matrix $H_5 = (H_5^x \mid H_5^x)$ in (3.16). It is known that all rows of H_5 are independent. Thus, any $5 - k$ rows of H_5, denoted by $\mathscr{H}_5 = (h_5^x \mid h_5^z)$, can be selected to generate the stabilizer $\mathcal{S}$ with $5 - k$ generators. According to the construction conditions of quantum codes in [5], we get the generator matrix of quantum codes $\mathcal{G}_5 = (g_5^x \mid g_5^z)$ satisfying

$$h_5^x \cdot g_5^z + h_5^z \cdot g_5^x = 0, \tag{4.3}$$

which can be rewritten as

$$\mathscr{H}_5 \cdot R \cdot \mathcal{G}_5 = 0, \tag{4.4}$$

where $R = \begin{pmatrix} 0_{5\times5} & I_{5\times5} \\ I_{5\times5} & 0_{5\times5} \end{pmatrix}$. To construct such a quantum code, we assume that there exists one unitary matrix U such that

$$U(hR) = \left(I_{(5-k)\times(5-k)} \mid \Lambda_{(5-k)\times(5+k)}\right). \tag{4.5}$$

According to (4.4), the generator matrix g is calculated:

$$\mathcal{G}_5 = \left(\Lambda^T_{(5-k)\times(5+k)} \mid I_{(5+k)\times(5+k)}\right), \tag{4.6}$$

from which quantum codes can be constructed with the parameters $[[5, 0, 4]]$, $[[5, 1, 2]]$, $[[5, 2, 1]]$, $[[5, 3, 1]]$, and $[[5, 4, 1]]$.

Taking the quantum code $[[5,1,2]]$ as an example, we select 4 rows to generate the matrix:

$$\mathscr{H}_5 = \begin{array}{c|c} 11001 & 00110 \\ 11100 & 00011 \\ 01110 & 10001 \\ 00111 & 11000 \end{array}. \tag{4.7}$$

From (4.4), we get

$$\mathcal{G}_5 = \begin{array}{c|c} 01101 & 00000 \\ 00010 & 10000 \\ 11010 & 01000 \\ 10110 & 00100 \\ 10000 & 00010 \\ 00110 & 00001 \end{array}. \tag{4.8}$$

Therefore, a quantum code $[[5,1,2]]$ can be constructed from (4.8), where $d = 2$, the Hamming weight of $\mathcal{G}_5$, can be calculated from the Hamming weight of the bitwise or of g_5^x with g_5^z.

Example 4.3. Suppose $n = 10$, and then we consider Pauli block matrix $Q_{10}^{(1)}$ for $i = 1$ and $j = 3$ with the concatenated matrix in (3.17). It is obvious that all rows of H_{10} are independent and commutative. Selecting any $10 - k$ $(0 \le k \le 10)$ row operators $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{10-k}}$ from $Q_{10}^{(1)}$, we obtain the stabilizer $\mathcal{S} = \langle \alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{10-k}} \rangle$, from which quantum codes can be constructed with the parameters $[[10,0,4]]$, $[[10,1,4]]$, $[[10,2,4]]$, $[[10,3,3]]$, $[[10,4,3]]$, $[[10,5,3]]$, $[[10,6,3]]$, $[[10,7,3]]$, $[[10,8,1]]$, and $[[10,9,1]]$.

5. Conclusion

A family of quantum codes is investigated with fast Pauli block transforms by using quadratic residues in the finite field $GF(q)$. We first investigate the construction approaches based on three kinds of Pauli block matrices with commutative row operators. Then the large-order Pauli block matrices are structurally constructed via the fast Pauli block constructing transforms based on the recursive relationship of identity matrices and successively lower-order Pauli block matrices. These Pauli block matrices have such a characteristic that all row operators are independent and commutative, which can generate an Abelian operator group. Finally, an instructive approach for constructions of quantum codes is suggested via the stabilizer formalism according to the Abelian group $\mathcal{S}$ yielded from Pauli block matrices. This code may provide the great flexibility in designing quantum codes with large block length through implementing the proposed fast construction algorithms.

Acknowledgment

This research was supported by the WCU R-32-2008-000-20014-0 NRF, South Korea.

References

[1] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer, New York, NY, USA, 2nd edition, 1986.

[2] C. G. J. Jacobi, *Uber die Kreisteilung und ihre Anwendung auf die Zahlentheorie*, Bericht Ak. Wiss, Berlin, Germany, 1837.

[3] G. Zeng, Y. Li, Y. Guo, and M. H. Lee, "Stabilizer quantum codes over the Clifford algebra," *Journal of Physics A*, vol. 41, no. 14, Article ID 145304, 8 pages, 2008.

[4] V. Aggarwal and A. R. Calderbank, "Boolean functions, projection operators, and quantum error correcting codes," *IEEE Transactions on Information Theory*, vol. 54, no. 4, pp. 1700–1707, 2008.

[5] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2492–2495, 1999.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[7] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, 2004.

[8] R. Matsumoto, "Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes," *IEEE Transactions on Information Theory*, vol. 48, no. 7, pp. 2122–2124, 2002.

[9] M. Lee and G. Zeng, "Family of fast jacket transform algorithms," *Electronics Letters*, vol. 43, no. 11, p. 651, 2007.

[10] M. H. Lee and J. Hou, "Fast block inverse jacket transform," *IEEE Signal Processing Letters*, vol. 13, no. 8, pp. 461–464, 2006.

[11] G. Zeng and M. H. Lee, "A generalized reverse block jacket transform," *IEEE Transactions on Circuits and Systems I*, vol. 55, no. 6, pp. 1589–1600, 2008.

[12] Z. Chen, M. H. Lee, and G. Zeng, "Fast cocyclic jacket transform," *IEEE Transactions on Signal Processing*, vol. 56, no. 5, pp. 2143–2148, 2008.

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK, 2000.

[14] M. H. Lee, "A new reverse jacket transform and its fast algorithm," *IEEE Transactions on Circuits and Systems II*, vol. 47, no. 1, pp. 39–47, 2000.

[15] M. H. Lee, B. S. Rajan, and J. Y. Park, "A generalized reverse jacket transform," *IEEE Transactions on Circuits and Systems II*, vol. 48, no. 7, pp. 684–690, 2001.