A Construction of Quantum Stabilizer Codes Based on Syndrome Assignment by Classical Parity-Check Matrices

Ching-Yi Lai and Chung-Chin Lu, Member, IEEE

Abstract—In this paper, a new but simple construction of stabilizer codes and related entanglement-assisted quantum error-correcting codes is proposed based on syndrome assignment by classical parity-check matrices. This method turns the construction of quantum stabilizer codes to the construction of classical parity-check matrices satisfying a specific commutative condition. The designed minimum distance \(2t^* + 1\) of the constructed quantum stabilizer codes can be achieved by a commutative classical parity-check matrix with classical minimum distance \(4t^* - m_n\), where the parameter \(m_n\), \(0 \leq m_n \leq 2t^*\), depends on a property of the parity-check matrix. As \(m_n\) decreases, there is an increasing set of additional correctable error operators beyond the designed error correcting capability \(t^*\). The (asymptotic) coding efficiency is at least comparable to that of CSS codes. A class of quantum Reed–Muller codes is constructed and codes in this class have a larger set of correctable error operators than that of the quantum Reed–Muller codes previously developed in the literature. Quantum circulant codes are also constructed and many of them are optimal in terms of their coding parameters.

Index Terms—Entanglement-assisted quantum error-correcting codes, quantum error-correcting codes, quantum information processing, quantum Reed–Muller codes, quantum stabilizer codes.

I. INTRODUCTION

THE theory of quantum error correction has been profoundly developed in the last decade since the first quantum error-correcting code proposed by Shor [1]. In [2], using a different approach from that of Shor, Steane gave a new quantum error-correcting code and studied the basic theory of quantum error correction. Later, Steane gave more new quantum codes and discussed the methods of constructing quantum error-correcting codes in [3]. The complete quantum error correction condition was given in [4]–[6]. After the CSS code construction [7], [8], the study of quantum error-correcting codes then turned to the study of classical self-orthogonal codes.

In quantum coding theory, stabilizer codes are probably the most important class of quantum codes. They are regarded as the quantum analogue of classical linear block codes and their properties have been carefully studied in the literature. The idea of stabilizer codes was proposed in [9], [10] and properties of stabilizer codes were extensively addressed in [10], [11]. CSS codes can then be viewed as one prominent class of stabilizer codes. In [12], Steane gave a further improvement, called an enlargement of CSS codes, which produces several families of quantum codes with greater minimum distance.

If shared entanglement between the encoder and the decoder is available, classical linear codes that are not self-orthogonal can be transformed to the corresponding stabilizer codes [13], [14]. These codes are called entanglement-assisted quantum error-correcting (EAQEC) codes. Then standard stabilizer codes become a special class of EAQEC codes with no entanglement between the encoder and the decoder. And EAQEC codes can be regarded as generalized stabilizer codes.

In this paper we will propose a new but simple construction of quantum stabilizer codes and EAQEC codes based on syndrome assignment by classical parity-check matrices and develop several classes of quantum codes from this construction.

This paper is organized as follows. In Section II, we begin in describing the basic properties of stabilizer codes, including a new formulation of CSS codes and their enlargement, and end with a brief introduction of EAQEC codes. The method of constructing stabilizer codes and EAQEC codes based on syndrome assignment by classical parity-check matrices is proposed in Section III, where we discuss the asymptotic coding efficiency of this method. As an illustration, we develop a family of quantum stabilizer codes from classical Reed–Muller codes in Section IV. Other quantum codes inspired by classical quadratic-residue codes are investigated in Section V, where many optimal quantum codes are constructed. A conclusion is given in Section VI.

II. STABILIZER CODES AND EAQEC CODES

A. Stabilizer Groups and Stabilizer Codes

Let \(\mathcal{H}\) be the state space of a qubit. An element in the Pauli group \(\mathcal{G}_n\), which acts on the state space \(\mathcal{H}^{\otimes n}\) of \(n\) qubits, is expressed as \(i^a M_1 \otimes M_2 \otimes \cdots \otimes M_n\), where each \(M_i\) is one of the Pauli operators \(I, X, Y,\) or \(Z\) on \(\mathcal{H}\), and \(a \in \{0, 1, 2, 3\}\).

A stabilizer group \(\mathcal{S}\) is a subgroup of \(\mathcal{G}_n\) so that its fixed space \(\mathcal{T} = \{\psi \in \mathcal{H}^{\otimes n} | \forall g \in \mathcal{S}, g\psi = \psi\}\) is a non-trivial subspace of \(\mathcal{H}^{\otimes n}\). A stabilizer group \(\mathcal{S}\) has to be abelian and \(-I \notin \mathcal{S}\). If \(\mathcal{S}\) is generated by \(n - k\) independent generators so that its fixed space \(\mathcal{T}\) is a \(2^k\)-dimensional subspace of \(\mathcal{H}^{\otimes n}\), \(\mathcal{T}\) will be called an \([n, k]\) quantum stabilizer code and denoted
as $\mathcal{C}(S)$. The quantum error-correction condition \cite{10}, \cite{11}, \cite{15} states that \{ $E_1$ \} is a collection of correctable error operators in $\mathcal{G}_n$ for $\mathcal{C}(S)$ if and only if

$$E_1^j E_k \notin N(S) \setminus \hat{S} \quad \forall j, k$$

where $N(S) = \{ g \in \mathcal{G}_n \mid ghg^\dagger \in \mathcal{S} \land h \in \mathcal{S} \}$ is the normalizer group of $S$ in $\mathcal{G}_n$, and $\hat{S} = SK = \{ gh \mid g \in \mathcal{G}_n, h \in K \}$, where $K = \{ \pm I^{2^n}, \pm iI^{2^n} \}$. The weight of an element $r' M_1 \otimes M_2 \otimes \cdots \otimes M_n$ in $\mathcal{G}_n$ is defined to be the number of $M_j$'s not equal to $I$. Then the minimum distance $d$ of the quantum code $\mathcal{C}(S)$ is defined to be the minimum weight of an element in $N(S) \setminus \hat{S}$. In this case, $\mathcal{C}(S)$ is an $[[n, k, d]]$ quantum code.

B. Check Matrices

Any element $x \in \mathbb{Z}_2^{2n}$ can be denoted by $x = (u, v)$ with $u, v$ two binary $n$-tuples. We use the product $uv$ to denote the $n$-tuple of the bitwise AND of $u$ and $v$. Then we define the generalized weight of a $2n$-tuple $x = (u, v)$ in $\mathbb{Z}_2^{2n}$ by $w(g) = w(u) + w(v) - w(uw)$, where $w(h)$ means the number of nonzero components of a binary $n$-tuple $h$. A $g$ in $\mathcal{G}_n$ can be uniquely expressed as $g = i^\alpha M_1 \otimes M_2 \otimes \cdots \otimes M_n$ in $\mathcal{G}_n$. The mapping $\varphi : \mathcal{G}_n \rightarrow \mathbb{Z}_2^{2n}$ given by $\varphi(i^\alpha X_1 Z_2) = (\alpha, \beta)$ is a group homomorphism which is an epimorphism with kernel $K$. It is clear that a subset \{ $g_1, \ldots, g_r$ \} of $\mathcal{G}_n$ is a set of independent generators if and only if $\varphi(g_1), \ldots, \varphi(g_r)$ are linearly independent $2n$-tuples in $\mathbb{Z}_2^{2n}$. Two elements $g, h$ in $\mathcal{G}_n$ are commutative if and only if

$$\varphi(g) \Lambda_{2n} \varphi(h)^T = 0, \quad \Lambda_{2n} = \begin{pmatrix} O_{n \times n} & I_{n \times n} & I_{n \times n} & O_{n \times n} \\ O_{n \times n} & I_{n \times n} & O_{n \times n} & I_{n \times n} \end{pmatrix}.$$ 

For a generating set \{ $g_1, \ldots, g_r$ \} of a stabilizer group $S$ with $r$ independent generators, we define a check matrix $H$ of $S$ by making $\varphi(g_i)$ as its $i$th row vector. $H$ is an $r \times 2n$ binary matrix and can be denoted by $H = [H_X \mid H_Z]$, with $H_X, H_Z$ two $r \times n$ binary matrices. Since $S$ is an abelian group, $\varphi(g) \Lambda_{2n} \varphi(h)^T = 0, \forall g, h \in S$, and a check matrix $H$ of $S$ has to satisfy the following commutative condition

$$H \Lambda_{2n} H^T = H_X H_Z^T + H_Z H_X^T = O_{r \times r}. \quad (2)$$

An $r \times 2n$ binary matrix $H = [H_X \mid H_Z]$ will be called commutative if it satisfies the commutative condition.

Let $\hat{S} = \varphi(S)$, $S$ is a subspace of $\mathbb{Z}_2^{2n}$ and can be viewed as a classical binary linear block code with a generator matrix $H$. As in \cite{10}, \cite{16}, a symplectic inner product $\ast$ can be defined on $\mathbb{Z}_2^{2n}$ by $(u_1, v_1) \ast (u_2, v_2) = u_1 \cdot v_2 + v_1 \cdot u_2$, which is just $(u_1, v_1)A_{2n}(u_2, v_2)^T$. Thus, two elements $g, h$ in $\mathcal{G}_n$ are commutative if and only if the symplectic inner product $\varphi(g) \ast \varphi(h)$ of $\varphi(g)$ and $\varphi(h)$ is zero. Let $S^{\perp}$ $\ast$ $\{ (u, v) \in \mathbb{Z}_2^{2n} \mid (u, v) \ast (\alpha, \beta) = 0, \forall (\alpha, \beta) \in \hat{S} \}$, the symplectic dual code of $\hat{S}$. Since the normalizer $N(S)$ of $S$ in $\mathcal{G}_n$ is just the centralizer of $S$ in $\mathcal{G}_n$, $N(S) = \varphi^{-1}(\hat{S}^{\perp})$. It is clear that $\hat{S}$ is a self-orthogonal code with respect to this symplectic inner product, i.e., $\hat{S} \subset S^{\perp}$. An $(2n-r) \times 2n$ binary matrix $G = [G_X \mid G_Z]$ of rank $2n-r$, where $G_X$ and $G_Z$ are $(2n-r) \times n$ binary matrices, is a generator matrix of $S^{\perp}$ if and only if

$$H \Lambda_{2n} G^T = H_X G_Z^T + H_Z G_X^T = O. \quad (3)$$

It can be seen that the minimum distance of $\mathcal{C}(S)$ is just the minimum generalized weight of a nonzero codeword in $S^{\perp} \setminus \hat{S}$. This helps decide the minimum distance of a stabilizer code, as illustrated in the construction of CSS codes \cite{7}, \cite{8} and their enlargement \cite{12} in the next subsection.

C. CSS Codes and Their Enlargement

To construct an $[[n, k, d]]$ CSS code $\mathcal{C}(S)$, we choose a classical $n, k_1$ binary code $C_1$ and an $[n, k_2]$ subcode $C_2$ of $C_1$ such that both the code $C_1$ and the classical dual code of $C_2$ have minimum distance $\geq d$. Then a check matrix of a stabilizer group $S$ is established as $H = [G_2 \mid G_1 \mid H_1], \text{ of rank } n - k_1 + k_2$, where $G_2$ is a generator matrix of $C_2$ and $H_1$ is a parity-check matrix of $C_1$. The minimum distance of the quantum code is no less than the minimum generalized weight of the symplectic dual code $\hat{S}^{\perp}$ with a generator matrix $G = [G_1 \mid O \mid G_2], \text{ of rank } n - k_1 + k_2$. The dimension of the quantum code is $k = n - (n - k_1 + k_2) = k_1 - k_2$.

The enlargement of CSS codes in \cite{12} is based on the CSS construction and exchanges code dimension for error-correcting capability. With additional stabilizer generators, this enlargement increases the minimum distance of the code by half. Let $C_1$ be a classical $[n, k_1, d_1]$ binary code which contains its classical dual $C_1^\perp$. Furthermore, let $C_1$ be able to be enlarged to $C_2 = [n, k_2, d_2]$, where $k_2 > k_1$. Suppose that $G_1, G_2 = [G_1 \mid G_3]$ are generator matrices of $C_1, C_2$, respectively, and $H_2, H_3 = \begin{pmatrix} H_2 \\ H_3 \end{pmatrix}$ are parity-check matrices of $C_2, C_1$, respectively. Let $P$ be a nonsingular $(k_2 - k_1) \times (k_2 - k_1)$ binary matrix so that $I + P$ is also nonsingular. If $H_3 G_2^T$ is a nonsingular $(k_2 - k_1) \times (k_2 - k_1)$ binary matrix, by taking

$$H = \begin{pmatrix} H_2 & O \\ O & QH_3 \end{pmatrix}, \quad \begin{pmatrix} G_1 \\ G_3 \end{pmatrix} = \begin{pmatrix} G_1 \\ O \end{pmatrix} \begin{pmatrix} O \quad G_2 \end{pmatrix}$$

as a check matrix of a stabilizer group $S$, where $Q = (H_3 G_2^T) (P^T)^{-1} (H_3 G_2^T)^{-1}$, an $[n, k_2 + k_1 - n]$ quantum code $\mathcal{C}(S)$ can be constructed. The symplectic dual code $\hat{S}^{\perp}$ of $S$ has a generator matrix

$$G = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix} \begin{pmatrix} O \\ O \end{pmatrix} \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$$

and has minimum generalized weight $\geq \min \{d_1, \frac{3d_2}{2} \}$. Thus $\mathcal{C}(S)$ is an $[[n, k_2 + k_1 - n, d \geq \min \{d_1, \frac{3d_2}{2} \}]]$ quantum code.
D. EAQEC Codes

Let $S$ be an arbitrary subgroup of $G_n$, possibly non-abelian. A result of [17] states that $S$ can be generated, up to overall phase, by a set $\{Z_1, \ldots, Z_n, X_1, \ldots, X_n\}$ of $r$ independent generators with $0 \leq r \leq n$ and

\[
\begin{align*}
|Z_i, Z_j| &= 0, \text{ for all } i, j, \\
|X_i, X_j| &= 0, \text{ for all } i, j \\
|Z_i, X_j| &= 0, \text{ for all } i \neq j, \\
|Z_i, X_i| &= 0, \text{ for all } i,
\end{align*}
\]

where $[g, h] = gh - hg$ and $\{g, h\} = gh + hg$. We say that $Z_i, X_i$ form a symplectic pair for each $i = 1, \ldots, c$. Let $S_h = \langle Z_1, \ldots, Z_c, X_1, \ldots, X_c \rangle$ denote the symplectic subgroup of $S$, generated by the symplectic pairs. Let $S_\tau = \langle \tilde{Z}_1, \ldots, \tilde{Z}_r, \tilde{X}_1, \ldots, \tilde{X}_r \rangle$ denote the isotropic subgroup of $S$, which is a commutative subgroup. Without loss of generality, we assume that $S = \langle S_\tau, S_h \rangle$.

The subgroup $S$ of $G_n$ can be extended such that the extended group $S'$ is a commutative subgroup of $G_n$, as follows. Let $\tilde{Z}_k = \tau^{ik} M_{k,1} \otimes M_{k,2} \otimes \cdots \otimes M_{k,n}$ and $\tilde{X}_j = \tau^{jk} N_{j,1} \otimes N_{j,2} \otimes \cdots \otimes N_{j,n}$. Defining a mapping $\phi : S \rightarrow S'$ given by $\phi(\tilde{Z}_k) = M_{k,1} \otimes M_{k,2} \otimes \cdots \otimes M_{k,n} \otimes M_{k,n+1} \otimes \cdots \otimes M_{k,n+c}$, where $M_{k,n+k} = Z_k \cap M_{k,n+k} = 1, l \neq k, 1 \leq l \leq c$, for $k = 1, \ldots, n + c$, and $M_{k,n+c} = I, 1 \leq k \leq c$, for $k = 1, \ldots, c$. Similarly, $\phi(\tilde{X}_j) = N_{j,1} \otimes N_{j,2} \otimes \cdots \otimes N_{j,n} \otimes N_{j,n+c+1} \otimes \cdots \otimes N_{j,n+c} = X_j$, for $j = 1, \ldots, c$. It can be verified that $S' = \langle \tilde{Z}_1, \ldots, \tilde{Z}_r, \tilde{X}_1, \ldots, \tilde{X}_r \rangle$ is a commutative subgroup of $G_n$.

Now let $B$ be the subgroup of $G_n$ generated by the $r$ independent generators $Z_1, \ldots, Z_r, X_1, \ldots, X_c$, where $Z_i = I^{(c-1)} \otimes \tau^i \otimes \tau^{i+1} \otimes \cdots \otimes \tau^{n-1} \otimes X \otimes \tau^{n+c-1} \otimes \cdots \otimes \tau^{n+c} \otimes \tau^{n+c+1}$ for $1 \leq i < j < n$. Similarly, $S$ can be extended to a commutative subgroup $B' = \langle \tilde{Z}_1, \ldots, \tilde{Z}_r, \tilde{X}_1, \ldots, \tilde{X}_r \rangle$ of $G_n$, $n' = n + c$, with $Z_i = I^{(c-1)} \otimes \tau^i \otimes \tau^{i+1} \otimes \cdots \otimes \tau^{n-1} \otimes \tau^j \otimes \cdots \otimes \tau^{n+c-1} \otimes \cdots \otimes \tau^{n+c} \otimes \tau^{n+c+1}$ for $1 \leq i < c$. The error-correction condition in (1) implies the following: if any two error operators $E_1$ and $E_2$ in $S$, each with weight less than or equal to $c$, satisfy that

\[
\begin{align*}
\psi_{E_1} \psi_{E_2} \in N(S) \setminus \tilde{S}_\tau \forall j, k
\end{align*}
\]

where $\tilde{S}_\tau = S_\tau K = \{gh \mid g \in S, h \in K \}$, then the minimum distance $d$ of the EAQEC code $C(S')$ is defined to be the minimum weight of an element in $N(S) \setminus \tilde{S}_\tau$. Hence the two groups $S_2$ and $S_3$ define an $[n, k, d]_\text{EAQEC}$ code with $k = n - r + c$. If $H$ is a check matrix of $S$, then

\[
2c = \text{rank}(H \Lambda_{2n} H^T).
\]

Note that standard stabilizer codes are in the special case of $c = 0$ or $S_\tau = S$.

III. A SIMPLE CONSTRUCTION OF STABILIZER CODES

A. Syndrome Assignment

In [9], Gottesman proposed a class of stabilizer codes, which are one-qubit error-correcting and saturate the quantum Hamming bound, by assigning distinct “error syndrome” to each correctable error operator according to a certain rule. We generalize this brilliant idea to construct $[n, k, d]_\text{quantum codes}$ with $d = \frac{4l-1}{2} \geq 1$.

The error-correction condition in (1) implies the following: if any two error operators $E_1$ and $E_2$ in $G_n$, each with weight less than or equal to $t^*$, satisfy that

\[
E_1^* E_2 \notin N(S), \tilde{S}
\]

for a certain stabilizer group $S, C(S)$ is at least $t^*$-qubit error-correcting. As in [9], for any $g \in G_n$, we define $f_g : g_n \rightarrow \mathbb{Z}_2$ by

\[
f_g(h) = \begin{cases} 
0, & \text{if } gh - hg = 0, \\
1, & \text{if } gh + hg = 0.
\end{cases}
\]

And for a given generating set of a stabilizer group $S$ with $r$ independent generators $g_1, g_2, \ldots, g_r$, we define $f_{S} : g_n \rightarrow \mathbb{Z}_2$ by $f_{S}(g) = (f_{g_1}(h), f_{g_2}(h), \ldots, f_{g_r}(h))^T$, which is called the syndrome of $h$ with respect to the (generating set $\{g_1, g_2, \ldots, g_r\}$) of the stabilizer group $S$. It is clear that

\[
f_{S}(h) = HA_{2n} \varphi(h)^T
\]

where $H$ is the check matrix of $S$ corresponding to the (ordered) generators $g_1, g_2, \ldots, g_r$. It can be verified that $f_{S}$ is a group homomorphism. From (7), the columns of the check matrix $H$ of $S$ are just the syndromes of the just stabilizers $Z_1, \ldots, Z_n, X_1, \ldots, X_n$ w.r.t. $S$. Thus to establish a check matrix $H$ of a target stabilizer group $S$ means to assign $2n$ syndromes $f_{S}(Z_1), \ldots, f_{S}(Z_n), f_{S}(X_1), \ldots, f_{S}(X_n)$.
as its columns and to verify this matrix to be commutative. Since 
\[ f_S(h) = (0, 0, \ldots, 0)^T \] if and only if \( h \in N(S) \) and by (6), the stabilizer code \( C(S) \) will be at least \( t^* \)-qubit error-correcting if \( f_S(E_1) \neq f_S(E_2) \) for any two error operators \( E_1 = i^v X_a Z_b \) and \( E_2 = i^v X_a Z_{-b} \) in \( G_n \) with \( gw(a, b), gw(u, v) \preceq t^* \) and \( (a, b) \neq (u, v) \). Note that \( f_S(E_1) = f_S(E_2) \) for all \( E \in G_n \), since \( \varphi(E) = \varphi(E) \). Let \( a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n), u = (u_1, u_2, \ldots, u_n) \) and \( v = (v_1, v_2, \ldots, v_n) \). Since \( f_S \) is a group homomorphism and \( gw(a, b), gw(u, v) \preceq t^* \), each of
\[
\begin{align*}
    f_S(E_1) &= f_S(i^v X_a Z_b) = \sum_{i=1}^{n} a_i f_S(X_i) + b_i f_S(Z_i) \\
    f_S(E_2) &= f_S(i^v X_a Z_{-b}) = \sum_{i=1}^{n} u_i f_S(X_i) + v_i f_S(Z_i)
\end{align*}
\]
is a sum of no more than \( 2t^* \) terms and then
\[
\begin{align*}
    f_S(E_1) &= s = \sum_{i=1}^{n} (a_i + u_i) f_S(X_i) + \sum_{i=1}^{n} (b_i + v_i) f_S(Z_i)
\end{align*}
\]
is a sum of no more than \( 4t^* \) terms. Thus any \( 4t^* \) out of the \( 2n \) chosen syndromes \( f_S(Z_1), \ldots, f_S(Z_n), f_S(X_1), \ldots, f_S(X_n) \) are linearly independent, then \( f_S(E_1) \neq f_S(E_2) \) for any two error operators \( E_1 = i^v X_a Z_b \) and \( E_2 = i^v X_a Z_{-b} \) in \( G_n \) with \( gw(a, b), gw(u, v) \preceq t^* \) and \( (a, b) \neq (u, v) \) and then the target stabilizer code will have minimum distance at least \( 2t^* + 1 \). This corresponds to a property of a parity-check matrix of a classical linear block code with minimum distance \( d' \geq 4t^* + 1 \), where any \( d' - 1 \) column vectors of the parity-check matrix must be linearly independent. Now we conclude the above discussion in the following basic theorem.

\textbf{Theorem 1:} Given an \( (n - k) \times 2n \) parity-check matrix \( H' \) of a binary \( 2n, n + k, d' \) linear block code \( C' \) with minimum distance \( d' \geq 4t^* + 1 \) such that the commutative condition
\[
H'P A_{2n} P^T H^T = O.
\]
holds for a certain \( 2n \times 2n \) permutation matrix \( P \), an \([n, k, d \geq 2t^* + 1]\) stabilizer code with a check matrix \( H = H'P \) can be constructed.

One reason to introduce a permutation matrix \( P \) in Theorem 1 is to possibly ease the establishment of a check matrix which has to satisfy the commutative condition in (8). In Section III-D, we will show that it is possible for a permutation matrix \( P \) to increase (the lower bound of) the minimum distance of a constructed stabilizer code by half.

By (4), similar result can be obtained for the scheme of EAQEC codes and hence together with (5), we have the following basic theorem.

\textbf{Theorem 2:} Given an \( (n - k) \times 2n \) parity-check matrix \( H \) of a binary \( 2n, n + k, d' \) linear block code \( C' \) with minimum distance \( d' \geq 4t^* + 1 \), let \( S \) be a subgroup of \( G_n \) having a check matrix \( H = H'P \), then an \([n, k + c, d \geq 2t^* + 1; c]\) EAQEC code defined by \( S \) can be constructed, where \( c = \frac{1}{2} \text{rank}(HA_{2n}H^T) \).

Note that the commutative condition in (8) is not required in Theorem 2 due to the entanglement-assistance in the scheme of EAQEC codes. Theorem 2 indicates that any classical binary linear block code of even length with minimum distance \( \geq 4t^* + 1 \) can be directly turned to construct an EAQEC code with minimum distance \( \geq 2t^* + 1 \).

\section{Additional Correctable Error Operators}

A \( t^* \)-error-correcting quantum stabilizer code of length \( n \) has \( \sum_{i=0}^{t^*} \binom{n}{3i} \) error syndromes. One may expect that a quantum stabilizer code constructed by the method of syndrome assignment in above can correct more than just those error operators of weight \( \leq t^* \) determined from \( \alpha' \) in Theorems 1 and 2. In fact, any error operator \( E = i^v X_a Z_b \) with \( w(a) + w(b) \leq 2t^* \) has its own unique syndrome and hence can be corrected. For example, error operators \( X_a \) and \( Z_a \) with \( w(a) = 2t^* \) are correctable.

Let \( E = i^v M_1 \otimes M_2 \otimes \cdots \otimes M_n = i^v X_a Z_b, a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n), \in \mathbb{Z}^n \), be a correctable error operator with \( w(a) + w(b) \leq 2t^* \). Let \( l = gw(a, b) \) be the weight of \( k \) so that \( 0 \leq l \leq 2t^* \). Let \( m_y = w(ab) \) be the number of \( M_y \) which are equal to \( X \) or \( Z \). Then \( m_X Z \triangleq l - m_y \) represents the number of \( M_y \) which are equal to \( X \) or \( Z \). Since \( w(a) + w(b) = 2m_Y + m_{XZ} = m_y + l \), we have \( m_Y + l \leq 2t^* \) (note that \( l = m_{XZ} + m_Y \)). There are \( 4t^* \binom{n}{t} 2t^* (m_Y) 2^{l-m_Y} \) correctable error operators for a certain \( l \) and a certain \( m_Y \) satisfying \( 0 \leq m_Y \leq l \) and \( 0 \leq m_Y + l \leq 2t^* \). Summing \( l \) from \( t^* + 1 \) to \( 2t^* \) and summing \( m_Y \) from 0 to \( 2t^* - l \), we have additional
\[
4 \sum_{l=t^*+1}^{2t^*} \sum_{m_Y=0}^{l} \binom{n}{l} \left( \frac{l}{m_Y} \right) 2^{l-m_Y}
\]
correctable error operators of weight \( >t^* \), which can be a large amount! Fig. 1 illustrates the \( m_X Z \)-\( m_Y \) region containing additional correctable error operators of weight \( l = m_{XZ} + m_Y > t^* \) as the dashed triangle.

On the other hand, for a given stabilizer group \( S \) with quantum error-correcting capability \( t \), the classical minimum distance \( d' \) of a check matrix of \( S \) can be used to determine the existence of additional correctable error operators of weight \( >t \) and how many of them as stated in the following proposition and illustrated in the slanted triangle in Fig. 1.

\textbf{Proposition 3:} Let \( t \) be the quantum error correcting capability of a stabilizer code or a EAQEC code \( C(S) \). Let \( t^* \) be an estimate of \( t \) by a check matrix of \( S \) as in Theorems 1 and 2. If \( t < 2t^* \) or \( \left| \frac{d'}{2} - 1 \right| < 2 \left| \frac{d'}{2} - \frac{1}{2} \right| \), then we have additional
\[
4 \sum_{l=t^*+1}^{2t^*} \sum_{m_Y=0}^{l} \binom{n}{l} \left( \frac{l}{m_Y} \right) 2^{l-m_Y}
\]
correctable error operators of weight \( >t \).

\section{Improvement of Basic Theorems}

We next strengthen Theorems 1 and 2. Define a matrix \( H_Y \triangleq H_X + H_Z \) for a check matrix \( H = (H_X \mid H_Z) \) of \( S \). The
columns of $H_Y$ are the syndromes $f_S(Y_i) = f_S(X_i) + f_S(Z_i)$ of basic operator $Y_i, 1 \leq i \leq n$. Let $C_X, C_Z, C_Y$ be classical binary linear block codes with parity-check matrices $H_X, H_Z, H_Y$, respectively. If syndromes of all error operators of weight no more than $t^*$ are distinct, it is necessary that $C_X, C_Z, C_Y$ have minimum distance $\geq 2t^* + 1$.

**Theorem 4:** Let $m$ be a given integer in $[0, 2t^*]$. If, for each $k$, $0 \leq k \leq m$, we replace any $k$ columns of $H_Y$ with the corresponding $k$ columns of either $H_X$ or $H_Z$ (not necessarily all from the same $H_X$ or the same $H_Z$) so that the resulting matrix $H'_Y$ is a parity-check matrix of a classical binary linear block code with minimum distance $\geq 2t^* + 1$, the minimum distance required for a classical binary linear block code in Theorems 1 and 2 can be reduced to $t^* - m$.

**Proof:** Let $E_1 = \vec{v} X_a Z_{\vec{v}}$ and $E_2 = \vec{v} X_a Z_{\vec{v}}$ be two error operators in $G_n$ such that $gw(a, b), gw(u, v) \leq t^*$ and $(a, b) \neq (u, v)$, where $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n), u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$. If

$$f_S(E_1 E_2) = f_S(E_1) + f_S(E_2)$$

$$= \sum_{i=1}^n (a_i + u_i) f_S(X_i) + \sum_{i=1}^n (b_i + v_i) f_S(Z_i)$$

(10)

is a linear combination of less than $4t^* - m$ columns of the check matrix $H$, then $f_S(E_1 E_2) \neq 0$ due to $d' \geq 4t^* - m$ and $(a, b) \neq (u, v)$. The remaining case is that (10) is a linear combination of no less than $4t^* - m$ columns of the check matrix $H$. Let $I_X, I_Y$ and $I_Z$ be the sets of indices $i$ such that $a_i = 1, b_i = 0, a_i = 1 = b_i$, and $a_i = 0, b_i = 1$ respectively. Similarly let $J_X, J_Y$ and $J_Z$ be the sets of indices $j$ such that $u_j = 1, v_j = 0, u_j = 1 = v_j$, and $u_j = 0, v_j = 1$, respectively. Then

$$f_S(E_1 E_2) = \sum_{i \in I_X} f_S(X_i) + \sum_{i \in I_Y} (f_S(X_i) + f_S(Z_i))$$

$$+ \sum_{j \in J_X \setminus I_X} f_S(Z_j) + \sum_{j \in J_Y \setminus I_Z} f_S(X_j)$$

(11)

$$- \sum_{i \in I_Y} f_S(Y_i) + \sum_{j \in J_X} f_S(X_j) + \sum_{j \in J_Z} f_S(Z_j)$$

$$+ \sum_{i \in I_X \setminus I_Y} f_S(X_i) + \sum_{i \in I_Z \setminus I_Y} f_S(Z_i)$$

(12)

where $I'_Y = I_Y \setminus J_Y, J'_X = J_X \setminus I_X, I'_Z = I_Z \setminus J_Z$. Since $gw(a_i, b_i) = I_X + |I_Y| + |I_Z| \leq t^* + gw(u_i, v_i) - |J_X| + |J_Y| + |J_Z| \leq t^*$

$$|I'_X| + |I'_Y| + |I'_Z| + |J'_X| + |J'_Y| + |J'_Z| \leq |I_X| + |I_Y| + |I_Z| + |J_X| + |J_Y| + |J_Z| \leq 2t^*$.

(13)

And since (11) is a linear combination of no less than $4t^* - m$ columns of the check matrix $H$,

$$|I_X| + |I_Y| + |J_X| + |J_Y| + |J_Z| \geq 4t^* - m.$$  

(14)

By (13) and (14), we have $|I_Y| + |J_Y| \geq 2t^* - m$ and again by (13)

$$|I_X| + |I_Y| + |J_X| + |J_Y| + |J_Z| \leq m.$$  

(15)

Note that $I'_X, I'_Y, I'_Z$ are disjoint and $J'_X, J'_Y, J'_Z$ are also disjoint. We next show that the number of terms in (12) can be reduced. If either $i \in I_X \setminus J_X$ or $i \in I_Z \setminus J_Z$, we replace the sum $f_S(X_i) + f_S(Z_i)$ by $f_S(Y_i)$ so that (12) becomes

$$f_S(E_1 E_2)$$

$$- \sum_{i \in I'_Y} f_S(Y_i) + \sum_{j \in J_X \setminus I_X} f_S(X_j)$$

$$+ \sum_{j \in J_Y \setminus I_Z} f_S(Z_j)$$

$$+ \sum_{i \in I_X \setminus I_Y} f_S(X_i) + \sum_{i \in I_Z \setminus I_Y} f_S(Z_i)$$

$$= \sum_{i \in I_X \setminus I_Y} f_S(X_i) + \sum_{i \in I_Z \setminus I_Y} f_S(Z_i)$$

(16)

where $I'_Y = I'_Y \cap (I_X \setminus J_X)$ and $J'_Y = J'_Y \setminus (I_X \setminus J_X)$. Furthermore if either $i \in I'_X \cap (J_X \setminus J_Y)$ or $i \in I'_Y \cap (J_X \setminus J_Z)$,
we replace either the sum $f_s(Y_i) + f_s(Z_i)$ by $f_s(X_i)$ or the sum $f_s(Y_j) + f_s(X_j)$ by $f_s(Z_j)$ so that (16) becomes

$$f_s(E_1 E_2) = \sum_{i \in I_X \cap I_Z} f_s(Y_i) + \sum_{j \in I_Y \cap I_Z} f_s(Y_j) + \sum_{i \in I_Y \cap I_X \cap I_Z} f_s(Z_i) + \sum_{j \in I_Y \cap I_X \cap I_Z} f_s(Z_j) = \sum_{i \in I_X} f_s(Y_i) + \sum_{j \in I_Y} f_s(Y_j) + \sum_{i \in I_X} f_s(Z_i) + \sum_{j \in I_Y} f_s(Z_j);$$

(17)

where $I_X \cap I_Y$, $I_X \cap I_Z$, $I_Y \cap I_X$, and $I_Y \cap I_Z$ are disjoint to each other, and $I_X \cap I_Y \cap I_Z$ is a subset of $I_X \cap I_Y \cap I_Z$.

After completing the reduction process, let $K = I_X \cap I_Y \cap I_Z$. Then $K$ is a non-empty set of indices $i$ such that either $f_s(X_i)$ or $f_s(Z_i)$ (not both) remains in (17). Then $r \leq |K|$ and $|I_X| + |I_Y| + |I_Z| + |I_X \cap I_Y| + |I_X \cap I_Z| + |I_Y \cap I_Z| 

= n$ by (15) and (17). The proof is now complete.

In particular, if $C_Y$ has minimum distance $2t_1 + 1$, then with $m_2 = 0$, the minimum distance required for a classical binary linear block code in Theorems 1 and 2 can be reduced to $d' \geq 2t_1$.

D. Constructions of Check Matrices

Our construction of a check matrix of a stabilizer group needs a binary commutative parity-check matrix of even length. In this subsection, we suggest four ways to establish commutative parity-check matrices by using classical constructions of new codes from old ones [19] such that the minimum distances of the resulting quantum stabilizer codes can be determined from the corresponding classical binary linear block codes.

Construction I: (diagonal construction) Suppose that $k_1 + k_2 > n$ and $H_1 H_2^T = 0$, i.e., the classical dual code of $C_2$ is a subcode of $C_1$ (and vice versa). Then $H = \begin{bmatrix} H_1 & O \\ O & H_2 \end{bmatrix}$ is a parity-check matrix of a 2$n$, $k_1 + k_2$, $d' = \min\{d_1, d_2\}$ classical binary linear block code with a generator matrix $G = \begin{bmatrix} G_1 \\ O \\ G_2 \end{bmatrix}$ and satisfies the commutative condition $H \Delta_2n H^T = 0$ in Theorem 1 with $P = I$. Thus $H$ is a check matrix of a stabilizer group $\mathcal{S}$. Since $H_X = \begin{bmatrix} H_1 \\ O \end{bmatrix}$, $H_Z = \begin{bmatrix} O \\ H_2 \end{bmatrix}$, and $H_Y = H_X + H_Z = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$, we can replace any number of columns of $H_Y$ with the corresponding columns of either $H_X$ or $H_Z$ so that the resulting matrix $H_Y'$ is a parity-check matrix of a classical binary linear block code with minimum distance $\geq 2t^* + 1$, where $t^* = [(d' - 1)/2]$. By Theorem 4 with $m = 2t^*$ and $d' \geq 4t^* - m - 2t^*$, $C(S)$ is an $[n, k_1 + k_2 - n, d \geq 2t^* + 1]$ stabilizer code. This can also be obtained by noting that the symplectic dual code $\tilde{S}^\perp$ of $\tilde{S}$ has a generator matrix $G \Delta_2n \begin{bmatrix} O \\ G_2 \\ G_1 \end{bmatrix}$ and the minimum distance $d$ of $C(S)$ is the minimum generalized weight of a nonzero codeword in $S^\perp \setminus \tilde{S}$ so that $d \geq d' \geq 2t^* + 1$. Note that this diagonal construction is equivalent to the construction of CSS codes.

Construction II: (circulant construction) To construct a check matrix $H = H_X H_Z$ of the following joint circulant form,

$$H = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ a_1' & a_2' & \cdots & a_n' \\ \vdots & \vdots & \ddots & \vdots \\ a_1'_{r-1} & a_r' & \cdots & a_{r-2} \\ a_r & a_{r-1} & \cdots & a_{r-2} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{r-1} \end{bmatrix}$$

(18)

where $r = n - k$ is the rank of the check matrix $H$ and $g_1 = \{a_0, a_1, \ldots, a_{n-1}\}$, $g_2 = \{b_0, b_1, \ldots, b_{r-1}\}$ are two binary $n$-tuples, called generators. This method will be called the circulant construction and quantum codes generated by this method will be called quantum circulant codes. Circulant construction and quantum circulant codes will be investigated in Section V.

Construction III: ([n]/v + v construction) Suppose that $k_1 + k_2 > n$ and $H_1 H_2 = 0$, i.e., the classical dual code of $C_2$ is a subcode of $C_1$ (and vice versa). Then $H = \begin{bmatrix} H_1 \\ O \end{bmatrix}$ is a parity-check matrix of a 2$n$, $k_1 + k_2$, $d' \geq 2t^* = \min\{d_1, d_2\}$ classical binary linear block code with a generator matrix $G = \begin{bmatrix} G_2 \\ G_1 \\ O \end{bmatrix}$ and satisfies the commutative condition $H \Delta_2n H^T = 0$ in Theorem 1 with $P = I$. Thus $H$ is a check matrix of a stabilizer group $\mathcal{S}$. Since $H_X = \begin{bmatrix} H_1 \\ O \end{bmatrix}$, $H_Z = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$, and $H_Y = H_X + H_Z = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$, we can replace any number of columns of $H_Y$ with the corresponding columns of either $H_X$ or $H_Z$ so that the resulting matrix $H_Y'$ is a parity-check matrix of a classical binary linear block code with minimum distance $\geq 2t^* + 1$, where $t^* = [(d' - 1)/2]$. By Theorem 4 with
m = 2t* and d' \geq d^* \geq 4t* - m = 2t*, C(S) is an 
[n, k_1 + k_2 - n, d \geq 2t* + 1] stabilizer code. This can also 
be seen by noting that the sympletic dual code \( \bar{S}^\perp \) of \( S \) has 
a generator matrix \( GA_{2n} = \begin{bmatrix} G_2 \\ G_1 \end{bmatrix} \) and the minimum 
distance \( d \) of \( C(S) \) is the minimum generalized weight of a 
nonzero codeword in \( \bar{S}^\perp \setminus S \) so that \( d \leq d^* \leq 2t* + 1 \).

**Construction IV:** (construction with permutation)
Suppose that \( k_1 + k_2 > n \) and there is an \( n \times n \) permutation 
matrix \( P \) such that \( H_1 = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix} \) and \( G_1 = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} \) classical binary linear block code with a generator matrix 
\( G = \begin{bmatrix} G_2 \\ G_1 \\ I_n \\ O \\ O \end{bmatrix} \) and satisfies the commutative condition \( H \Lambda_2 H^T = 0 \) in Theorem 
1 with \( H' = \begin{bmatrix} H_1 \\ H_2 \\ H_1 \end{bmatrix} \) and \( P = \begin{bmatrix} I_n \\ O \\ O \end{bmatrix} \). Thus \( H \) is a check matrix of a stabilizer group \( S \). Similar to the \( |u|+v \) 
construction (without permutation), by applying Theorem 4 
with \( t^* = \lfloor (d^* - 1)/2 \rfloor, m = 2t^* \) and \( m' \geq m' \geq 4t* - m = 2t^* \), \( C(S) \) is an 
\([n, k_1 + k_2 - n, d \geq 2t^* + 1] \) stabilizer code. This can also be seen by noting that the simplectic dual code 
\( \bar{S}^\perp \) of \( S \) has a generator matrix \( GA_{2n} = \begin{bmatrix} G_2 \\ G_1 \end{bmatrix} \).

Consider a nonzero codeword in \( \bar{S}^\perp \),

\[
(c_1, c_2) = (u_1, u_2) \begin{bmatrix} G_2 \\ G_1 \end{bmatrix} = (u_1 G_2 Q, u_1 G_2 Q + u_2 G_1 Q)
\]

with a \( k_1 \)-tuple \( u_1 \) and a \( k_2 \)-tuple \( u_2 \), not both zeros. If \( u_1 \neq 0 \), then \( g_2(u_1, c_2) \geq d_2 \). And if \( u_1 = 0 \) and \( u_2 \neq 0 \), then \( g_2(u_1, c_2) \geq d_1 \). Thus the minimum distance \( d \) of \( C(S) \) is 
\( d \geq d^* = \min \{d_1, d_2\} \geq 2t^* + 1 \).

Moreover, the introduction of a permutation matrix \( P = \begin{bmatrix} I_n \\ O \\ O \end{bmatrix} \) to the \( |u|+v \) construction may improve (the lower bound of) the minimum distance of the constructed 
stabilizer code \( C(S) \), as illustrated in the following theorem.

**Theorem 5:** In the \( |u|+v \) construction with permutation, 
where \( k_1 + k_2 > n \) and \( Q \) is an \( n \times n \) permutation matrix such that 
\( H_1 (Q + Q^T) H_1^T = O \) and \( H_2 Q H_2^T = O \), assume that 
\( G_1 = \begin{bmatrix} H_2 \end{bmatrix} \) for some \( (k_2 - k_1) \times n \) matrix \( G_3 \) so that \( C_1 \) is a 
subcode of \( C_2 \) with \( d_1 > d_2 \),

\[
C_1 Q = C_1,
\]

and

\[
u G_3 + u G_3 Q \in C_2 \setminus C_1 \text{ for any } (k_2 - k_1) \text{-tuple } u \neq 0.
\]

Then there is an \([n, k_2 + k_1 - n, d \geq \min \{d_1, \frac{2d^* + 1}{3}\}]\) 
stabilizer code \( C(S) \) corresponding to a stabilizer group \( S \) with 

a check matrix \( H = \begin{bmatrix} H_1 \\ H_2 \\ Q \end{bmatrix} \).

**Proof:** Note that \( GA_{2n} = \begin{bmatrix} G_2 Q \\ O \\ G_1 \end{bmatrix} \) is a generator 
matrix of \( \bar{S}^\perp \). Consider a nonzero codeword

\[
(r_1, r_2) = (u_1, u_2, u_3) \begin{bmatrix} G_2 Q \\ G_1 Q \\ O \end{bmatrix} = (u_1 G_2 Q + u_2 G_1 Q, u_3 G_3 Q)
\]

in \( \bar{S}^\perp \), with a \((k_2 - k_1)\)-tuple \( u_1 \) and two \( k_1 \)-tuples \( u_2, u_3 \), not 
all zero tuples. Assume that \( u_1 \neq 0 \). Then \( c_1 \neq 0 \) and \( c_2 \neq 0 \). 
Since \( c_1 \in C_2 Q \) and \( c_2 \in C_2, w(c_1) \geq d_2 \) and \( w(c_2) \geq d_2 \). 
Also we have

\[
c_1 + c_2 - u_1 G_2 Q + u_1 G_1 Q + u_1 G_3 + (u_2 + u_3) G_1
\]

\[
= (u_1 G_2 Q + u_1 G_1 Q + u_1 G_3 + (u_2 + u_3) G_1)
\]

Since \( u_1 G_2 Q + u_1 G_3 \in C_2 \setminus C_1 \) by (20) and \( u_2 G_1 Q + (u_2 + 
\]

\[
u_3 G_1 Q \in C_1 \) by (19), we have \( c_1 + c_2 \neq 0 \) in \( C_2 \) and \( w(c_1 + c_2) \geq d_2 \).

Then

\[
gw(c_1, c_2) = \frac{1}{2} (w(c_1) + w(c_2) + w(c_1 + c_2)) \geq \frac{3d_2}{2}
\]

Next if \( u_1 = 0 \), we have \( c_1 = u_2 G_1 Q \in C_1 \) and 
\( c_2 = (u_2 + u_3) G_1 \in C_1 \), not both \( 0 \). Hence \( gw(c_1, c_2) \geq d_1 \).

Therefore, the minimum distance of the quantum code is 
\( d \geq \min \{d_1, \frac{3d_2}{2}\} \).

**Remark 1:** If a permutation \( Q \) is in the intersection of the 
automorphism groups \( Aut(C_1) \) and \( Aut(C_2) \) of \( C_1 \) and \( C_2 \) [19], 
then (19) is satisfied and \( u G_3 + u G_3 Q \in C_2 \) for any \((k_2 - 
\]

\[
k_1)\)-tuple \( u \neq 0 \) so that (20) is equivalent to

\[
u G_3 + u G_3 Q \neq C_1
\]

for any \((k_2 - k_1)\)-tuple \( u \neq 0 \). Since \( Aut(C_1) = Aut(C_1^T) \) 
and \( Aut(C_2) = Aut(C_2^T) \) [19] and \( H_1 = \begin{bmatrix} H_2^T \\ H_1 \end{bmatrix} \) for some 
\((k_2 - k_1) \times n \) matrix \( H_2 \), if \( H_1 \) is weakly self-dual, i.e., \( H_1 H_1^T = O \), 
then \( H_2 Q H_2^T = O \) and

\[
H_1 Q H_1^T - O, H_1 Q T H_1^T - H_1 (H_1 Q)^T - O
\]

which imply that \( H_1 (Q + Q^T) H_1^T = O \). We conclude that if 
\( Q \in Aut(C_1) \cap Aut(C_2) \) and \( H_1 H_1^T = O \), then all the conditions 
required for \( Q \) in Theorem 5 will hold if (21) is verified.

**E. Existence of Commutative Parity-Check Matrices**
There is a related question: for a given \( r \times (2n) \) parity-check 
matrix \( H \), where \( r < n \), does there exist a permutation matrix 
\( P \) such that \( HP \) is commutative?

To answer this question, we run a simulation on a computer as 
follows. Let \( H = \begin{bmatrix} I_r x_r \\ B \end{bmatrix} \), where \( B \) is a randomly generated 
\( r \times (2n - r) \) matrix. Each element of \( B \) is 1 or 0 with probability 
\( p_1 \) and \( p_0 = 1 - p_1 \), respectively. By exhaustive search 
with \( (2n)! \) permutations for the case \( n = 5 \), unfortunately, we 
found that there exists an \( H \) which has no permutation matrix 
\( P \) such that \( HP \) is commutative. However, there is a high probability 
that for a randomly generated matrix \( H = \begin{bmatrix} I_r x_r \\ B \end{bmatrix} \),
there is a permutation matrix $P$ such that $HP$ is commutative. Moreover, if $p_1 < p_2$, the probability becomes higher. This simulation suggests that parity-check matrices of classical LDPC codes may highly probably be transformed into check matrices of stabilizer codes through Theorem 1. However, it becomes extremely harder to verify this suggestion for $n \geq 8$ due to prohibitive computing complexity. $(16!) \approx 2 \times 10^{13}$, which is about $10^5$ times the case $n = 5$.) The question of determining a permutation matrix $P$ for a parity-check matrix $H$ so that $HP$ is commutative remains open. The construction of quantum stabilizer codes can be converted to the construction of classical binary linear block codes of even length which have rate $> 1/2$ and a commutative parity-check matrix.

### F. Asymptotic Coding Efficiency

In this subsection, we will investigate the asymptotic coding efficiency of the construction of stabilizer codes as stated in Theorem 1 by assuming that for any $n$, $k$, $d'$ considered, there is at least one code with a commutative parity-check matrix among all classical $[2n, n + k, d']$ binary linear block codes.

Now an $[n, k, d \geq d' = 2t' + 1]$ stabilizer code is constructed by Theorem 1 from an $[n', k' = k + n, d' \geq 4t' + 1]$ classical binary linear block code, where $t' = \left\lceil \frac{d' - 4}{4} \right\rceil$.

Let $\alpha' = \lim_{n \to \infty} \sup_{n \to \infty} \frac{k}{n}$ and $\alpha = \lim_{n \to \infty} \sup_{n \to \infty} \frac{k}{n}$. Since $\alpha' = \lim_{n \to \infty} \sup_{n \to \infty} \frac{k + n}{2n} = \frac{1}{2} + \frac{1}{2} \alpha$, we have

$$\alpha = 2\alpha' - 1. \quad (22)$$

Let $\delta' = \frac{d' - 4}{n}$, $\delta' = \frac{d' - 4}{n}$ and $\delta = \frac{d}{n}$. Since \( \left\lceil \frac{d' - 4}{4} \right\rceil \leq \frac{d' - 4}{4} < \left\lceil \frac{d' - 4}{4} \right\rceil + 1 \), we have $t' \leq \frac{d' - 4}{4} < t' + 1$ and $2d' - 1 \leq t' < 2d' + 3$. Thus we have $\frac{2d' - 1}{2n} \leq \delta' \leq \frac{2d' - 1}{2n}$ and $\delta - \frac{1}{2n} \leq \delta' < \delta + \frac{1}{2n}$. Thus for sufficiently large $n$, we have

$$\delta' \approx \delta'. \quad (23)$$

It is obvious that $\delta \geq \delta' \geq \delta'$. From [20], the classical Hamming bound says that $\alpha' \left( \delta' \right) \leq 1 - H_2 \left( \frac{1}{2} \delta' \right)$, where $H_2(x) = -x \log_2(x) - \{1 - x\} \log_2(1 - x)$. By (22) and (23), we have a corresponding quantum Hamming bound of the code construction in Theorem 1, which is

$$\alpha(\delta') \leq 1 - 2H_2 \left( \frac{1}{2} \delta' \right). \quad (24)$$

The classical Plotkin Bound says that

$$\alpha'(\delta') \leq 1 - 2\delta', \quad \text{if } 0 \leq \delta' \leq \frac{1}{2};$$
$$\alpha'(\delta') = 0, \quad \text{if } \frac{1}{2} < \delta' \leq 1$$

and by (22) and (23), the corresponding quantum Plotkin bound of the code construction in Theorem 1 is

$$\alpha(\delta') \leq 1 - 4\delta', \quad \text{if } 0 \leq \delta' \leq \frac{1}{2};$$
$$\alpha(\delta') = 0, \quad \text{if } \frac{1}{4} < \delta' \leq 1. \quad (25)$$

The classical Elias Bound says that

$$\alpha'(\delta') \leq 1 - H_2 \left( \frac{1}{2} \sqrt{\frac{1}{2} - \delta'} \right), \quad \text{if } 0 \leq \delta' \leq \frac{1}{2};$$
$$\alpha'(\delta') = 0, \quad \text{if } \frac{1}{2} < \delta' \leq 1$$

and by (22) and (23), the corresponding quantum Elias bound is

$$\alpha(\delta') \leq 1 - 2H_2 \left( \frac{1}{2} \sqrt{\frac{1}{2} - \delta'} \right), \quad \text{if } 0 \leq \delta' \leq \delta_c;$$
$$\alpha(\delta') = 0, \quad \text{if } \delta_c < \delta' \leq 1 \quad (26)$$

where $0 < \delta_c < \frac{1}{2}$ is a constant such that $H_2 \left( \frac{1}{2} \sqrt{\frac{1}{2} - \delta_c} \right) = \frac{1}{2}$ and $\delta_c = 0.1958$ by MATLAB. The classical weaker McEliece-Rodemich-Rumsey-Welch (MRRW) bound says that $\alpha'(\delta') \leq H_2 \left( \frac{1}{2} - \sqrt{\delta'(1 - \delta')} \right)$ and by (22) and (23), the corresponding weaker quantum MRRW bound is

$$\alpha(\delta') \leq 2H_2 \left( \frac{1}{2} - \sqrt{\delta'(1 - \delta')} \right) - 1, \quad \text{if } 0 \leq \delta' \leq \delta_c;$$
$$\alpha(\delta') = 0, \quad \text{if } \delta_c < \delta' \leq 1 \quad (27)$$

where $0 < \delta_c < \frac{1}{2}$ is a constant such that $H_2 \left( \frac{1}{2} - \sqrt{\delta_c(1 - \delta_c)} \right) = \frac{1}{2}$ and $\delta_c = 0.1871$ by MATLAB. The classical McEliece-Rodemich-Rumsey-Welch (MRRW) bound says that

$$\alpha(\delta') \leq 2F(\delta') - 1, \quad \text{if } 0 \leq \delta' \leq \delta_c;$$
$$\alpha(\delta') = 0, \quad \text{if } \delta_c < \delta' \leq 1 \quad (28)$$

where $F(\delta') = \min \{1 + g(u^2) - g(u^2 + 2\delta'u + 2\delta') \mid 0 \leq u \leq 1 - 2\delta'\}$, where $g(x) = H_2 \left( \frac{1 - \sqrt{1 - x}}{2} \right)$ for $0 \leq x \leq 1$. By (22) and (23), the corresponding quantum MRRW bound is

$$\alpha(\delta') \leq 2F(\delta') - 1, \quad \text{if } 0 \leq \delta' \leq \delta_c;$$
$$\alpha(\delta') = 0, \quad \text{if } \delta_c < \delta' \leq 1 \quad (29)$$

The classical Gilbert-Varshamov bound says that $\alpha'(\delta') \geq 1 - H_2(\delta')$, and by (22) and (23), the corresponding quantum Gilbert-Varshamov bound is

$$\alpha(\delta') \geq 1 - 2H_2(\delta'). \quad (30)$$

The above asymptotic bounds for the stabilizer code construction in Theorem 1 are depicted in Fig. 2.

We next compare these asymptotic bounds with known bounds of quantum codes in the literature. In [4], [9], the quantum Hamming bound says that for an $[n, k, d \geq d' \geq d]$.
2t + 1] quantum code, $2^k \sum_{i=0}^{t} 3^{i} \binom{k}{i} \leq 2^n$, and the asymptotic form is $\frac{k}{n} \leq 1 - \frac{1}{n} \log_2 3 - H_2\left(\frac{1}{2}\right)$, or

$$\alpha(\delta) \leq 1 - \frac{1}{2} \delta \log_2 3 - H_2\left(\frac{1}{2}\delta\right).$$

The quantum singleton bound [6], [21] says that for an $[n, k, d]$ quantum code, $n - k \geq 2d - 2$, or

$$\alpha(n^*) \leq 1 - 2\delta. \quad (31)$$

The Gilbert-Varshamov bound for a general quantum stabilizer codes, proved in Theorem 2 in [10], says that an $[n, k, d = 2t + 1]$ stabilizer code exists if $\frac{k}{n} \geq 1 - \frac{2t}{n} \log_2 3 - H_2\left(\frac{2t}{n}\right)$, or

$$\alpha(\delta) \geq 1 - \delta \log_2 3 - H_2(\delta). \quad (32)$$

The Gilbert-Varshamov bound for CSS codes, proved in Section V in [7], says that an $[n, k, d = 2t + 1]$ CSS code exists if $\frac{k}{n} \geq 1 - 2H_2\left(\frac{2t}{n}\right)$, or

$$\alpha(\delta) \geq 1 - 2H_2(\delta). \quad (33)$$

The above known quantum bounds in the literature are depicted in Fig. 3. It can be seen that the two singleton bounds (29) and (31) for the stabilizer code construction in Theorem 1 and for the general quantum codes, respectively, are exactly the same. And the two Gilbert-Varshamov bounds (30) and (33) for the stabilizer code construction in Theorem 1 and for CSS codes are also exactly the same. The Gilbert-Varshamov bounds (32) for general stabilizer codes is still better than the Gilbert-Varshamov bounds (30) for the stabilizer code construction in Theorem 1. All above quantum bounds are depicted in Fig. 4.

IV. QUANTUM REED–MULLER CODES

In this section, we will give a family of quantum stabilizer codes from the parity-check matrices of classical Reed–Muller codes by Construction III, i.e., the $[u, u + v]$ construction, in Subsection III-D. Permutation matrices that increase the quantum minimum distance as stated in Theorem 5 are also investigated.

A. Properties of Classical Reed–Muller Codes

Classical Reed–Muller codes are weakly self-dual codes and have simple but good structural properties [19]. A Reed–Muller code has two parameters $r, m$, $0 \leq r \leq m$, and is denoted by $RM(r, m)$. This code is of length $2^m$ and $r$ is called its order. Consider the following $(m + 1)^{2m}$-tuples:

$$\begin{align*}
1 &= (1111 \cdots 1111 1111 \cdots 1111), \\
v_1 &= (0000 \cdots 0000 0000 \cdots 0000), \\
v_2 &= (0101 \cdots 0101 0101 \cdots 0101), \\
\vdots &= \vdots \cdots \vdots \cdots \vdots \cdots \vdots \cdots \\
v_m &= (1111 \cdots 1111 1111 \cdots 1111). \\
\end{align*}$$

Then $RM(r, m)$ is generated by

$$(\text{degree 0})1, \quad (\text{degree 1})v_1, \cdots, v_m, \quad (\text{degree 2})v_1v_2, \cdots, v_{m-1}v_m \cdots$$

$$(\text{degree } r)v_1v_2 \cdots v_r, \cdots, v_{m-r+1}v_m \cdots \cdots v_m$$
Fig. 3. Known quantum bounds in the literature.

Fig. 4. A Comparison between Quantum Bounds and possible Quantum Bounds for Theorem 1.
where the product of the $v_i$'s means the bitwise AND of the $v_i$'s and the degree means the number of $v_i$'s appearing in the product. There are several properties of $RM(r, m)$ which can be derived directly from its construction [19]. The dimension of $RM(r, m)$ is $k = \sum_{i=0}^{r-1} \binom{m}{i}$ and the minimum distance of $RM(r, m)$ is $d = 2^{m-r}$. The dual code of $RM(r, m)$ is $RM(m - r - 1, m)$ for $0 \leq r < m$, where $RM(-1, m) \triangleq \{0\}$. Let $G_{r(m)}$ denote a generator matrix of $RM(r, m)$. Reed–Muller code $RM(m + 1, m + 1)$ can be obtained from $RM(r, m)$ and $RM(r - 1, m)$ by using the $u | v$ construction. A generator matrix of $RM(r, m + 1)$ is

$$G_{(r, m+1)} = \begin{pmatrix} G_{(r, m)} & \bar{G}_{(r, m)} \\ O & G_{(r-1, m)} \end{pmatrix}.$$

(34)

Since $RM(m - r - 1, m)$ is the dual code of $RM(r, m)$, a parity-check matrix of $RM(r, m)$ is $G_{(r, m)} G_{(m-r-1, m)}^T$ and $G_{(r, m)} G_{(m-r-1, m)}^T = O$. For convenience, the orthogonality of Reed–Muller codes can be remarked in the following lemma.

**Lemma 6**: For $r + s \leq m - 1$ and $m \geq 1$, $G_{(r, m)}$ and $G_{(s, m)}$ are orthogonal, i.e., $G_{(r, m)} G_{(s, m)}^T = O$.

**B. Quantum Reed–Muller Codes From Parity-Check Matrices**

By the $u | v$ construction in Section III-D and Lemma 6, we have

**Lemma 7**: For $1 \leq r$ and $2r \leq m$, $H = G_{(r, m+1)}$ is commutative and is a check matrix of a stabilizer group $S$.

By the $u | v$ construction, the stabilizer code $C(S)$ corresponding to the stabilizer group $S$ in Lemma 7 is of length $n = 2^m$ and dimension $k = 2^m - \sum_{i=0}^{r-1} \binom{m}{i}$. Since $S$ and its symplectic dual $S^\perp$ have generator matrices $H = G_{(r, m+1)}$ and $G = G_{(m-r-1, m)}$, respectively, the minimum distance $d$ of $C(S)$ is the minimum generalized weight of the nonzero codeword in $S^\perp \setminus S$ and is $d = 2^r$ if $2r < m$ and $d = \infty$ if $2r = m$. We have the following theorem.

**Theorem 8**: The parity-check matrix of a classical Reed–Muller code $RM(r, m+1)$ in (34) with $1 \leq r$ and $2r \leq m$ is a check matrix of a $\left[2^m, 2^m - \sum_{i=0}^{r-1} \binom{m}{i}, 2^r\right]$ quantum stabilizer code.

The quantum code in Theorem 8 will be called the quantum Reed–Muller code with parameters $r, m$, denoted as $QRM(r, m)$. Since the quantum error correcting capability $t = 2^r - 1$ of $QRM(r, m)$ equals to the lower bound $t^* = 2^r - 1$ predicted by Theorem 1, $QRM(r, m)$ will have additional correctable error operators of weight $> t$.

Since Reed–Muller codes $RM(r, m)$ with $2r + 1 \leq m$ are weakly self-dual codes, by Lemma 6, we can use them to construct CSS codes. Take $C_1 = RM(r_1, m)$ with minimum distance $2^{m-r_1}$. Then choose $C_2 = RM(r_2, m)$, a subcode of $C_1$, with $r_2 < r_1$. The dual code of $C_2$ is $C_2^\perp = RM(m - r_2 - 1, m)$ with minimum distance $2^{r_1 - 1}$. By CSS construction, we obtain a quantum code with parameters $\left[2^m, 2^{m-r_1} \binom{m}{r_1}, 2^{r_1} \binom{m}{r_1} + 1\right]$. For the best efficiency, we take $r_2 = m - 1$. Let $r = r_2 + 1$. Then $2r \leq r_2 + r_1 + 1 = m$. We now construct a CSS code with parameters

$$\left[2^m, 2^m - 2 \sum_{i=0}^{r_2-1} \binom{m}{i}, 2^r\right].$$

(35)

Comparing the dimension of a CSS code in (35) with that of a $QRM(r, m)$ in Theorem 8, both having the same length $2^m$ and the same minimum distance $2^r$, we know that the CSS construction has a higher efficiency. Nevertheless, the quantum error correcting capability $t = 2^r - 1$ of the CSS code $\left[2^m, 2^m - 2 \sum_{i=0}^{r_2-1} \binom{m}{i}, 2^r\right]$ is greater than the double of the lower bound $d^* = 2^r - 1$ predicted by Theorem 1 so that there are no additional correctable error operators for this CSS code as stated in Proposition 3. However, the construction of $QRM(r, m)$ in Theorem 8 gives us additional correctable error operators of weight $> t$ since $t = t^*$ for $QRM(r, m)$. In Table I, we list the number of additional correctable error operators for $QRM(r, m)$ in Theorem 8 constructed from classical Reed–Muller codes with parameters $(r, m) = (2, 5), (3, 6), (3, 7)$. #A and #O are the numbers of additional and original correctable error operators, respectively. #D is the dimension deficit $\left(\binom{m}{r}\right)$ relative to the corresponding CSS code with the same length and minimum distance.

On the other hand, when comparing the efficiency of the $QRM(r - 1, m)$ is $\left[2^m, 2^m - \sum_{i=0}^{r_2-1} \binom{m}{i}, 2^r\right]$ in Theorem 8 with that of the $\left[2^m, 2^m - 2 \sum_{i=0}^{r_2-1} \binom{m}{i}, 2^r\right]$ CSS code, the former code has a surplus $\left(\binom{m}{r}\right)$ in dimension, while the minimum distance of the former code is only half of that of the latter CSS code. However, the former code has a lot of additional correctable error operators which will strengthen the error performance of the former code.

**C. Permutations Which Increase the Minimum Distance**

We find that if we multiply $G_{(1, m+1)}$ by the permutation matrix $P = \begin{pmatrix} I & O \\ O & Q \end{pmatrix}$ with $Q$ being the permutation matrix used
in [9], a stabilizer group $S$ with a check matrix $H = G_{[1,m+1]} \text{P}$ will give a quantum stabilizer code $C(S)$ with the same parameters $[2^m, 2^m - m - 2, 3]$ as those of the code constructed in [9], while the code by our construction has a larger set of correctable error operators. For example, when $m = 3$

$$Q = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$ 

There are many other permutation matrices that will work by Theorem 10 in [16], which means that a column permutation on a parity-check matrix may give a stabilizer code $C(S)$ with higher quantum error-correcting capability.

We first investigate the effect of permutation matrices on $G_{[r,m+1]}$ with $1 \leq r$ and $2r < m$.

**Theorem 9:** Let $P = \begin{pmatrix} I & \text{O} \\ \text{O} & Q \end{pmatrix}$, where $Q$ is a permutation matrix such that all the conditions in Theorem 5 hold with $C_1 = RM(m - r - 1, m), C_2 = RM(m - r, m)$ and $d_1 = 2^{r+1}, d_2 = 2^r$. Then for $1 \leq r$ and $2r < m$, the quantum stabilizer code $C(S)$ with a check matrix $H = G_{[r,m+1]} \text{P}$ will have parameters $[2^m, 2^m - \sum_{i=0}^{r} \binom{m+1}{i}, d \geq 2^r + 2^{r-1}]$. In addition, $C(S)$ will have additional correctable error operators when $r > 3$.

**Proof:** By Theorem 5, the minimum distance $d$ of $C(S)$ is at least $\min \{ d_1, \frac{3d_1 - 1}{2} \} = 2^r + 2^{r-1}$. Since the classical minimum distance of the parity-check matrix $H = G_{[r,m+1]} \text{P}$ remains unchanged after a column permutation, the lower bound of the quantum error correcting capability for $C(S)$ predicted by Theorem 1 is $t^* = 2^r - 2^{r-1} - 1$, the same as that for $QRM(r, m)$. With $d \geq 2^r + 2^{r-1}$, the error-correcting capability of the quantum code $C(S)$ is $t \geq \hat{i} = \frac{d - 1}{2}$ with $\hat{i} = 3 \cdot 2^r - 2 - 1$ if $r \geq 2$ and $\hat{i} = 1$ if $r = 1$. Then we have $2^r - \hat{i} = 2^r - 2 - 1 > 0$ if $r > \hat{i}$. Thus by Proposition 3 with $\hat{i}$ substituting $\hat{t}$, the quantum code $C(S)$ will have additional correctable error operators of weight $\geq \hat{i} - 3 \cdot 2^{r-2} - 1 \geq 2^r$.

In [22], Steane gave a class of quantum Reed–Muller codes with parameters $[2^m, 2^m - \sum_{i=0}^{r} \binom{m+1}{i}, d \geq 2^r + 2^{r-1}]$. If there exists a permutation matrix $P$ satisfying the assumptions in Theorem 9, a stabilizer group $S$ with a check matrix $H = G_{[r,m+1]} \text{P}$, $r \geq 1$, will give a quantum stabilizer code $C(S)$ having the same parameters as those in [22] but having additional correctable error operators if $r \geq 3$.

We next discuss effective permutation matrices for $G_{[r,m+1]}$ with $1 \leq r$ and $2r < m$. Considering the following two $2^m \times 2^m$ permutation matrices $T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, and $S = \begin{pmatrix} I_{2^m-1} & 0 \\ 0 & I_{2^m-3} \end{pmatrix}$. For example, when $m = 3$

$$Q = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$ 

It can be verified that $v_i T = v_{i+1}$ for $1 \leq i \leq |m| - 1$ and $v_m T = v_1$. Also $v_1 S = v_1 + v_m$ and $v_2 S = v_i$ for $2 \leq i \leq m$. Thus $TS$ is a permutation matrix such that $v_i(TS) = v_{i+1}$ for $1 \leq i < (m - 1)$ and $v_m(TS) = v_1 + v_m$. Note that $(v_i, v_i, \ldots, v_i) X = (v_1, X)(v_2, X) \cdots (v_i, X)$ for any $1 \leq i \leq m$, where $X = T, S$ or $T S$. For a generator $v_1, v_2, \ldots, v_i$ of degree $i$, $v_i X(v_1, X) \cdots (v_i, X)$ can be any of the following three cases: (1) a generator of degree $i$; (2) a sum of two generators of degree $i$; (3) a sum of a generator of degree $i$ and a generator of degree $i - 1$. We then prove the following lemma.

**Lemma 10:** $T, S$ and $TS$ are in the automorphism group $\text{Aut}(RM(r, m))$ of $RM(r, m)$ for $0 \leq r \leq m$.

**Lemma 11:** The permutation matrices $T, S$ and $TS$ satisfy all the conditions required for a permutation matrix $Q$ in Theorem 5 with $C_1 = RM(m - r - 1, m), C_2 = RM(m - r, m)$ and $d_1 = 2^{r+1} > d_2 = 2^r$ for $1 \leq r$ and $2r < m$, except (21).

**Proof:** By Lemma 10, $T, S$ and $TS$ are in $\text{Aut}(C_1) \cap \text{Aut}(C_2)$. Since $H_1 = G_{[r,m]}$ is a parity-check matrix of $C_1 = RM(m - r - 1, m)$ and $2r \leq m - 1$, we have $H_1 H_1^T$ by Lemma 6. Thus by Remark 1, $T, S$ and $TS$ satisfy all the conditions for a permutation matrix $Q$ in Theorem 5 except (21).

We next show that $TS$ is effective for $G_{[1,m+1]}$.

**Theorem 12:** The permutation matrix $Q = T S$ satisfies all the conditions for a permutation matrix in Theorem 5 with $C_1 = RM(m - 2, m), C_2 = RM(m - 1, m)$ and $d_1 = 4 > d_2 = 2$ for $m > 2$ so that the quantum stabilizer code $C(S)$ with a.
check matrix \( H = G_{1,m+1} \begin{pmatrix} I & O \\ O & Q \end{pmatrix} \) will have parameters \([2^m, 2^m - m - n \geq 2 \geq 3]\\). 

**Proof:** By Lemma 11, we only need to verify (21). Then by Theorem 9, the proof will be completed. The generator matrices of \( C_1 = H M(m - 2, m) \) and \( C_2 = H M(m - 1, m) \) are 

\[ G_1 = G_{(m-2,m)} \quad \text{and} \quad G_2 = \begin{pmatrix} G_3 \\ G_1 \end{pmatrix} = G_{(m-1,m)} \] 

respectively. The row vectors of \( G_3 \) are \( v_1 v_2 \cdots v_{m-1} \cdots v_2 v_3 \cdots v_m \), which are the \( m \) generators of degree \( m - 1 \). For a generator \( v_j \cdots v_{i-1} \), of degree \( m - 1 \), we let \( v_j = v_j \cdots v_{i-1} \), where \( j \) is not equal to any of \( i_1, \ldots, i_{m-1} \). Then the row vectors of \( G_3 \) are \( w_m \), \( w_{m-1} \), \( \cdots \), \( w_2, w_1 \) with

\[ w_m = (v_1 v_2 \cdots v_{m-1}) Q = v_2 v_3 \cdots v_m = w_1, \\
 w_{m-1} = v_2 v_3 \cdots v_{m-1} v_1 = w_1 + w_m, \\
 w_{m-2} = v_2 v_3 \cdots v_{m-2} v_{m-1} v_1 = v_2 v_3 \cdots v_{m-2} v_{m-1} + w_m, \\
 \cdots \\
 w_2 = v_2 v_3 \cdots v_{m-2} v_{m-1} v_{m-2} v_1 = v_2 v_3 \cdots v_{m-2} v_{m-1} v_{m-2} + w_m, \\
 w_1 = v_2 v_3 \cdots v_{m-2} v_{m-1} v_{m-2} v_{m-1} = v_2 v_3 \cdots v_{m-2} v_{m-1} + w_2. \\
\]

If \( uG_3 + uG_2 \in C_1 \) for some binary \( m \)-tuple \( u = (a_1, \ldots, a_m) \), then 

\[ \sum_{i=1}^{m} a_i w_i + \sum_{i=1}^{m} a_i w_i Q \in RM(m - 2, m), \tag{36} \]

which implies that all the coefficients of the terms of degree \( m - 1 \) in (36) must be zero, i.e.

\[ a_1 + a_2 + a_3 + \cdots + a_{m-1} + a_m = a_1 + a_{m-1} + a_m = 0 \]

and then \( a_i = 0 \) for all \( 1 \leq i \leq m \). Therefore, we have \( uG_3 + uG_2 \notin C_1 \) for any nonzero \((k_2 - k_1)\)-tuple \( u \) so that (21) is verified.

There are permutation matrices, other than \( TS \), which will work by similar proofs. However, the search for an effective permutation for a general \( RM(m, m) \) with \( 2 \leq r \) and \( 2r < m \) is still an open problem.

### V. QUANTUM CIRCULANT CODES

In this section, we investigate the circulant construction in Section III-D with a check matrix \( H = [H_X, H_Z] \) of the following joint circulant form

\[ H = [H_X | H_Z] = [G_1 | G_2] \]

We find the best \([n, k] \) quantum stabilizer codes by computer search as follows. Given two generators \( g_1 = (a_0, a_1, \ldots, a_{n-1}), g_2 = (b_0, b_1, \ldots, b_{n-1}) \), we justify the rank of the circulant check matrix \( H \) in (37) and the commutativity of \( H \) as in (2). Then the minimum distance of the quantum circulant code with the justified check matrix \( H \) is determined by computer search.

We list the best \([n, k] \) quantum stabilizer codes of length 5 ≤ \( n \leq 24 \) in Table II, where many are extremal quantum codes with parameters achieving the upper bounds in Table III in [16]. We find new stabilizer codes of lengths 23 and 24 with parameters \([23,8,5],[24,2,7],[24,8,5] \) and \([24,9,5] \) in Table II. In addition, stabilizer codes of length 25 with parameters \([25,8,5] \) and \([25,9,5] \) are also found. Each of which increases the lower bound of the highest achievable...
minimum distance in Table III in [16]. Note that these parameters can also be found in the table of [23]. The two circular generators for each of the six stabilizer codes with parameters \([23, 8, 5], [24, 2, 7], [24, 8, 5], [24, 9, 5], [25, 8, 5]\) and \([25, 9, 5]\) are listed in Table III. The quantum cyclic codes that have comparable parameters are quantum BCH codes [24]. We find that for \(n = 21\) our parameters \([21, 3, 6], [21, 9, 4], [21, 15, 3]\) are better than the parameters \([21, 3, 5], [21, 9, 3], [21, 15, 2]\) of quantum BCH codes and for \(n = 5, 7, 13, 15, 17, 23\), the parameters are the same.

When considered as classical parity-check matrices, the check matrices of these best quantum circulant codes are observed to have classical minimum distances exactly the same as their corresponding quantum minimum distances. Indeed, Theorem 4 is well applicable to the check matrices of these best quantum circulant codes for \(n = 21\) parameters. For example, when \(p = 13\), we have

\[g_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad g_2 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}\]

We begin with the following lemma to apply the circulant construction for quadratic residue related quantum stabilizer codes modulo a prime \(p \equiv 1 \mod 4\).

**Lemma 13:** For a prime \(p \equiv 1 \mod 4\), the two \(p \times p\) matrices

\[
H^*_X = \begin{bmatrix}
0 & 1 & \cdots & 0 \\
1 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & 1
\end{bmatrix}
\quad \text{and}
\]

\[
H^*_Z = \begin{bmatrix}
0 & \cdots & 0 \\
\ddots & \ddots & \ddots \\
0 & \cdots & 1
\end{bmatrix}
\]

are symmetric.

**Proof:** We have \(a_j = 1\) if \(j \in Q\) and \(a_j = 0\), else, by the definition of \(g_1\). For a prime \(p \equiv 1 \mod 4\), \(-1 \in Q\) and we have \(a_j = a_{-j} = a_{(j-p)\mod p}\). The element in the \(i\)-th row and the \(j\)-th column of \(H^*_X\) is \((H^*_X)_{ij} = a_{j-i} \mod p\). Since \((H^*_X)_{ij} = a_{(j-i)\mod p} = a_{-(j-i)\mod p} = (H^*_X)_{ji}\), the matrix \(H^*_X\) is symmetric. The proof for the symmetry of \(H^*_Z\) is similar.

**Theorem 14:** For a prime \(p \equiv 1 \mod 4\), the matrix \(H' = [H^*_X \ H^*_Z]\) is commutative and has rank \(p - 1\).

**Proof:** Let \(H'_Y = H'_X + H'_Z\). Since \(H'_Y H'_Y^T + H'_Z H'_Z^T = (H'_X + H'_Z) H'^T_X H'_X^T + H'_Z H'_Z^T = H'_X H'_X^T + H'_Z H'_Z^T\), the matrix \(H'_Y \ H'_Z\) is commutative if and only if the matrix \([H'_Y \ H'_Z]\) is commutative. Note that \(H'_Y\) is of the form

\[
H'_Y = \begin{bmatrix}
0 & 1 & \cdots & 1 \\
1 & 0 & \cdots & 1 \\
\vdots & \vdots & \ddots & \vdots \\
1 & 1 & \cdots & 0
\end{bmatrix}
\]

where \(J_p\) and \(I_p\) are the \(p \times p\) all-1 matrix and the \(p \times p\) identity matrix, respectively. Denote the \(i\)-th row vectors of \(H^*_X\) and \(H^*_Z\) by \(\alpha_i\) and \(\beta_i\), respectively. Since \(\alpha_i\) and \(\beta_i\) are the \(i\)-th right cyclic shifts of the indicator vectors of all nonzero elements and all nonresidues in \(GF(q)\), respectively, the inner product \(\alpha_i \cdot \beta_i\)
of $\alpha_i$ and $\beta_j$ is equal to the sum of $|N|$ 1's modulo 2, where $|N|$ is the size of the nonresidue set $N$. When $p \equiv 1 \mod 4$, $|N|$ is an even number so that $\alpha_i + \beta_j = 0$ for all $0 \leq i \leq p - 1$. Note that $\alpha_i + \alpha_j = 0 \cdot \cdots \cdot 010 \cdots 010 \cdots 0$ with two 1's at the $i$th and the $j$th positions when $i \neq j$. The matrix $[H'_Y | H'_Z]$ is commutative if and only if $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$ for all $0 \leq i, j \leq p - 1$. Since $\alpha_i \cdot \beta_i = 0$, we have

$$\alpha_i \cdot \beta_i + \beta_i \cdot \alpha_i = 0$$

for all $0 \leq i \leq p - 1$. And for $i \neq j$, $0 \leq i, j \leq p - 1$

$$\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = (\alpha_i + \alpha_j) \cdot (\beta_i + \beta_j) = (H'_Z)_{i,i} + (H'_Z)_{j,j} + (H'_Z)_{i,j} + (H'_Z)_{j,i} = 0$$

since $H'_Z$ is symmetric by Lemma 13 and $(H'_Z)_{i,i} = b_0 = 0$ for all $i$. This proves that $[H'_Y | H'_Z]$ is commutative and then $[H'_Y | H'_Z] | H'_Z$ is commutative too. Since $[H'_Y | H'_Z]$ can be obtained from $[H'_X | H'_Z]$ by elementary column operations, the rank of $[H'_X | H'_Z]$ is the same as that of $[H'_Y | H'_Z]$. We note that the sum of any even number of rows of $H'_Y$ is a non-zero vector since the component of the sum is nonzero in a position at which a zero component appears in any of its summands. And except the sum of all rows of $H'_Y$, which is the zero vector, the sum of any odd number of rows of $H'_Y$ is also a non-zero vector since the component of the sum is nonzero in a position at which no zero component appears in any of its summands. Thus the rank of $H'_Y$ is $p - 1$, which implies that the rank of $[H'_Y | H'_Z]$ is at least $p - 1$. Since $|N|$ is an even number, the sum of all rows of $H'_Z$ is the zero vector so that the sum of all rows of the matrix $[H'_Y | H'_Z]$ is the zero vector, which implies that the rank of $[H'_Y | H'_Z]$ is at most $p - 1$. We then conclude that the rank of the matrix $[H'_Y | H'_Z]$ is $p - 1$ so that the rank of the matrix $[H'_X | H'_Z]$ is also $p - 1$.

Now from the above theorem, the matrix $H = [H'_X | H'_Z]$ obtained by removing the last row of the matrix $[H'_X | H'_Z]$ becomes to a check matrix of a $[[p, 1, d]]$ quantum stabilizer code, where the minimum distance $d$ is to be determined.

In [10], the quadratic residue related quantum codes with $p \equiv 5 \mod 8$ are special cases of above theorem. Parameters of several quantum codes constructed from Theorem 14 are given in Table IV. The minimum distances of these codes are determined by computer search. When considered as classical parity-check matrices, the check matrices of these quadratic residue related quantum codes are observed to have classical minimum distances exactly the same as their corresponding quantum minimum distances. Note that the minimum distance of the quantum codes in Table IV with $p \equiv 5 \mod 4$, $p \equiv 13 \mod 4$, $p \equiv 17 \mod 4$, and $p \equiv 29 \mod 4$ achieves the upper bound in [16]. However, the minimum distance of a generic quantum code from Theorem 14 is still not known yet.

**B. A General Construction for Stabilizer Codes With $k - 1$**

Inspired by the proof of Theorem 14, we give a construction of $[[n, l]]$ quantum stabilizer codes for general $n$ in this section. Let $g = (a_0, a_1, \cdots, a_{n-1})$ be a binary vector of length $n$, odd or even, with $a_0 = 0$ and $a_i = a_{n-i} = a_{n-i \mod n}$ for $1 \leq i \leq \frac{n-1}{2}$. Let

$$H'_X = \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1+1 \end{bmatrix} = \begin{bmatrix} I_{n-1} \\ \cdots \\ \cdots \\ \cdots \\ 0 \\ 0 \end{bmatrix}$$

with $(H'_X)_{i,i} = (H'_X)_{n-1,i} = 1$ for $0 \leq i \leq n - 2$ and $(H'_X)_{i,j} = 0$ otherwise. And let $H'_Z$ be an $n \times n$ binary matrix with $(H'_Z)_{i,j} = a_{(j+1)\mod n} + a_{(j-1)\mod n}$ for $0 \leq i, j \leq n - 1$, i.e.

$$H'_Z = \begin{bmatrix} a_1 + a_0 & a_2 + a_1 & \cdots & a_{n-1} + a_{n-2} & a_0 + a_{n-1} \\ a_1 + a_{n-1} & a_2 + a_0 & \cdots & a_{n-1} + a_{n-3} & a_0 + a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 + a_2 & a_2 + a_3 & \cdots & a_{n-1} + a_0 & a_0 + a_1 \\ a_1 + a_1 & a_2 + a_2 & \cdots & a_{n-1} + a_{n-1} & a_0 + a_0 \\ a_1 + a_{n-1} & a_2 + a_2 & \cdots & a_{n-1} + a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 + a_2 & a_2 + a_3 & \cdots & a_{n-1} & a_1 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

Since the last row of the matrix $[H'_X | H'_Z]$ is the zero vector, the rank of $[H'_X | H'_Z]$ is at most $n - 1$. Since the rank of $H'_Y$ is $n - 1$, the rank of $[H'_Y | H'_Z]$ is at least $n - 1$. Thus the matrix $[H'_X | H'_Z]$ has rank $n - 1$. Let $\alpha_i$ and $\beta_j$ be the $i$th rows of $H'_X$ and $H'_Y$, respectively. The commutativity of $[H'_X | H'_Z]$ can be justified as follows. For $0 \leq i \leq n - 1$

$$\alpha_i \cdot \beta_j - a_{(i+1)\mod n} + a_0 + a_0 + a_{(i+1)\mod n} - 0$$

which implies that $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$, and for $i \neq j$, $0 \leq i, j \leq n - 1$

$$\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = (a_0 + a_1) \cdot (\beta_i + \beta_j) = (0 \cdots 010 \cdots 010 \cdots 0) \cdot (\beta_i + \beta_j) = (H'_Z)_{i,i} + (H'_Z)_{j,j} + (H'_Z)_{i,j} + (H'_Z)_{j,i} = a_{(i+1)\mod n} + a_{(j+1)\mod n} + a_{(j-1)\mod n} + a_{(i-j)\mod n}$$

Again the matrix $H = [H'_X | H'_Z]$ obtained by removing the last row of the matrix $[H'_X | H'_Z]$ becomes to a check matrix of an $[[n, 1, d]]$ quantum stabilizer code, where the minimum distance $d$ is to be determined.

It is observed that the quadratic residue related quantum codes for prime numbers $p \equiv 1 \mod 4$ in the last subsection can be constructed in this way with $g = (a_0, a_1, \cdots, a_{p-1})$.
being the indicator vector of the quadratic non-residues. Some quantum codes achieving the upper bound in [16] can be constructed in this way. For example, when \( n = 17 \), each of the following four vectors
\[
0111010011010110, \quad 0110010111111100110, \\
010101011110110001, \quad 0111100000111101
\]
generates a \([17, 1, 7]\) quantum stabilizer code that achieves the upper bound in [16]. A \([17, 1, 7]\) quantum stabilizer code can be constructed by quantum BCH codes in [24], [25]. However, the above four vectors are found by computer search. In general, it is difficult to determine a well-performed vector \( q \) and the minimum distance of the resulted quantum code efficiently.

VI. CONCLUSION

In this paper, a simple stabilizer code construction is proposed based on syndrome assignment by classical parity-check matrices. The construction of quantum stabilizer codes can then be converted to the construction of classical binary linear block codes with commutative parity-check matrices. The asymptotic coding performance of this construction is shown to be promisingly at least comparable to that of the CSS construction. Note that only nondegenerate codes are studied in this paper since the method of syndrome assignment is unnatural for degenerate codes.

With the proposed code construction, the designed minimum distance \( 2t^* + 1 \) of the constructed quantum stabilizer codes can be achieved by a commutative classical parity-check matrix with classical minimum distance \( 4t^* - m \), where the parameter \( m, 0 \leq m < 2t^* \), depends on a property of the parity-check matrix. As \( m \) decreases, there is an increasing set of additional correctable error operators beyond the designed error correcting capability \( t^* \). Thus with a commutative parity-check matrix having \( m = 2t^* \), a designed quantum minimum distance \( d \geq 2t^* + 1 \) can be achieved by a classical minimum distance \( d' \geq 2t^* \). This is explicitly illustrated in the diagonal construction and the \([n, n-r] \) construction with/without permutation as well as the best quantum circulant codes and quadratic residue related quantum codes.

Permutation matrices may help transform non-commutative parity-check matrices to commutative ones and/or increase the minimum distance of the constructed quantum codes. However, for a given parity-check matrix \( H \), it remains open to find an effective permutation matrix \( P \) such that \( HP \) is commutative and/or corresponds to a code with greater minimum distance.

We have constructed a family of stabilizer codes from classical binary Reed–Muller codes with performance comparable to that of the CSS construction. We have also investigated sufficient conditions for permutation matrices to be able to increase the minimum distance of our constructed quantum Reed–Muller codes by half. We have also proposed a specific kind of effective permutations and showed that they meet the sufficient conditions for stabilizer codes constructed from the \( RM(1, m + 1) \) Reed–Muller codes. However, the search for an effective permutation for a general \( RM(r, m) \) with \( 2 \leq r \) and \( 2r < m \) is still an open problem.

With the circuit construction, the best quantum circulant codes constructed include many optimal quantum stabilizer codes in terms of their coding parameters. When the generators of quantum circulant codes are indicator vectors of quadratic residue and nonresidue sets, the constructed quadratic-residue related quantum codes are often optimal, although their quantum minimum distance is hard to determine as in the classical case. Finally, inspired by the construction of quadratic-residue related quantum codes, a construction of \([n, 1]\) quantum stabilizer codes for general \( n \) is proposed. By computer search, this construction yields quite a few optimal codes, which shows that this method is promising.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their valuable comments and suggestions that helped improve the presentation of this paper.

REFERENCES

[1] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” Phys. Rev. A, vol. 52, no. 4, pp. 2493–2496, 1995.
[2] A. M. Steane, “Error correcting codes in quantum theory,” Phys. Rev. Lett., vol. 77, no. 5, pp. 793–797, 1996.
[3] A. M. Steane, “Simple quantum error-correcting codes,” Phys. Rev. A, vol. 54, no. 6, pp. 4741–4751, 1996.
[4] A. Ekert and C. Macchiavello, “Quantum error-correction for communication,” Phys. Rev. Lett., vol. 77, no. 12, pp. 2585–2588, 1996.
[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, “Mixed state entanglement and quantum error correction,” Phys. Rev. A vol. 54, no. 5, pp. 3824–3851, 1996 [Online]. Available: http://arxiv.org/abs/quant-ph/9604024
[6] E. Knill and R. Laflamme, “A theory of quantum error-correcting codes,” Phys. Rev. A, vol. 55, no. 2, pp. 900–911, 1997.
[7] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” Phys. Rev. A vol. 54, no. 2, pp. 1098–1105, 1996 [Online]. Available: http://arxiv.org/abs/quant-ph/9512032
[8] A. M. Steane, “Multiple particle interference and quantum error correction,” in Proc. R. Soc. London A, 1996, vol. 452, pp. 2551–2576 [Online]. Available: http://arxiv.org/abs/quant-ph/9601029, 1996 [Online]. Available:
[9] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum hamming bound,” Phys. Rev. A vol. 54, no. 3, pp. 1862–1868, 1996 [Online]. Available: http://arxiv.org/abs/quant-ph/9604038
[10] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction and orthogonal geometry,” Phys. Rev. Lett. vol. 78, no. 3, pp. 405–408, 1997 [Online]. Available: http://arxiv.org/abs/quant-ph/9605005
[11] D. Gottesman, “Stabilizer Codes and Quantum Error Correction” Ph.D. dissertation, Calif. Inst. Technol., Pasadena, CA, 1997 [Online]. Available: http://arxiv.org/abs/quant-ph/9705052
[12] A. M. Steane, “Enlargement of Calderbank-Shor-Steane quantum codes,” IEEE Trans. Inf. Theory vol. 45, no. 7, pp. 2492–2495, 1999 [Online]. Available: http://arxiv.org/abs/quant-ph/9802061
[13] T. Brun, I. Devetak, and M.-H. Hsieh, “Correcting quantum errors with entanglement,” Science, vol. 314, pp. 436–439, 2006.
[14] T. Brun, I. Devetak, and M.-H. Hsieh, “Catalytic Quantum Error Correction 2006” [Online]. Available: http://arxiv.org/abs/quant-ph/0608007
[15] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[16] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over GF(4),” IEEE Trans. Inf. Theory vol. 44, no. 4, pp. 1369–1387, 1998 [Online]. Available: http://arxiv.org/abs/quant-ph/9608006
[17] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, “Ghz extraction yield for multipartite stabilizer states,” J. Math. Phys., vol. 47, p. 062106, 2006.
[18] S. Bravyi, D. Fattal, and D. Gottesman, “Ghz extraction yield for multipartite stabilizer states,” J. Math. Phys., vol. 314, pp. 436–439, 2006.
[19] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland, 1977.
[20] J. H. van Lint, Introduction to Coding Theory. New York: Springer-Verlag, 1982.
[21] J. Preskill, *Physics 229: Advanced Mathematical Methods of Physics—Quantum Computation and Information*. Pasadena: Calif. Inst. Technol., 1998.

[22] A. M. Steane, “Quantum Reed–Muller codes,” *IEEE Trans. Inf. Theory* vol. 45, no. 5, pp. 1701–1703, 1999 [Online]. Available: http://arxiv.org/abs/arXiv:quant-ph/9608026

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

[24] M. Grassl and T. Beth, “Quantum BCH codes,” in *Proc. X. Int. Symp. Theoret. Elect. Eng.*, Magdeburg, 1999, pp. 207–212 [Online]. Available: http://arxiv.org/abs/quant-ph/9910060

[25] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, “Primitive quantum BCH codes over finite fields,” in *Proc. IEEE ISIT’2006*, pp. 1105–1108 [Online]. Available: http://arxiv.org/abs/quant-ph/0501126

Ching-Yi Lai received the B.S. degree in 2004 and M.S. degree in 2006 from the Department of Electrical Engineering, National Tsing Hua University, Taiwan. He is currently a Ph.D. student in the Communication Sciences Institute, Electrical Engineering Department, University of Southern California. His research interests include quantum computation and quantum information, especially on quantum error-correcting codes and fault-tolerant quantum computation.

Chung-Chin Lu (S’86–M’88) received the B.S. degree from National Taiwan University, Taiwan, in 1981 and the Ph.D. degree from the University of Southern California, in 1987, both in electrical engineering. Since 1987, he has been with the Department of Electrical Engineering, National Tsing Hua University, Taiwan. He is currently a professor. His current research interests include coding theory, digital communications, bioinformatics, and quantum communications.