Duality in Entanglement-Assisted Quantum Error Correction

Ching-Yi Lai, Todd A. Brun, *Senior Member, IEEE*, and Mark M. Wilde, *Member, IEEE*

***Abstract*—The dual of an entanglement-assisted quantum error-correcting (EAQEC) code is defined from the orthogonal group of a simplified stabilizer group. From the Poisson summation formula, this duality leads to the MacWilliams identities and linear programming bounds for EAQEC codes. We establish a table of upper and lower bounds on the minimum distance of any maximal-entanglement EAQEC code with length up to 15 channel qubits.**

***Index Terms*—Entanglement-assisted quantum error correction (EAQEC), linear programming bound, MacWilliams identity, quantum dual code.**

I. Introduction

THE theory of quantum error correction underpins the practical realization of quantum computation and quantum communication [1]–[6]. Quantum stabilizer codes are an extensively analyzed class of quantum error-correcting codes because their encoding, decoding, and recovery are straightforward to describe using their algebraic properties [7]–[10].

Entanglement-assisted quantum error correction (EAQEC) is a paradigm in which the sender and receiver share entanglement before quantum communication begins [11]. An $[[n, k, d; c]]$ EAQEC code encodes k information qubits into n channel qubits with the help of c pairs of maximally entangled Bell states. The code can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors acting on the n channel qubits, where d is the minimum distance of the code. Standard stabilizer codes are a special case of EAQEC codes with $c = 0$, and we use the notation $[[n, k, d]]$ for such codes.

Bowen proposed the first EAQEC code [12], which is equivalent to the well-known five-qubit code [13]. Fattal *et al.* established a technique for handling entanglement in the stabilizer formalism [14]. Brun *et al.* then devised the entanglement-assisted (EA) stabilizer formalism and showed how to transform any $[n, k, d]$ classical quaternary code[1] into an $[[n, 2k - n + c, d; c]]$ EAQEC code, where c depends on the properties of the classical code [15]. Lai and Brun further explored the properties of EAQEC codes and proposed an optimization method to find optimal EAQEC codes that cannot be obtained by the aforementioned construction [16]. By optimal, we mean that d is the highest achievable minimum distance for given parameters n, k, and c.

In classical coding theory, a well-established notion is that of a dual code. Suppose that $\mathcal{C}$ is an $[n, k]$ linear code over an arbitrary field $\mathrm{GF}(q)$ with a generator matrix G and a corresponding parity check matrix H such that $HG^T = 0$. The dual code of $\mathcal{C}$ is the $[n, k' = n - k]$ linear code $\mathcal{C}^\perp$ with H as a generator matrix and G as a parity check matrix. The dimensions of the code $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$ satisfy the relation $k + k' = n$. It is well known that the MacWilliams identity gives a relationship between the weight enumerator of $\mathcal{C}$ and the weight enumerator of its dual code $\mathcal{C}^\perp$[17], which can be used to determine the minimum distance of the dual code $\mathcal{C}^\perp$, given the weight enumerator of $\mathcal{C}$.

The MacWilliams identity for quantum codes connects the weight enumerator of a classical quaternary self-orthogonal code associated with the quantum code to the weight enumerator of its dual code [18]–[21]. This leads to the linear programming bounds (upper bound) on the minimum distance of quantum codes. We will show that this type of MacWilliams identity for quantum stabilizer codes can be directly obtained by applying the Poisson summation formula from the theory of orthogonal groups. However, the orthogonal group of a stabilizer group with respect to the symplectic inner product (which will be defined later) does not define another quantum stabilizer code. So this is not a duality between codes in the usual quantum case.

In this paper, we define a notion of duality in EAQEC based on the theory of orthogonal groups, and this notion of duality bears more similarity to the classical notion of duality because the orthogonal group of an EA code forms a nontrivial EA quantum code. We then show how a quantum analog of the MacWilliams identity and the linear programming bound for EAQEC codes follow in a natural way. We apply the EAQEC code constructions from [11], [16], and [22] to find good EAQEC codes with maximal entanglement for $n \leq 15$. Combining the results of the linear programming bounds, we give a table of upper and lower bounds on the highest achievable

Manuscript received April 29, 2011; revised April 20, 2012; accepted October 25, 2012. Date of publication February 08, 2013; date of current version May 15, 2013. T. A. Brun and C.-Y. Lai were supported in part by the National Science Foundation under Grant CCF-0830801. M. M. Wilde was supported by the MDEIE (Québec) PSR-SIIRI International Collaboration Grant. This paper was presented at the 14th Workshop on Quantum Information Processing, Singapore, January 2011.

C.-Y. Lai and T. A. Brun are with the Communication Sciences Institute, Electrical Engineering Department, University of Southern California, Los Angeles, CA 90089 USA (e-mail: laiching@usc.edu; tbrun@usc.edu).

M. M. Wilde is with the School of Computer Science, McGill University, Montreal, QC H3A 2A7, Canada (e-mail: mwilde@gmail.com).

Communicated by J.-P. Tillich, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2013.2246274

[1]An $[n, k, d]$ classical linear code over a certain field encodes k information digits into n digits, where d is its minimum distance.

minimum distance of any maximal-entanglement EAQEC code[2] for $n \leq 15$.

We organize this paper as follows. We first review some basics of EA quantum codes in Section II. In Section III, we define the dual of an EAQEC code. The MacWilliams identity for EAQEC codes and the linear programming bound for EAQEC codes are derived in Section IV, followed by a table of upper and lower bounds on the minimum distance of any EAQEC code with maximal entanglement and $n \leq 15$. The final section concludes with a summary and future questions.

II. Review of EAQEC Codes

We begin with some notation. The Pauli matrices

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

form a basis of the space of linear operators on a 2-D single-qubit state space $\mathcal{H}$. Let

$$\mathcal{G}_n = \{eM_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}, e \in \{\pm 1, \pm i\}\}$$

be the n-fold Pauli group. We use the notation X_j, Y_j, or Z_j to denote a Pauli operator on qubit number j. We define $X^u = \prod_{i:u_i=1} X_i$ for some binary n-tuple $u = (u_1 \cdots u_n)$ and similarly $Z^v = \prod_{j:v_j=1} Z_j$ for some binary n-tuple $v = (v_1 \cdots v_n)$. Any element $g = eM_1 \otimes \cdots \otimes M_n \in \mathcal{G}_n$ can be expressed as $g = e' X^u Z^v$ for some $e' \in \{\pm 1, \pm i\}$ and two binary n-tuples u and v. The weight $\mathrm{wt}(g)$ of g is the number of M_j's that are not equal to the identity operator I. Since the overall phase of a quantum state is not important, we consider the quotient of the Pauli group by its center $\bar{\mathcal{G}}_n = \mathcal{G}_n / \{\pm 1, \pm i\}$, which is an Abelian group and can be generated by a set of $2n$ independent generators. For $g_1 = X^{u_1} Z^{v_1}$, $g_2 = X^{u_2} Z^{v_2} \in \bar{\mathcal{G}}_n$, the symplectic inner product $*$ in $\bar{\mathcal{G}}_n$ is defined by

$$g_1 * g_2 = u_1 \cdot v_2 + u_2 \cdot v_1 \bmod 2$$

where $\cdot$ is the usual inner product for binary n-tuples. Note that $*$ is commutative. We define a map $\phi : \mathcal{G}_n \to \bar{\mathcal{G}}_n$ by $\phi(eX^u Z^v) = X^u Z^v$. For $g, h \in \mathcal{G}_n$, $\phi(g) * \phi(h) = 0$ if they commute, and $\phi(g) * \phi(h) = 1$, otherwise. The orthogonal group of a subgroup V of $\bar{\mathcal{G}}_n$ with respect to $*$ is

$$V^{\perp} = \{g \in \bar{\mathcal{G}}_n : g * h = 0, \forall h \in V\}.$$

For example, consider a stabilizer group $\mathcal{S}$, which is an Abelian subgroup of $\mathcal{G}_n$ and does not contain the negative identity operator $-I$. Then, the orthogonal group of $\phi(\mathcal{S})$ is $(\phi(\mathcal{S}))^{\perp} = \phi(\mathcal{N}(\mathcal{S}))$, where $\mathcal{N}(\mathcal{S})$ is the normalizer group of $\mathcal{S}$.

An $[[n, k, d]]$ stabilizer code is a 2^k-dimensional subspace of the n-qubit Hilbert space $\mathcal{H}^{\otimes n}$, and is the joint $+1$-eigenspace of $n-k$ independent generators of a stabilizer subgroup $\mathcal{S}$ of $\bar{\mathcal{G}}_n$. The minimum distance d is the minimum weight of any element in $\phi(\mathcal{N}(\mathcal{S})) \setminus \phi(\mathcal{S})$.

In the scheme of EAQEC codes [11], [16], Alice and Bob share c maximally entangled pairs $|\Phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Suppose Alice tries to send a k-qubit state $|\phi\rangle$ to Bob through a noisy channel, using an additional $n-k-c$ ancilla qubits in the state $|0\rangle$. We assume that Bob's qubits suffer no errors since they do not pass through the noisy channel. Let $J = (J^i, J^e, J^a)$ be the set of positions of the information qubits, the entangled pairs, and the ancilla qubits on Alice's side, respectively. For example, if the initial state is $|\phi\rangle|\Phi_+\rangle_{AB}^{\otimes c}|0\rangle^{\otimes n-k-c}$, we have $J^i = \{1, \ldots, k\}$, $J^e = \{k+1, \ldots, k+c\}$, and $J^a = \{k+c+1, \ldots, n\}$. Then, Alice applies a *Clifford encoder* U on her n qubits to protect the information qubits. A Clifford encoder is a unitary operator that maps elements $\bar{\mathcal{G}}_n$ to elements of $\bar{\mathcal{G}}_n$ under unitary conjugation. An $[[n, k, d; c]]$ EAQEC code is defined by the pair (U, J), where d is the minimum distance and will be defined later. For convenience, let $g_j = UZ_jU^{\dagger}$ and $h_j = UX_jU^{\dagger}$ for $j = 1, \ldots, n$ in $\bar{\mathcal{G}}_n$. The encoded state associated with (U, J) has a set of stabilizer generators

$$\begin{aligned} \{&g^A_{J^e_1} \otimes Z^B_1, \ldots, g^A_{J^e_c} \otimes Z^B_c, \\ &h^A_{J^e_1} \otimes X^B_1, \ldots, h^A_{J^e_c} \otimes X^B_c, \\ &g^A_{J^a_1} \otimes I^B, \ldots, g^A_{J^a_{n-k-c}} \otimes I^B\} \end{aligned}$$

in $\bar{\mathcal{G}}_{n+c}$, where the superscript A or B indicates that the operator acts on the qubits of Alice or Bob, respectively, and J^x_j denotes the jth element in the set J^x. Since Bob's qubits are error-free, we only consider the operators on Alice's qubits. The simplified stabilizer subgroup $\mathcal{S}'$ associated with the pair (U, J) of $\bar{\mathcal{G}}_n$ is

$$\mathcal{S}' = \langle g_{J^e_1}, \ldots, g_{J^e_c}, h_{J^e_1}, \ldots, h_{J^e_c}, g_{J^a_1}, \ldots, g_{J^a_{n-k-c}} \rangle.$$

Note that the commutation relations are as follows:

$$g_i * g_j = 0 \quad \text{for all } i \text{ and } j \tag{1}$$

$$h_i * h_j = 0 \quad \text{for all } i \text{ and } j \tag{2}$$

$$g_i * h_j = 0 \quad \text{for } i \neq j \tag{3}$$

$$g_i * h_i = 1 \quad \text{for all } i. \tag{4}$$

We say that g_j and h_j are *symplectic partners* for $j \in J^i \cup J^e$. The logical subgroup $\mathcal{L}$ associated with the pair (U, J) of the encoded state is

$$\mathcal{L} = \langle g_j, h_j, j \in J^i \rangle.$$

The symplectic subgroup $\mathcal{S}_S$ associated with the pair (U, J) of $\mathcal{S}'$ is the subgroup generated by the c pairs of symplectic partners of $\mathcal{S}'$:

$$\mathcal{S}_S = \langle g_j, h_j, j \in J^e \rangle.$$

The isotropic subgroup $\mathcal{S}_I$ associated with the pair (U, J) of $\mathcal{S}'$ is the subgroup generated by the generators g_i of $\mathcal{S}'$. Therefore, $g_i * g = 0$ for all g in $\mathcal{S}'$:

$$\mathcal{S}_I = \langle g_j, j \in J^a \rangle.$$

Notice that $\mathcal{S}' = \mathcal{S}_S \times \mathcal{S}_I$ in $\bar{\mathcal{G}}_n$. The minimum distance d of the EAQEC code is the minimum weight of any element in $\mathcal{S}'^{\perp} \setminus \mathcal{S}_I$.

[2]One might wonder why we are considering EAQEC codes that exploit the maximum amount of entanglement possible, given that noiseless entanglement could be expensive in practice. But there is good reason for doing so. The so-called father protocol is a random EA quantum code [23], [24], and it achieves the EA quantum capacity of a depolarizing channel (the EA hashing bound [12], [25]) by exploiting maximal entanglement. Furthermore, there is numerical evidence that maximal-entanglement turbo codes come within a few decibels of achieving the EA hashing bound [26].

III. Duality in EAQEC Codes

Observe that the orthogonal group of $\mathcal{S}' = \mathcal{S}_S \times \mathcal{S}_I$ associated with the pair $(U, J = (J^i, J^e, J^a))$ in $\bar{\mathcal{G}}_n$ is $\mathcal{L} \times \mathcal{S}_I$. That is,

$$\mathcal{L} \times \mathcal{S}_I = (\mathcal{S}_S \times \mathcal{S}_I)^{\perp}.$$

We can define another EAQEC code with logical subgroup $\mathcal{S}_S$, symplectic subgroup $\mathcal{L}$, and isotropic subgroup $\mathcal{S}_I$ associated with the pair $(U, J' = (J^e, J^i, J^a))$.

The number of a set of independent generators of $\mathcal{S}_S \times \mathcal{S}_I$ is $K = 2c + (n - k - c) = n - k + c$, and the number of a set of independent generators of its orthogonal group $\mathcal{L} \times \mathcal{S}_I$ is $K' = 2k + (n - k - c) = n + k - c$. These parameters satisfy the following relation:

$$K + K' = 2n = N$$

where N is the number of a set of independent generators of the full Pauli group $\bar{\mathcal{G}}_n$. This equation is parallel to the classical duality between a code and its dual code, which motivates the definition of the dual code of an EAQEC code as follows.

Definition 1: The dual of an $[[n, k, d; c]]$ EAQEC code, defined by a simplified stabilizer group $\mathcal{S}' = \mathcal{S}_S \times \mathcal{S}_I$ and a logical group $\mathcal{L}$ associated with the pair $(U, J = (J^i, J^e, J^a))$, is the $[[n, c, d'; k]]$ EAQEC code associated with the pair $(U, J' = (J^e, J^i, J^a))$, where $\mathcal{L} \times \mathcal{S}_I$ is the simplified stabilizer group and $\mathcal{S}_S$ is the logical group for some minimum distance d'.

When $c = n-k$, we call such a code a *maximal-entanglement* EAQEC code. In this case, $\mathcal{S}_I$ is the trivial group that contains only the identity, and the simplified stabilizer group is $\mathcal{S}_S$. Its dual code is a maximal-entanglement EAQEC code defined by the logical group $\mathcal{L}$.

When $c = 0$, the code is a standard stabilizer code, with a stabilizer group $\mathcal{S} = \mathcal{S}_I = \langle g_j, j \in J^a \rangle$, and a logical group $\mathcal{L} = \langle g_j, h_j, j \in J^i \rangle$. $\mathcal{S}_S$ is the trivial group in this case. The simplified stabilizer group $\mathcal{L}$ defines an $[[n, 0, d', k]]$ EAQEC code—that is, a single entangled stabilizer state that encodes no information.

IV. MacWilliams Identity and the Linear Programming Bounds

The MacWilliams identity for general quantum codes can be obtained from the general theory of classical additive codes as indicated in [8] or by applying the Poisson summation formula from the theory of orthogonal groups [27].

Theorem 2: Suppose $W_V(x, y) = \sum_{w=0}^{n} B_w x^{n-w} y^w$ and $W_{V^\perp}(x, y) = \sum_{w'=0}^{n} A_{w'} x^{n-w'} y^{w'}$ are the weight enumerators of a subgroup V of $\bar{\mathcal{G}}_n$ and its orthogonal group $V^\perp$ in $\bar{\mathcal{G}}_n$. Then

$$W_V(x, y) = \frac{1}{|V^\perp|} W_{V^\perp}(x + 3y, x - y) \tag{5}$$

or equivalently

$$B_w = \frac{1}{|V^\perp|} \sum_{w'=0}^{n} P_w(w', n) A_{w'}, \text{ for } w = 0, \ldots, n \tag{6}$$

where $P_w(w', n) = \sum_{u=0}^{w} (-1)^u 3^{w-u} \binom{w'}{u} \binom{n-w'}{w-u}$ is the Krawtchouk polynomial [17].

Applying Theorem 2 to the simplified stabilizer group $\mathcal{S}_S \times \mathcal{S}_I$ and the isotropic subgroup $\mathcal{S}_I$, respectively, we obtain the MacWilliams Identity for EAQEC codes.

Corollary 3: The MacWilliams identities for EAQEC codes are as follows:

$$W_{\mathcal{L} \times \mathcal{S}_I}(x, y) = \frac{1}{|\mathcal{S}_S \times \mathcal{S}_I|} W_{\mathcal{S}_S \times \mathcal{S}_I}(x + 3y, x - y) \tag{7}$$

$$W_{\mathcal{S}_I}(x, y) = \frac{1}{|\mathcal{L} \times \mathcal{S}_S \times \mathcal{S}_I|} W_{\mathcal{L} \times \mathcal{S}_S \times \mathcal{S}_I}(x + 3y, x - y). \tag{8}$$

The significance of the MacWilliams identities is that linear programming techniques can be applied to find upper bounds on the minimum distance of EAQEC codes. For an $[[n, k, d; n-k]]$ EAQEC code, $\mathcal{S}_I$ is trivial and the minimum distance is the minimum weight of any element in the logical subgroup $\mathcal{L}$. We must have $B_w = 0$ for $w = 1, \ldots, d - 1$. If we cannot find any solutions to an integer program with the following constraints:

$$\begin{aligned}
&A_0 = B_0 = 1;\\
&A_w \geq 0, B_w \geq 0, \text{ for } w = 1, \ldots, n;\\
&A_w \leq |\mathcal{S}_S|, B_w \leq |\mathcal{L}|, \text{ for } w = 1, \ldots, n;\\
&\sum_{w=0}^{n} A_w = |\mathcal{S}_S|, \sum_{w=0}^{n} B_w = |\mathcal{L}|;\\
&B_w = \frac{1}{|\mathcal{S}_S|} \sum_{w'=0}^{n} P_w(w', n) A_{w'}, \text{ for } w = 0, \ldots, n;\\
&B_w = 0, \text{ for } w = 1, \ldots, d - 1;
\end{aligned}$$

for a certain d, this result implies that there is no $[[n, k, d; n-k]]$ EAQEC code. If d^* is the smallest of such d's, then $d^* - 1$ is an upper bound on the minimum distance of an $[[n, k, d; n - k]]$ EAQEC code. This bound is called the linear programming bound for EAQEC codes.

For $0 < c < n - k$, both $\mathcal{S}_I$ and $\mathcal{S}_S$ are nontrivial. The minimum distance is the minimum weight of any element in $\mathcal{S}_I \times \mathcal{L} \backslash \mathcal{S}_I$. We need constraints on both the weight enumerators of $\mathcal{S}_I \times \mathcal{S}_S$ and $\mathcal{S}_I$ from (7) and (8).

For $c = 0$, $V^\perp$ is the stabilizer group $\mathcal{S}$, V is the normalizer group of $\mathcal{S}$, and (5) gives the MacWilliams Identity for stabilizer codes [9], [18].

Now we can establish a table of upper and lower bounds on the minimum distance of maximal-entanglement EAQEC codes for $n \leq 15$. The upper bounds for $n \leq 15$ and $k \geq 2$ are from the linear programming bound, which is generally tighter than the singleton bound [11] and the Hamming bound for nondegenerate EAQEC codes [12]. The linear programming bounds are not necessarily tight, however. In some cases, they can be improved by other arguments. For instance, it can be proved that $[[n, 1, n; n-1]]$ and $[[n, n-1, 2; 1]]$ EAQEC codes do not exist for even n [28].

Lai and Brun proposed a construction of $[[n, 1, n; n-1]]$ EA repetition codes for n odd in [16]. By slightly modifying that construction, we construct $[[n, 1, n-1; n-1]]$ EA repetition codes for n even [28], which are optimal.

TABLE I
UPPER AND LOWER BOUNDS ON THE MINIMUM DISTANCE OF ANY $[[n, k, d; n-k]]$ MAXIMAL-ENTANGLEMENT EAQEC CODES

$n\backslash k$	1	2	3	4	5	6	7
3	3	2					
4	3	2-3	1				
5	5	3-4	2-3	2			
6	5	4	3-4	2	1		
7	7	5	4	3	2	2	
8	7	6	5	4	3	2	1
9	9	6-7	5-6	5	4	3	2
10	9	7-8	6-7	6	4-5	4	3
11	11	8	7-8	6-7	6	5	3-4
12	11	9	7-8	6-7	6-7	5-6	4-5
13	13	10	9	6-8	6-7	6-7	4-6
14	13	10-11	9-10	7-9	6-8	6-7	6-7
15	15	11-12	9-11	8-10	8-9	7-8	6-7

$n\backslash k$	8	9	10	11	12	13	14
9	2						
10	2	1					
11	3	2	2				
12	4	3	2	1			
13	4-5	4	3	2	2		
14	5-6	4-5	3-4	3	2	1	
15	6-7	5-6	4	3-4	2-3	2	2

The following codes are obtained by applying the EAQEC code construction from classical codes in [11]: $[[7, 2, 5; 5]]$, $[[9, 4, 5; 5]]$, $[[9, 5, 4; 4]]$, $[[10, 4, 6; 6]]$, $[[11, 5, 6; 6]]$, $[[11, 4, 6; 7]]$, $[[11, 6, 5; 5]]$, $[[12, 2, 9; 10]]$, $[[12, 8, 4; 4]]$, $[[12, 5, 6; 7]]$, $[[13, 2, 10; 11]]$, $[[13, 3, 9; 10]]$, $[[13, 6, 6; 7]]$, $[[14, 7, 6; 7]]$, $[[14, 8, 5; 6]]$, $[[15, 9, 5; 6]]$, $[[15, 8, 6; 7]]$. The following codes are from the circulant code construction in [16]: $[[7, 3, 4; 4]]$, $[[8, 2, 6; 6]]$, $[[10, 3, 6; 7]]$, $[[11, 3, 7; 8]]$, $[[15, 5, 8; 10]]$, $[[15, 6, 7; 9]]$. The following codes are obtained by transforming standard stabilizer codes into EAQEC codes in [22]: $[[6, 2, 4; 5]]$, $[[8, 4, 4; 4]]$, $[[9, 6, 3; 3]]$, $[[10, 6, 4; 4]]$, $[[10, 7, 3; 3]]$, $[[11, 8, 3; 3]]$, $[[12, 6, 5; 6]]$, $[[12, 7, 4; 5]]$, $[[12, 9, 3; 3]]$, $[[13, 5, 6; 8]]$, $[[13, 9, 4; 4]]$, $[[13, 10, 3; 3]]$, $[[14, 11, 3; 3]]$, $[[15, 4, 8; 11]]$, $[[15, 10, 4; 5]]$. These codes give lower bounds on the achievable distance for many values of n and k.

If an $[[n, k, d; c]]$ code exists, it can be shown that both an $[[n+1, k, d; c+1]]$ and an $[[n, k-1, d' \geq d; c+1]]$ code exist [28], which proves the existence of the following codes: $[[14, 3, 9; 11]]$, $[[14, 9, 4; 5]]$, $[[13, 8, 4; 5]]$, $[[14, 10, 3; 4]]$, $[[14, 6, 6; 8]]$, codes. We used MAGMA [29] to find the optimal quantum stabilizer codes, and then applied the encoding optimization algorithm in [16] to obtain the other lower bounds.

V. DISCUSSION

In this paper, we defined the dual code of an EAQEC code and derived the MacWilliams identities for EAQEC codes. Based on these identities, we found a linear programming bound on the minimum distance of an EAQEC code. We provided a table of upper and lower bounds on the minimum distance of maximal-entanglement EAQEC codes for $n \leq 15$. Most lower bounds in Table I are from the optimization algorithm [16]. To make the bounds in Table I tighter, we need to consider other code constructions to raise the lower bounds. We also plan to explore the existence of other $[[n, k, d; n-k]]$ codes to decrease the upper bound. Similar tables for EAQEC codes with $0 < c < n-k$ can be constructed by the same techniques.

Rains introduced the idea of the *shadow* enumerator of a quantum stabilizer code [30], which can be related to the weight enumerator of the stabilizer group similar to the MacWilliams identity. This relation provides additional constraints on the linear programming problem and can improve the linear programming bound for quantum codes. To introduce the "shadow enumerator" of an EAQEC code may be a potential way to improve on the linear programming bound.

ACKNOWLEDGMENT

We are indebted to an anonymous referee and Associate Editor Jean-Pierre Tillich for constructive comments on our manuscript. MMW acknowledges useful discussions with Omar Fawzi and Jan Florjanczyk.

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.
[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, 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.
[8] A. R. Calderbank, "Quantum error correction via codes over $GF(4)$," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998.
[9] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Inst. Technol., Pasadena, CA, USA, 1997.
[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.
[11] T. A. Brun, I. Devetak, and M.- H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436–439, 2006.
[12] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Phys. Rev. A*, vol. 66, pp. 052313-1–052313-8, 2002.
[13] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, no. 1, pp. 198–201, 1996.
[14] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, Entanglement in the stabilizer formalism 2004 [Online]. Available: http://arxiv.org/abs/quant-ph/0406168
[15] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Phys. Rev. A*, vol. 77, pp. 064302-1–064302-4, 2008.
[16] C.-Y. Lai and T. A. Brun, Entanglement Increases the error-correcting ability of quantum error-correcting codes 2010 [Online]. Available: http://arxiv.org/abs/1008.2598v1
[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
[18] P. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities for classical coding theory," *Phys. Rev. Lett.*, vol. 78, no. 8, pp. 1600–1602, Feb. 1997.
[19] E. M. Rains, "Quantum weight enumerators," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1388–1394, Jul. 1998.
[20] E. M. Rains, "Monotonicity of the quantum linear programming bound," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2489–2492, Nov. 1999.
[21] A. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1206–1215, May 1999.

[22] C.-Y. Lai and T. A. Brun, "Entanglement-assisted quantum error-correcting codes with imperfect ebits," *Phys. Rev. A*, vol. 86, p. 032319, Sep. 2012.
[23] I. Devetak, A. W. Harrow, and A. Winter, "A resource framework for quantum Shannon theory," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4587–4618, Oct. 2008.
[24] I. Devetak, "A family of quantum protocols," *Phys. Rev. Lett.*, vol. 93, no. 23, p. 230504, Dec. 2004.
[25] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Phys. Rev. Lett.*, vol. 83, no. 15, pp. 3081–3084, Oct. 1999.
[26] M. M. Wilde and M.-H. Hsieh, Entanglement-assisted quantum turbo codes 2010 [Online]. Available: http://arxiv.org/abs/1010.1256
[27] A. W. Knapp, *Basic Algebra*. Boston, MA, USA: Birkhauser, 2006.
[28] C.-Y. Lai, T. A. Brun, and M. M. Wilde, Dualiities and Identities for entanglement-assisted quantum codes 2010 [Online]. Available: http://arxiv.org/abs/1010.5506
[29] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbol. Comput.*, vol. 24, no. 3–4, pp. 235–265, 1993.
[30] E. M. Rains, "Quantum shadow enumerators," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2361–2366, Nov. 1999.

Ching-Yi Lai was born in Taipei, Taiwan. He received the B.S. degree in 2004 and the M.S. degree in 2006 from National Tsing Hua University in Taiwan, both in electrical engineering.

Currently, he is a Ph.D. student in the Communication Sciences Institute of the Electrical Engineering Department at the University of Southern California. His research interests include quantum error-correcting codes and fault-tolerant quantum computation.

Todd A. Brun (SM'10) was born in Hannibal, Missouri, USA. He received the A.B. degree in Physics from Harvard University in Cambridge, Massachusetts in 1989, the M.S. degree in Physics from Caltech in Pasadena, California in 1991, and the Ph.D. degree in Physics from Caltech in 1994.

Currently, he is Associate Professor of Electrical Engineering at the University of Southern California in Los Angeles, California. He is the author of almost 100 scientific papers, and co-editor (with Daniel A. Lidar) of the forthcoming book "Quantum Error Correction," to be published by Cambridge University Press. He does research on quantum computation, quantum information, error correction, and other aspects of quantum theory.

Prof. Brun is also a member of the American Physical Society and the American Mathematical Society. He has been an associate editor of IEEE TRANSACTIONS ON COMPUTERS, and of the *Journal of Computer and Systems Sciences*, and served on the editorial boards of *Physical Review A* and *Journal of Physics A*. He has served extensively as a referee for journals and conferences, and written many reviews of articles and books for *Mathematical Reviews*.

Mark M. Wilde (M'99) was born in Metairie, Louisiana, USA. He received the B.S. degree in computer engineering from Texas A&M University, College Station, Texas, in 2002, the M.S. degree in electrical engineering from Tulane University, New Orleans, Louisiana, in 2004, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, California, in 2008.

Currently, he is a Postdoctoral Fellow at the School of Computer Science, McGill University, Montreal, QC, Canada and will start in August 2013 as an Assistant Professor in the Department of Physics and Astronomy and the Center for Computation and Technology at Louisiana State University. He has published over 60 articles and preprints in the area of quantum information processing and is the author of the text "Quantum Information Theory," to be published by Cambridge University Press. His current research interests are in quantum Shannon theory and quantum error correction.

Dr. Wilde is a member of the American Physical Society and has been a reviewer for the IEEE TRANSACTIONS ON INFORMATION THEORY and the IEEE International Symposium on Information Theory.