Entanglement increases the error-correcting ability of quantum error-correcting codes

Ching-Yi Lai and Todd A. Brun

Phys. Rev. A **88**, 012320 — Published 19 July 2013

DOI: 10.1103/PhysRevA.88.012320

Entanglement Increases the Error-Correcting Ability of Quantum Error-Correcting Codes

Ching-Yi Lai* and Todd A. Brun†
Electrical Engineering Department,
University of Southern California,
Los Angeles, California, USA 90089.

If entanglement is available, the error-correcting ability of quantum codes can be increased. We show how to optimize the minimum distance of an entanglement-assisted quantum error-correcting (EAQEC) code, obtained by adding ebits to a regular quantum stabilizer code, over different encoding operators. By this encoding optimization procedure, we found several new EAQEC codes, including a family of entanglement-assisted (EA) quantum repetition codes and several *optimal* EAQEC codes.

I. INTRODUCTION

Since Shor proposed the first quantum error-correcting code [1], the theory of quantum error correction has been extensively developed. Today, quantum stabilizer codes [2–6] are the most widely-used class of quantum error-correcting codes. One reason for this is that the CSS and CRSS code constructions [2, 3, 7, 8] allow classical dual-containing binary or quaternary codes to be easily transformed into quantum stabilizer codes.

Bowen constructed an EAQEC code from a three-qubit bit-flip code with the help of two pairs of maximally-entangled states (ebits) [9]. He converted the two ancilla qubits to ebits and then applied a unitary transformation (another encoding operator) such that the EA code is equivalent to the five-qubit code [10, 11]. Bowen's code, which can correct an arbitrary one-qubit error, serves as an example that entanglement increases the error-correcting ability of quantum codes.

An $[n, k, d]$ classical linear quaternary code encodes k quaternary information digits into n quaternary digits and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ quaternary digit errors, where d is called the minimum distance of the code. Brun, Devetak and Hsieh showed that an $[n, k, d]$ classical linear quaternary code can be transformed to an $[[n, 2k-n+c, d; c]]$ EAQEC code that encodes $2k-n+c$ information qubits into n qubits with the help of c ebits for some c [12, 13]. This EAQEC code can correct at least $\lfloor \frac{d-1}{2} \rfloor$ qubit errors and has the same minimum distance d as the classical code or higher. If entanglement is used, it boosts the rate of the code. However, it has not been explored how entanglement can instead help increase the minimum distance. In addition, given parameters n, k, c, it is not clear how to construct an $[[n, k, d; c]]$ EAQEC code directly. We will answer these questions in this paper. We say that an $[[n, k, d; c]]$ EAQEC code is *optimal* if it saturates any upper bound on the minimum distance d for given n, k, c and that an $[[n, k, d; c]]$ EAQEC code is not equivalent to any regular quantum stabilizer code if there is no regular $[[n+c, k, d]]$ quantum code. We will construct several optimal EAQEC codes that are not equivalent to any regular quantum stabilizer codes

New EAQEC codes are constructed by adding ebits to a given regular stabilizer code. The minimum distance of these EAQEC codes can be optimized over distinct *unitary row operators* that determine the set of logical operators. We summarize the process in an encoding optimization procedure. If we add fewer than the maximum number of ebits, we have the freedom to choose the set of generators of the stabilizer group, and the freedom to replace different ancilla qubits with ebits. This leads to higher computational complexity. When $n + k$ becomes large, the encoding procedure is intractable, and we adopt a random optimization procedure instead.

Applying these optimization procedures to regular stabilizer codes, we construct several new EAQEC codes, including a family of EA quantum repetition codes, which are optimal and are not equivalent to any regular stabilizer code. Finally, we give a circulant construction of EAQEC codes to find EAQEC codes of small length. Some of our EAQEC codes exploit large numbers of ebits, though that much noiseless entanglement could be expensive in practice. However, there is evidence that EAQEC codes with maximal entanglement achieve the EA quantum capacity of a depolarizing channel [9, 14–17]. This establishes a limit on the performance of EAQEC codes and it is still worthwhile to study EAQEC codes with large numbers of ebits.

This paper is organized as follows. Basics of stabilizer codes and EAQEC codes are introduced in Section II. In Section III, we discuss the encoding optimization procedure by first considering the case of maximal entanglement and then generalize to arbitrary amounts of entanglement. The results of applying the encoding optimization procedure to some regular quantum stabilizer codes are provided in Section IV, together with some EAQEC codes of small length obtained by the circulant construction. Then we conclude in Section V.

* laiching@usc.edu
† tbrun@usc.edu

II. PRELIMINARIES

A. Stabilizer Codes

The n-fold Pauli group is $\mathcal{G}_n = \{i^a M_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}, a = 0, 1, 2, 3\}$, where I, X, Y, Z are the Pauli operators:

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

Let $X_i = I^{\otimes i-1} \otimes X \otimes I^{\otimes n-i}$, $Y_i = I^{\otimes i-1} \otimes Y \otimes I^{\otimes n-i}$, $Z_i = I^{\otimes i-1} \otimes Z \otimes I^{\otimes n-i}$ for $i = 1, \cdots, n$. An element $g = i^m M_1 \otimes M_2 \otimes \ldots \otimes M_n$ in $\mathcal{G}_n$, where $M_i \in \{I, X, Y, Z\}$ and $m \in \{0, 1, 2, 3\}$, can be expressed as $g = i^{m'} X_\alpha Z_\beta$ with α, β two binary n-tuples and $m' \in \{0, 1, 2, 3\}$. In this expression, if $M_j = I$, X, Z, or Y, then the j-th bits of α and β are $(\alpha_j, \beta_j) = (0, 0)$, $(1, 0)$, $(0, 1)$, or $(1, 1)$, respectively, and $m' \equiv m + l \pmod 4$, where l is the number of M_j's equal to Y. The weight $\mathrm{wt}(g)$ of g is the number of operators M_j that are not equal to the identity operator I.

We define a homomorphism $\varphi : \mathcal{G}_n \mapsto \mathbb{Z}_2^{2n}$ by $\varphi(i^{m'} X_\alpha Z_\beta) = (\alpha, \beta)$, and define a symplectic inner product $\odot$ between two elements (α_1, β_1) and (α_2, β_2) in $\mathbb{Z}_2^{2n}$ by $(\alpha_1, \beta_1) \odot (\alpha_2, \beta_2) \triangleq \alpha_1 \cdot \beta_2 + \beta_1 \cdot \alpha_2$, where $\cdot$ is the usual inner product in $\mathbb{Z}_2^n$. Two elements g, h in $\mathcal{G}_n$ commute if and only if the symplectic inner product $\varphi(g) \odot \varphi(h)$ is zero. Otherwise, they anticommute.

Suppose $\mathcal{S}$ is an Abelian subgroup of the n-fold Pauli group $\mathcal{G}_n$ that does not include $-I$, with a set of $r \equiv n-k$ independent generators $\{g_1, g_2, \cdots, g_r\}$. An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ corresponding to the stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n qubit state space fixed by $\mathcal{S}$. The minimum distance d is the minimum weight of an element in $\mathcal{N}(\mathcal{S}) - \mathcal{S}$, where $\mathcal{N}(\mathcal{S})$ is the normalizer group of $\mathcal{S}$.

A check matrix H corresponding to the stabilizer $\mathcal{S}$ is defined as a binary $r \times 2n$ matrix such that the the i-th row vector of H is $\varphi(g_i)$. The check matrix H must satisfy the commutative condition $H\Lambda_{2n}H^T = O_{r\times r}$,where $\Lambda_{2n} = \begin{bmatrix} O_{n\times n} & I_{n\times n} \\ I_{n\times n} & O_{n\times n} \end{bmatrix}$, $O_{i\times j}$ is an $i \times j$ zero matrix, and $I_{r\times r}$ is an r-dimensional identity matrix. The error syndrome of an operator $g \in \mathcal{G}_n$ is a binary r-tuple $s_1 \cdots s_r$, where $s_j = 1$ if g anti-commutes with g_j, and $s_j = 0$, otherwise. For a code with minimum distance d, if the error syndromes of error operators of weight smaller than or equal to $\lfloor \frac{d-1}{2} \rfloor$ are distinct, we call that code nondegenerate. Otherwise, it is degenerate.

The encoding procedure is described as follows. Consider the initial n-qubit state $|\psi\rangle = |0\rangle^{\otimes r} |\phi\rangle$, where there are $r = n-k$ ancilla qubits $|0\rangle$'s and an arbitrary k-qubit state $|\phi\rangle$. A set of generators of the stabilizer group of this class of states is $\{Z_1, \cdots, Z_r\}$ with a check matrix

$$H_0 = \left[\, O_{r\times n} \, \middle| \, I_{r\times r} \;\; O_{r\times(n-r)} \, \right]. \tag{1}$$

The operators $Z_{r+1}, \cdots, Z_n$, and $X_{r+1}, \cdots, X_n$ act to modifiy the quantum information $|\phi\rangle$, and these operator are called *logical* operators.

If U_E is a unitary operator such that $\{U_E Z_1 U_E^\dagger, \cdots, U_E Z_r U_E^\dagger\}$ is a set of generators of the stabilizer group $\mathcal{S}$, then U_E is an encoding operation of $\mathcal{C}(\mathcal{S})$, and the encoded state $U_E|\psi\rangle$ is fixed by the stabilizer group $\mathcal{S}$. In particular, we can choose $g_i = U_E Z_i U_E^\dagger$ for $i = 1, \cdots, r$. The logical operators on $U_E|\psi\rangle$ are

$$\bar{Z}_j = U_E Z_{r+j} U_E^\dagger,$$
$$\bar{X}_j = U_E X_{r+j} U_E^\dagger,$$

for $j = 1, \cdots, k$. U_E must map Pauli operators to Pauli operators; such unitaries are called Clifford operators. Note that the logical operators commute with the stabilizers, and the normalizer group of $\mathcal{S}$ is

$$\mathcal{N}(\mathcal{S}) = \langle g_1, g_2, \cdots, g_r, \bar{Z}_1, \bar{Z}_2, \cdots, \bar{Z}_k, \bar{X}_1, \bar{X}_2, \cdots, \bar{X}_k \rangle,$$

with $2n - r = r + 2k$ independent generators.

Given a check matrix H of a stabilizer group, the encoding unitary operator can be implemented by applying a certain quantum circuit. For example, Wilde gave an algorithm [18] to find an encoding circuit for a given quantum stabilizer code. This algorithm applies a series of CNOT gates, Hadamard gates, Phase gates, SWAP gates, and row operations to the check matrix H such that H takes the form (1). This process is like performing Gaussian elimination on a matrix, but using CNOT gates, Hadamard gates, Phase gates, and SWAP gates, in addition to the elementary row operations of Gaussian elimination. The series of operations used in the algorithm serve as a unitary operation $U_E^\dagger$ such that $U_E^\dagger g_i U_E = Z_i$, and hence the inverse operator U_E is a desired encoding operation. The check matrix H_0 is mapped to the desired matrix H. Note that the encoding circuit is not unique. This fact will be important later in this paper.

B. Entanglement-Assisted Quantum Error-Correcting Codes

Brun, Devetak and Hsieh proposed a theory of quantum stabilizer codes when shared entanglement between the encoder (Alice) and decoder (Bob) is available [12]. Suppose that Alice and Bob share c pairs of qubits in maximally entangled states $|\Phi_+\rangle^{AB}$, where AB means that Alice and Bob each have one qubit of $|\Phi_+\rangle = \frac{|00\rangle + |11\rangle}{2}$. (Such a shared pair is called an ebit.) Assume further that Bob's halves of the c ebits are not subject to error since they do not pass through the chan-

nel. Let $T = \{t_1, \cdots, t_c\}$ be an arbitrary subset of $\{1, 2, \cdots, n-k\}$. T denotes the positions of the ancilla qubits that are ebits. The $(n+c)$-qubit initial state is

$$|\psi\rangle_{EA} = \left[\bigotimes_{i=1}^{r} |\eta_i\rangle\right] \otimes |\phi\rangle,$$

where

$$|\eta_i\rangle = \begin{cases} |0\rangle, & \text{if } i \notin T; \\ |\Phi_+\rangle^{AB}, & \text{if } i \in T. \end{cases}$$

For convenience, the qubits on Alice's side will be numbered 1 to n and the qubits on Bob's side will be numbered 1 to c. Hence the t_i-th qubit of Alice and the i-th qubit of Bob form a maximally-entangled pair. Then a set of independent generators of a stabilizer group of $|\psi\rangle_{EA}$ is

$$\begin{cases} Z_i^A \otimes I^B, & \text{if } i \notin T; \\ Z_i^A \otimes Z_j^B, & \text{if } i = t_j \in T; \\ X_{t_j}^A \otimes X_j^B, & \end{cases} \begin{array}{l} \text{for } i = 1, \cdots, r, \\ \\ \text{for } j = 1, \cdots, c. \end{array} \tag{2}$$

Note that the operators on the left and right of the tensor product $\otimes$ are applied to Alice's qubits and Bob's qubits, respectively, and the superscripts A and B will be omitted throughout the rest of this article. The logical operators on $|\psi\rangle_{EA}$ are $Z_{r+1} \otimes I$, $\cdots$, $Z_n \otimes I$, and $X_{r+1} \otimes I$, $\cdots$, $X_n \otimes I$. Now consider the operators on Alice's qubits. These operators have commutation relations

$$[Z_i, Z_j] = 0, \text{ for } 0 \le i, j \le r, \tag{3}$$
$$[X_{t_i}, X_{t_j}] = 0, \text{ for } 0 \le i, j \le c, \tag{4}$$
$$\{Z_{t_i}, X_{t_i}\} = 0, \text{ for } 0 \le i \le c, \tag{5}$$
$$[Z_i, X_{t_j}] = 0, \text{ for } i \ne t_j, \tag{6}$$

where $[g, h] = gh - hg$ and $\{g, h\} = gh + hg$. This means

$$\varphi(Z_i) \odot \varphi(Z_j) = 0, \text{ for } 0 \le i, j \le r, \tag{7}$$
$$\varphi(X_{t_i}) \odot \varphi(X_{t_j}) = 0, \text{ for } 0 \le i, j \le c, \tag{8}$$
$$\varphi(Z_{t_i}) \odot \varphi(X_{t_i}) = 1, \text{ for } 0 \le i \le c, \tag{9}$$
$$\varphi(Z_i) \odot \varphi(X_{t_j}) = 0, \text{ for } i \ne t_j. \tag{10}$$

If a set of $(r + c)$ operators satisfy equations (3–6) or equations (7–10), we say that the two operators in (5) or the two vectors in (9) form a *symplectic pair*, and they are *symplectic partners* of each other. Hence Z_{t_i} and X_{t_i} form a symplectic pair.

An encoding operation U_E is applied to Alice's n qubits, while no operation is performed on Bob's c qubits. A set of generators of a stabilizer group $\mathcal{S}$ of the encoded state $(U_E \otimes I)|\psi\rangle_{EA}$ is $\{g_1, \cdots, g_r, h_1, \cdots, h_c\}$, where

$$g_i = \begin{cases} U_E Z_i U_E^\dagger \otimes I, & \text{if } i \notin T; \\ U_E Z_i U_E^\dagger \otimes Z_j, & \text{if } i = t_j \in T, \end{cases}$$
$$h_j = U_E X_{t_j} U_E^\dagger \otimes X_j.$$

The logical operators on $(U_E \otimes I)|\psi\rangle_{EA}$ are

$$\bar{Z}_j = U_E Z_{r+j} U_E^\dagger \otimes I,$$
$$\bar{X}_j = U_E X_{r+j} U_E^\dagger \otimes I,$$

for $j = 1, \cdots, k$.

The 2^k-dimensional subspace of the $(n+c)$ qubit state space fixed by the stabilizer group $\mathcal{S}$ with independent generators $\{g_1, \cdots, g_r, h_1, \cdots, h_c\}$ is called an EAQEC code with parameters $[[n, k, d; c]]$ for some minimum distance d. With the help of c ebits, the stabilizer group of an $[[n, k, d; c]]$ EAQEC code has c more generators than that of an $[[n, k, d]]$ regular stabilizer code. Since we assume that the c qubits of Bob suffer no error, we consider errors that act on Alice's qubits. For convenience, we denote

$$g_i' = U_E Z_i U_E^\dagger,$$

and

$$h_j' = U_E X_{t_j} U_E^\dagger,$$

and the g_i's and h_j's will be called the *simplified generators* of the stabilizer group. Similarly, we denote $\bar{Z}_i' = U_E Z_{r+i} U_E^\dagger, \bar{X}_j' = U_E X_{r+j} U_E^\dagger$. It is obvious that $\{g_1', \cdots, g_r', h_1', \cdots, h_c'\}$ satisfy the commutation relations (3–6), and g_{t_i}' and h_i' are a symplectic pair. Let $\mathcal{S}' = \langle g_1', \cdots, g_r', h_1', \cdots, h_c' \rangle$, and $\mathcal{S}_I' = \langle g_j : j \notin T \rangle$ is the isotropic subgroup of $\mathcal{S}'$. The normalizer group of $\mathcal{S}'$ is

$$\mathcal{N}(\mathcal{S}') = \langle g_i : i \notin T, \bar{Z}_1', \cdots, \bar{Z}_k', \bar{X}_1', \cdots, \bar{X}_k' \rangle$$

with $2n - (r + c) = 2k + r - c$ independent generators. The minimum distance d of the EAQEC code defined by $\mathcal{S}$ is the minimum weight of an element in $\mathcal{N}(\mathcal{S}') - \mathcal{S}_I'$. In particular, when $c = r$, $\mathcal{S}_I'$ is the trivial group that contains only the identity, and

$$\mathcal{N}(\mathcal{S}') = \langle \bar{Z}_1', \cdots, \bar{Z}_k', \bar{X}_1', \cdots, \bar{X}_k' \rangle.$$

An $[[n, k, d; c]]$ EAQEC code must satisfy some upper bounds on the minimum distance. For example, we have the singleton bound for EAQEC codes [12]

$$n + c - k \ge 2(d - 1), \tag{11}$$

the Hamming bound for non-degenerate EAQECCs [9]

$$\sum_{j=0}^{t} 3^j \binom{n}{j} \le 2^{n-k+c}, \tag{12}$$

and linear programming bounds for EAQECCs [19, 20].

We define a simplified check matrix H' as a binary $(r+c)\times 2n$ matrix such that the $r+c$ row vectors of H' are $\varphi(g_i')$ for $i=1,\cdots,r$ and $\varphi(h_j')$ for $j=1,\cdots,c$. For simplicity, we usually order the generators g_i' and h_j' so that $\varphi(g_i')$ is the i-th row vector of H' for $i=1,\cdots,r$, $\varphi(h_j')$ is the $(j+r)$-th row vector of H' for $j=1,\cdots,c$, and the j-th and $(j+r)$-th row vectors are a symplectic pair. H' must satisfy the commutation relations (7–10), and in the case $c=r$,

$$H'\Lambda_{2n}H'^T=\left[\begin{array}{c|c} O_{r\times r} & I_{r\times r} \\ \hline I_{r\times r} & O_{r\times r}\end{array}\right]. \tag{13}$$

For example, the simplified check matrix corresponding to the set of generators (2) of a stabilizer group of the initial state $|\psi\rangle_{EA}$ is

$$\left[\begin{array}{c|c} O_{r\times n} & I_{r\times r}\ O_{r\times(n-r)} \\ \hline I_{r\times r}\ O_{r\times(n-r)} & O_{r\times n}\end{array}\right]. \tag{14}$$

Conversely, an $(r+c)\times 2n$ binary matrix $\tilde{H}$, serving as a simplified check matrix, can define a stabilizer group and hence an EAQEC code. The number of ebits required to construct an EAQEC code [21] is

$$c=\frac{1}{2}\mathrm{rank}(\tilde{H}\Lambda\tilde{H}^T). \tag{15}$$

Like the check matrix of a standard quantum error-correcting code, the simplified check matrix H' can be used to determine the minimum distance of nondegenerate EAQEC codes. Note that Wilde's encoding circuit algorithm [18] can also be applied to a simplified check matrix to find an encoding unitary operator of the EAQEC code, just as for a regular stabilizer code.

Similarly, we define a simplified logical matrix L' corresponding to the logical operators by putting $\varphi(\bar{Z}_i')$ to be the i-th row vector of L' for $i=1,\cdots,k$, and $\varphi(\bar{X}_j')$ to be the $(j+k)$-th row vector of L' for $j=1,\cdots,k$. Since the logical operators commute with $\{g_1',\cdots,g_r',h_1',\cdots,h_r'\}$, we have

$$H'\Lambda_{2n}L'^T=O_{(r+c)\times 2k}. \tag{16}$$

Since the logical operators satisfy the commutation relations (3–6), we have

$$L'\Lambda_{2n}L'^T=\left[\begin{array}{c|c} O_{k\times k} & I_{k\times k} \\ \hline I_{k\times k} & O_{k\times k}\end{array}\right].$$

For example, the simplified logical matrix corresponding to the initial state $|\psi\rangle_{EA}$ is

$$\left[\begin{array}{c|c} O_{k\times n} & O_{k\times r}\ I_{k\times k} \\ \hline O_{k\times r}\ I_{k\times k} & O_{k\times n}\end{array}\right]. \tag{17}$$

III. THE ENCODING OPTIMIZATION PROCEDURE FOR EAQECCS

An $[[n,2k+c-n,d;c]]$ EAQEC code can be constructed from an $[n,k,d]$ classical linear quaternary code by the construction of [12], and c is determined by (15). It seems that only the number of information qubits is increased by introducing ebits. However, with the help of entanglement it is possible to define more distinct error syndromes for a given codeword size, and hence the set of correctable error operators might be larger. We would like to construct EAQEC codes with a higher minimum distance instead of a higher rate.

One way to construct an EAQEC code is to start with a regular QECC and move c of the qubits from Alice's side to Bob's side. So long as $c\le d/2$, the resulting code can be encoded by a unitary operator on Alice's side, given c ebits of initial shared entanglement between Alice and Bob [22]. While such codes can be interesting and useful, they are not the subject of interest for this paper; because such codes retain an ability to correct errors on Bob's qubits, they are in a sense not making full use of the fact that Bob's halves of the ebits are noise-free. They therefore are less likely to have the maximum error correcting power on Alice's qubits for the given parameters n, k and c. We are interested in EAQEC codes that can do better than any regular stabilizer code, in this sense.

To make this idea precise, we say that an $[[n,k,d;c]]$ EAQEC code is not equivalent to any regular stabilizer code if there is no regular $[[n+c,k,d]]$ quantum code. If there exists a regular $[[n+c,k,d]]$ quantum code, then we may not be achieving the maximum boost to our error correcting power from the c ebits of shared entanglement. We expect added entanglement in general to increase the error-correcting ability of a quantum error-correcting code, such that the EAQEC code is not equivalent to any regular stabilizer code, and indeed this turns out to be possible by our encoding optimization procedure. (Note that this is not *always* possible—the smallest examples of the $[[3,1,3;2]]$ and $[[4,1,3;1]]$ codes are both equivalent to the regular $[[5,1,3]]$ QECC, and this is the best that can be done.)

We now consider how added entanglement affects an $[[n,k,d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ defined by a stabilizer group $\mathcal{S}=\langle g_1',g_2',\cdots,g_r'\rangle$ The basic idea is to replace a set T of c ancilla qubits by ebits. This introduces the symplectic partners h_j's of c generators g_j's to the generating set of the stabilizer group $\mathcal{S}$. An EAQEC code is obtained. As we will examine in detail below, the encoding unitary operator for a standard QECC is not uniquely defined. The EAQEC code defined by $S'=\langle g_1',\cdots,,g_r',h_1',\cdots,,h_c'\rangle$ may gain higher error-correcting ability by modifying the encoding operator.

We first discuss the case $c=r$, where the generator h_i' is the symplectic partner of g_i' for all $i=1,\cdots,r$. We will treat the case $c<r$ later, by optimizing the

choice of c linearly independent generators from the group $\langle h'_1, \cdots, , h'_r \rangle$.

A. Selecting Symplectic Partners and Logical Operators

Since the symplectic partners of $g'_1, \cdots, g'_r$ are not unique, we now explain how to select these partners such that the minimum distance of the EAQEC code is higher than the code without entanglement. Suppose W is a unitary Clifford operator that commutes with $Z_1, \cdots, Z_r$ such that after the operation of W, the simplified check matrix of the initial state (14) becomes

$$\left[\begin{array}{c|cc} O_{r\times n} & I_{r\times r} & O_{r\times(n-r)} \\ \hline I_{r\times r}\ A & C & B \end{array}\right], \tag{18}$$

where A and B are two $r \times (n-r)$ binary matrices, and C is an $r \times r$ binary matrix. The simplified check matrix satisfies the commutation relations (7–10) if

$$C^T + AB^T + C + BA^T = O_{r\times r}. \tag{19}$$

In addition, it can be checked that the simplified logical matrix is of the form

$$\left[\begin{array}{c|cc} O_{k\times n} & A^T & I_{k\times k} \\ \hline O_{k\times(n-k)}\ I_{k\times k} & B^T & O_{k\times k} \end{array}\right]$$

after Gaussian elimination such that (16) and (17) hold. Since

$$(U_E W) Z_i (U_E W)^\dagger = U_E Z_i U_E^\dagger = g'_i$$

for $i = 1, \cdots, r$, $U_E W$ is also an encoding operator of the quantum stabilizer code $\mathcal{C}(\mathcal{S})$. However, the symplectic partners of the g'_i's, $U_E(WX_iW^\dagger)U_E^\dagger$, may differ from $U_E X_i U_E^\dagger$ for $i = 1, \cdots, r$, and the logical operators $U_E(WX_iW^\dagger)U_E^\dagger$, $U_E(WZ_jW^\dagger)U_E^\dagger$, for $i, j = r+1, \cdots, n$ are different. Choosing a set of matrices A, B, C such that $C^T + AB^T + C + BA^T = O_{r\times r}$ determines a unitary operator W by the encoding circuit algorithm, which in turn determines a set of symplectic partners of $g'_1, \cdots, g'_r$ and a set of logical operators. Thus we call W the *selection operator* for EAQEC codes. The minimum distance of the EAQEC code can be optimized by examining each distinct encoding operator $U_E W$. Note that the simplified logical matrix is not affected by the matrix C. Therefore, there are 2^{2rk} distinct sets of logical operators.

Lemma 1. Given matrices A and B, then a matrix C that satisfies (19) is of the form

$$C = BA^T + M,$$

where M is a symmetric matrix.

Proof. Suppose C is matrix that satisfies Eq. (19). We can assume that $C = BA^T + M$ for some matrix M. From Eq. (19), we have

$$O_{r\times r} = AB^T + BA^T + C' + (C')^T = M + M^T,$$

which implies that M is symmetric. □

We construct an EAQEC code that achieves the quantum singleton bound by applying this procedure to a regular stabilizer code in the following example.

Example 1. A check matrix of the regular $[[5, 1, 1]]$ 5-qubit bit flip code (the repetition code) is

$$\left[\begin{array}{c|c} 00000 & 11000 \\ 00000 & 01100 \\ 00000 & 00110 \\ 00000 & 00011 \end{array}\right].$$

Applying the encoding circuit algorithm to this check matrix, we obtain an encoding operator U_E. In particular, if $C = O_{r\times r}$ in (19), then

$$AB^T + BA^T = O_{r\times r}.$$

When $k = 1$, $AB^T + BA^T = O_{r\times r}$ holds if and only if $A = B$ or at least one of A and B is the zero vector. Let W be the selection operator determined by the encoding circuit algorithm with $A = \begin{bmatrix}0 & 0 & 0 & 0\end{bmatrix}^T$ and $B = \begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}^T$. Then the encoding operator $U_E W$ generates a $[[5, 1, 5; 4]]$ EAQEC code with a simplified check matrix

$$\left[\begin{array}{c|c} 00000 & 11000 \\ 00000 & 01100 \\ 00000 & 00110 \\ 00000 & 00011 \\ \hline 01111 & 00000 \\ 11000 & 00000 \\ 00011 & 00000 \\ 11110 & 00000 \end{array}\right]$$

and a simplified logical matrix

$$\left[\begin{array}{c|c} 11111 & 00000 \\ \hline 00000 & 11111 \end{array}\right].$$

With the help of 4 ebits, the minimum distance is increased from 1 to 5. The quantum singleton bound (11) is saturated by the parameters $[[5, 1, 5; 4]]$. Because the minimum distance of a regular $[[9, 1]]$ quantum stabilizer code is at most 3 from the upper bound in [3], this $[[5, 1, 5; 4]]$ code is not equivalent to any regular 9-qubit code. □

The result in Example 1 can be generalized to the construction of a family of EA repetition codes as follows.

Theorem 2. There are $[[n, 1, n; n-1]]$ EAQEC codes for n odd and $[[n, 1, n-1; n-1]]$ EAQEC codes for n even. These codes are optimal, and are not equivalent to any regular stabilizer code for $n \geq 5$.

Proof. Suppose $\hat{H}_n$ is an $(n-1)\times n$ parity-check matrix of a classical $[n,1,n]$ repetition code:

$$\hat{H}_n = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 1 \end{bmatrix}.$$

The $[[n,1,1]]$ n-qubit bit-flip code has a check matrix

$$\left[\, O_{(n-1)\times n} \,\middle|\, \hat{H}_n \,\right].$$

We want to introduce $(n-1)$ simplified generators to the generating set of the stabilizer group such that the minimum distance of the code is increased to n. Consider a simplified check matrix $H' = \begin{bmatrix} O_{(n-1)\times n} & \hat{H}_n \\ \hat{H}_n & O_{(n-1)\times n} \end{bmatrix}$. By (15), the number of symplectic pairs in H' is

$$\frac{1}{2}\mathrm{rank}(H'\Lambda H'^T) = \mathrm{rank}(\hat{H}_n\hat{H}_n^T) = n-1,$$

for n odd. It can be verified that H' is a simplified check matrix with minimum distance n. Therefore, there exists a set of symplectic partners of the generators of the stabilizer group of the n-qubit bit flip code such that the minimum distance of the code is n. It is easy to verify that (11) is saturated by the parameters $[[n,1,n;n-1]]$.

These $[[n,1,n;n-1]]$ codes are not equivalent to any regular stabilizer code, for there are no regular $[[2n-1,1,n]]$ quantum codes for $n>3$. This is because they violate the quantum Hamming bound, which says that an $[[n,k,d=2t+1]]$ code satisfies

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i} 3^i.$$

Let $n=2t+1$. The $[[2n-1,1,n]] = [[4t+1,1,2t+1]]$ code would have $\sum_{i=0}^{t}\binom{4t+1}{i}3^i$ error syndromes if it exists. The last term $\binom{4t+1}{t}3^t$ is of order $O\left((12t+3)^t\right)$, which is larger than the total number of possible syndromes 2^{4t} for sufficiently large t. We have checked that it holds when $t>1$ or $n>3$.

In the case of even n, the above construction gives a series of $[[n,0,n;n-2]]$ EAQEC codes with no information qubits. A series of $[[n,1,n-1;n-1]]$ EAQEC codes for n even is constructed in [19]. These EAQEC codes are optimal, since it is proved that there is no $[[n,1,n;n-1]]$ EAQEC codes for n even in [19]. These EAQEC codes are not equivalent to any regular stabilizer codes for $n>4$ by the same argument as in the case of n odd.

□

According to Ref. [12], given a parity-check matrix $\hat{H}$ of an $[n,k,d]$ classical binary linear code, the simplified check matrix

$$H' = \begin{bmatrix} O_{(n-k)\times n} & \hat{H} \\ \hat{H} & O_{(n-k)\times n} \end{bmatrix} \tag{20}$$

defines an $[[n,2k+c-n,d;c]]$ EAQEC code, where the number of ebits c is given by (15). The family of EAQEC codes in Theorem 2 for n odd can also be obtained by this construction. When $c=n-k$, the quantum singleton bound (11) becomes

$$n-k \geq d-1,$$

which is exactly the same as the classical singleton bound. However, no nontrivial classical binary codes achieve the singleton bound [23].

B. Unitary Row Operators

Since we have the freedom to choose among different sets of generators of a stabilizer group, and also the freedom to choose which ancilla qubits are replaced by ebits when $c<r$, we will show that the minimum distance can be further optimized over these two freedoms when $c<r$. We first discuss the effect of "unitary row operators" that preserve the overall commutation relations (3–6).

Consider a unitary operator $U = \frac{1}{\sqrt{2}}(I+iQ)$, where Q is a Pauli operator with eigenvalues ± 1. It is easy to verify that

$$UgU^\dagger = \begin{cases} g, & \text{if } [Q,g]=0; \\ iQg, & \text{if } \{Q,g\}=0. \end{cases}$$

We define $V_{1,2} = V_3V_2V_1$, where $V_1 = \frac{1}{\sqrt{2}}(I+ig_1'h_2')$, $V_2 = \frac{1}{\sqrt{2}}(I-ih_2')$, and $V_3 = \frac{1}{\sqrt{2}}(I-ig_1')$. Then

$$V_{1,2}g_j'V_{1,2}^\dagger = \begin{cases} g_1'g_2', & \text{if } j=2; \\ g_j', & \text{if } j\neq 2. \end{cases}$$

Therefore, $V_{1,2}$ is a unitary operator that performs multiplication of g_1' to g_2', which corresponds to adding the first row to the second in the simplified check matrix. On the other hand,

$$V_{1,2}h_j'V_{1,2}^\dagger = \begin{cases} h_2'h_1', & \text{if } j=1; \\ h_j', & \text{if } j\neq 1. \end{cases}$$

Hence a row operation performed on $\{g_1',\cdots,g_r'\}$ induces a row operation performed on $\{h_1',\cdots,h_r'\}$ in order to preserve the commutation relations (3–6). We call $V_{1,2}$ a *unitary row operator*. Later we will need unitary row operators that change h_j' to $h_j'g_i'$, h_j' to $h_j'\bar{Z}_i'$, and h_j' to $h_j'\bar{X}_i'$ seperately. These four types of unitary row operators are summarized in Table I.

When a different set of generators of the stabilizer group is chosen instead of $\{g_1',\cdots,g_r'\}$, this is equivalent to performing a unitary transformation V, which

Type 1.	$Vh'_jV^\dagger = \begin{cases} h'_lh'_m, & \text{if } j=l; \\ h'_j, & \text{if } j\neq l. \end{cases}$	$Vg'_jV^\dagger = \begin{cases} g'_mg'_l, & \text{if } j=m; \\ g'_j, & \text{if } j\neq m. \end{cases}$
Type 2.	$Vh'_jV^\dagger = \begin{cases} h'_lg'_m, & \text{if } j=l; \\ h'_j, & \text{if } j\neq l. \end{cases}$	$Vh'_jV^\dagger = \begin{cases} h'_mg'_l, & \text{if } j=m; \\ h'_j, & \text{if } j\neq m. \end{cases}$
Type 3.	$Vh'_jV^\dagger = \begin{cases} h'_lZ'_m, & \text{if } j=l; \\ h'_j, & \text{if } j\neq l. \end{cases}$	$V\bar{X}'_jV^\dagger = \begin{cases} g'_lX'_m, & \text{if } j=m; \\ X'_j, & \text{if } j\neq m. \end{cases}$
Type 4.	$Vh'_jV^\dagger = \begin{cases} h'_l\bar{X}'_m, & \text{if } j=l; \\ h'_j, & \text{if } j\neq l. \end{cases}$	$V\bar{Z}'_jV^\dagger = \begin{cases} g'_lZ'_m, & \text{if } j=m; \\ Z'_j, & \text{if } j\neq m. \end{cases}$

TABLE I. Four types of unitary row operators

comprises a sequence of unitary row operators of type 1 on $\{g'_1,\cdots,g'_r\}$. The effect of V on the simplified check matrix H' corresponding to $\{g'_1,\cdots,g'_r,h'_1,\cdots,h'_r\}$ is to multiply H' from the left by a $(2n-2k)\times(2n-2k)$ matrix of the form

$$M_V = \left[\begin{array}{c|c} M_Z & O_{(n-k)\times(n-k)} \\ O_{(n-k)\times(n-k)} & M_X \end{array}\right].$$

If $M_X = R_mR_{m-1}\cdots R_1$, where the R'_is are elementary row operations, then $M_Z = R_m^TR_{m-1}^T\cdots R_1^T$. It can be checked that MH' satisfies (13). If a set $T=\{t_1,\cdots,t_c\}$ of $c<r$ ancilla qubits are replaced by ebits, it is possible that after the operation of V, the group $\mathcal{S}'_{\mathcal{I}} = \langle g_j : j\notin T\rangle$ changes, and so does the set $\mathcal{N}(\mathcal{S}')-\mathcal{S}'_{\mathcal{I}}$. In addition, the span of a subset of $\{h'_1,\cdots,h'_r\}$ can change after the operation of V, though the span of the full set remains unchanged. This means that if we add less than the maximum amount of entanglement to a code, we must optimize over all such unitary row operations. Since the group $\mathcal{S}'_{\mathcal{I}}$ and the set $\mathcal{N}(\mathcal{S}')-\mathcal{S}'_{\mathcal{I}}$ remain the same under type 1 unitary row operators on the h'_j for $j\notin T$, it suffices to assume that the operation V consists of type 1 unitary row operators that operate only on the h'_j for $j\in T$.

Let M_V be a $c\times r$ matrix such that the i-th row of M_V is the t_i-th row of M_Z for $i=1,\cdots,c$. It is obvious that different M_V's can have the same effect on the row space of H'. For example, if $c=2$, $\{g'_1g'_2,g'_2,\cdots,g'_r,h'_1,h'_1h'_2\}$ and $\{g'_1,g'_2,\cdots,g'_r,h'_1,h'_2\}$ are two different sets of generators, but they generate the same group, and hence their corresponding EAQEC codes have the same minimum distance. Therefore, without loss of generality a distinct unitary row operation V can be assumed to be be represented by a matrix M_V in reduced row echelon form.

Theorem 3. The operation of V is equivalent to applying a series of type 1 unitary row operators on the h'_j for $j\in T$. There are

$$N(r,c) \triangleq \sum_{l_c=0}^{r-c}\sum_{l_{c-1}=0}^{l_c}\sum_{l_{c-2}=0}^{l_{c-1}}\cdots\sum_{l_1=0}^{l_2} 2^{c(r-c)-\sum_{i=1}^c l_i}$$

distinct unitary row operations.

Proof. The total number of distinct unitary row operations $N(r,c)$ is determined as follows. If we begin with matrices of the form

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & \square & \cdots & \square \\ 0 & 1 & \cdots & 0 & \square & \cdots & \square \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \square & \cdots & \square \end{bmatrix},$$

where $\square$ can be 0 or 1, there are $2^{c(r-c)}$ distinct unitary row operations. Now we consider matrices in which the leading ones are shifted to the right. Let l_j denote the shift amount of the leading 1 of j-th row from its initial position for $j=1,\cdots,c$. It can be observed that $l_j\leq l_i$ if $j<i$. For a set $\{l_1,l_2,\cdots,l_c\}$, the number of $\square$ is $c(r-c)-\sum_{i=1}^c l_i$, and hence there are $2^{c(r-c)-\sum_{i=1}^c l_i}$ distinct unitary row operations. Therefore, summing over all possible sets of $\{i_1,\cdots,i_c\}$ shows that there is a total of

$$N(r,c) = \sum_{l_c=0}^{r-c}\sum_{l_{c-1}=0}^{l_c}\sum_{l_{c-2}}^{l_{c-1}}\cdots\sum_{l_1=0}^{l_2} 2^{c(r-c)-\sum_{i=1}^c l_i}$$

distinct unitary row operations up to Gaussian elimination. □

The function $N(r,c)$ has a symmetry given in the following lemma, which can be proved by induction.

Lemma 4. $N(r,c)=N(r,r-c)$ for any r and $0\leq c\leq r$.

On the other hand, the selection operator W in the previous subsection can be decomposed as a series of unitary row operators of type 2, type 3, and type 4. The matrix A determines a series of type 4 unitary row operators, the matrix B determines a series of type 3 unitary row operators, and the symmetric matrix M, satisfying $C=BA^T+M$, determines a series of type 2 unitary row operators. Unitary row operators of type 2 do not affect the set $\mathcal{N}(\mathcal{S}')-\mathcal{S}'_{\mathcal{I}}$ or the error-correcting ability, and so the symmetric matrix M can be dropped. It is the same as choosing a different basis for the same code space. If a set $T=\{t_1,\cdots,t_c\}$ of $c<r$ ancilla qubits are replaced by ebits, one can show that $\mathcal{N}(\mathcal{S}') = \langle g_j : j\notin T,\bar{Z}_1,\cdots,\bar{Z}_k,\bar{Z}_1,\cdots,\bar{Z}_k\rangle$ remains unchanged by the operation of type 3 and type 4 unitary row operators on the h'_j for $j\notin T$. It suffices to assume

that the operation W consists of type 3 and type 4 unitary row operators that act only on the h'_j for $j \in T$. To sum up, we have the following theorem.

Theorem 5. The operation of W is equivalent to applying a series of type 4 unitary row operators, followed by a series of type 3 unitary row operators, on the h'_j for $j \in T$. There are 2^{2ck} distinct selection operators with $C = BA^T$.

Combining the effects of the unitary row operation V with the selection operator W in the previous section, we can optimize an encoding operation of the form $U = VU_EW$ over

$$2^{2ck}N(r,c)$$

possibilities. We call this the *encoding optimization procedure* for EAQEC codes.

Note that we can find another unitary row operator W' corresponding to W such that $W'U_E$ and U_EW are equivalent encoding operators. While W operates on the raw stabilizer generators and logical operators, W' operates on the encoded stabilizer generators and logical operators. Hence, we can also solve the optimization problem for an operator of the form $U = VW'U_E$ (which is what we actually do in practice, combining VW' into a single optimization).

IV. RESULTS

A. Results of the Encoding Optimization Procedure

We applied the encoding optimization procedure to a $[[7,1,3]]$ quantum BCH code [24, 25] and Shor's $[[9,1,3]]$ code [1], and the results are shown in Table II and Table III, where d_{opt} is the minimum distance of the optimized EAQEC codes, and d_{std} is the highest minimum distance of an $[[n+c,k]]$ regular stabilizer code.

Example 2. The check matrix of a regular $[[7,1,3]]$ quantum BCH code adopted in the encoding optimization procedure is

$$\begin{bmatrix} 0000000 & 1001011 \\ 0000000 & 0101110 \\ 0000000 & 0010111 \\ 1001011 & 0000000 \\ 1100101 & 0000000 \\ 1011100 & 0000000 \end{bmatrix}.$$

As shown in Table II, the parameters $[[7,1,7;6]]$, $[[7,1,5;3]]$ and $[[7,1,5;2]]$ achieve the quantum singleton bound for EAQEC codes (11) and are not equivalent to any standard quantum stabilizer code. We would like to compare these two EAQEC codes to a competing EAQEC code with $n = 7$ and $d = 5$ by the construction of [12]. According to Grassl's table [26], a classical linear code over $GF(4)$ (or $GF(2)$) that meets our requirement is a $[7,2,5]$ linear quaternary code, which can be used to construct a $[[7,2,5;5]]$ EAQEC code. This means that the $[[7,1,5;2]]$ and $[[7,1,5;3]]$ EAQEC codes cannot be obtained by the construction of [12], and thus are new.

In addition, all the $[[7,1,5;2]]$ EAQEC codes we found are degenerate codes, for some simplified stabilizer generators are of weight 4 from the check matrix. For example, the simplified check matrix and simplified logical matrix of a $[[7,1,5;2]]$ EAQEC code are

$$\left[\begin{array}{cc} 0000000 & 1001011 \\ 0000000 & 1100101 \\ 0000000 & 0010111 \\ 1001011 & 0000000 \\ 1100101 & 0000000 \\ 0010111 & 0000000 \\ \hline 1000011 & 0100011 \\ 1101000 & 0010010 \end{array}\right], \begin{bmatrix} 1001011 & 0100011 \\ 1101000 & 1001011 \end{bmatrix},$$

with $T = \{1,4\}$. On the other hand, all the $[[7,1,7;6]]$ EAQEC codes are nondegenerate codes, while $[[7,1,5;3]]$, $[[7,1,5;4]]$, and $[[7,1,5;5]]$ EAQEC codes can be either degenerate or nondegenerate.

□

TABLE II. Optimization over the $[[7,1,3]]$ quantum BCH code

c	1	2	3	4	5	6
d_{opt}	3	5	5	5	5	7
d_{std}	3	3	4	5	5	5

Example 3. The check matrix of Shor's $[[9,1,3]]$ code is

$$\begin{bmatrix} 000000000 & 110000000 \\ 000000000 & 011000000 \\ 000000000 & 000110000 \\ 000000000 & 000011000 \\ 000000000 & 000000110 \\ 000000000 & 000000011 \\ 111111000 & 000000000 \\ 000111111 & 000000000 \end{bmatrix}.$$

As can be seen in Table III, the parameters $[[9,1,9;8]]$, $[[9,1,7;5]]$ and $[[9,1,7;4]]$ achieve the quantum singleton bound for EAQEC codes (11) and are not equivalent to any regular stabilizer code. A competing EAQEC code with $n = 9$ and $d = 7$ by the construction of [12] is a $[[9,1,7;6]]$ EAQEC code, obtained from a $[9,2,7]$ linear quaternary code in Grassl's table. Therefore, the $[[9,1,7;5]]$ and $[[9,1,7;4]]$ EAQEC codes are new. All the $[[9,1,5;2]]$, $[[9,1,5;3]]$, $[[9,1,7;4]]$, $[[9,1,7;5]]$ and $[[9,1,7;6]]$ codes are degenerate codes, and all the $[[9,1,9;8]]$ codes are nondegenerate codes, while the $[[9,1,7;7]]$ codes can be either degenerate or nondegenerate.

□

TABLE III. Optimization over Shor's $[[9,1,3]]$ code

c	2	3	4	5	6	7	8
d_{opt}	5	5	7	7	7	7	9
d_{std}	5	5	5	6	6	6	7

B. Random Optimization Procedure

It is easy to check that

$$2^{c(n+k-c)} \leq 2^{2ck} N(r,c) \leq \binom{r}{c} 2^{c(n+k-c)}.$$

A complete encoding optimization procedure for a $[[n,k,d]]$ regular stabilizer code becomes impossible when $n+k$ becomes large. Hence one can consider random search algorithms for the encoding optimization procedure. For each iteration of optimization, we randomly generate two matrices A and B, and randomly choose a unitary row operation V. Then we optimize the minimum distance until a target minimum distance is obtained or a preset of maximum number of iterations is reached. Some examples of random optimization follow:

Example 4. We applied the random optimization algorithm to Gottesman's $[[8,3,3]]$ code [4] and the results are shown in Table IV. By the construction of [12], the $[8,3,5]$ classical linear quaternary codes in Grassl's Table can be transformed to an $[[8,2,5;4]]$ EAQEC code. Hence the $[[8,3,5;5]]$ and $[[8,3,4;3]]$ EAQEC codes are new, and are not equivalent to any regular stabilizer code. In addition, these two EAQEC codes saturate the linear programming bounds and are optimal. □

TABLE IV. Optimization over Gottesman's $[[8,3,3]]$ code

c	2	3	4	5
d_{opt}	3	4	4	5
d_{std}	3	3	4	4

Example 5. We applied random optimization to a $[[15,7,3]]$ quantum BCH code and the results are shown in Table V. Note that could not fully optimize parameters

TABLE V. Optimization over a $[[15,7,3]]$ Quantum BCH code

c	3	4	5	6	7	8
d_{opt}	3	4	4	5	5	6
d_{std}	4	4-5	4-5	5-6	5-6	5-6

in this case, since the complexity is very high. However, compared with the $[[15,3,5;4]]$ EAQEC code, obtained by the construction of (20) from a $[15,7,5]$ classical BCH code, the $[[15,7,5;7]]$ and the $[[15,7,5;6]]$ EAQEC codes have 4 more information qubits at the cost of 3 and 2 more ebits, respectively. The $[[15,7,6;8]]$ EAQEC code has 4 more information qubits and a higher minimum distance at the cost of 4 more ebits. In addition, the $[[15,7,6;8]]$ EAQEC code is not equivalent to any known regular stabilizer code.

On the other hand, the classical linear quaternary $[15,9,5]$ code and $[15,8,6]$ code in Grassl's table can be used to construct a $[[15,9,5;6]]$ EAQEC code and a $[[15,8,6;7]]$ EAQEC code by the construction of [12]. These codes are better than the $[[15,7,6;8]]$ EAQEC code we obtained. This may be because our codes were not fully optimized, but in any case BCH codes may not give the best possible EAQEC codes, even using the encoding optimization procedure.

□

Example 6. We applied the random optimization algorithm to the $[[13,1,5]]$ quantum QR code [2, 27], and the results are shown in Table VI. By the construction of [12], the $[13,3,9]$, $[13,4,8]$, and $[13,5,7]$ classical linear quaternary codes in Grassl's table can be transformed to $[[13,3,9;10]]$, $[[13,0,8;5]]$, and $[[13,1,7;4]]$ EAQEC codes, respectively. The $[[13,1,11;11]]$, $[[13,1,11;10]]$, $[[13,1,9;9]]$, and $[[13,1,9;8]]$ EAQEC codes are new, and are not equivalent to any regular stabilizer code. □

TABLE VI. Optimization over the $[[13,1,5]]$ quantum QR code

c	4	5	6	7	8	9	10	11	12
d_{opt}	7	7	7	7	9	9	11	11	13
d_{std}	7	7	7	7	7	7-8	7-9	8-9	9

C. Circulant Construction of EAQEC Codes

Since optimization over all codes is computationally intensive, it is worthwhile to also study particular code constructions. In this subsection we show a construction of EAQEC codes that gives more examples of EAQEC codes of small length that are not equivalent to regular stabilizer codes. We construct the simplified check matrix directly, rather than starting from a classical binary code.

Let H' be a $r \times 2n$ simplified check matrix cyclicly generated by a binary $2n$-tuple $\mathbf{a} = a_0 a_1 \cdots a_{2n-2} a_{2n-1}$:

$$H' = \left[\begin{array}{ccc|ccc} a_0 & \dots & a_{n-1} & a_n & \dots & a_{2n-1} \\ a_1 & \dots & a_n & a_{n+1} & \dots & a_0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{r-1} & \dots & a_{r+n-2} & a_{r+n-1} & \dots & a_{r-2} \end{array}\right].$$

If the rank of H' is exactly r, then $c = \frac{1}{2}\mathrm{rank}(H'\Lambda H')$ and H' defines an $[[n, n+c-r, d; c]]$ EAQEC code for some minimum distance d. For example, a $[[6,1,4;1]]$ code

TABLE VII. Parameters of circulant $[[n,k,d;c]]$ EAQEC codes not equivalent to any regular $[[n+c,k]]$ codes.

n	$[[n,k,d;c]]$
5	$[[5,1,5;4]]$, $[[5,1,4;3]]$, $[[5,1,4;2]]$, $[[5,2,3;2]]$
6	$[[6,1,5;4]]$, $[[6,1,4;3]]$, $[[6,2,4;3]]$, $[[6,2,3;1]]$
7	$[[7,1,7;6]]$, $[[7,2,5;5]]$, $[[7,3,4;4]]$, $[[7,3,4;3]]$ $[[7,4,3;2]]$
8	$[[8,1,6;6]]$, $[[8,2,6;6]]$, $[[8,1,6;5]]$, $[[8,3,5;5]]$ $[[8,2,5;4]]$, $[[8,1,4;1]]$, $[[8,3,4;3]]$,$[[8,5,3;2]]$
9	$[[9,1,9;8]]$, $[[9,1,7;6]]$, $[[9,1,7;7]]$, $[[9,2,6;6]]$ $[[9,1,6;5]]$, $[[9,1,6;6]]$, $[[9,2,5;4]]$, $[[9,5,3;1]]$
10	$[[10,1,8;8]]$, $[[10,1,7;6]]$, $[[10,1,6;5]]$, $[[10,1,6;4]]$ $[[10,2,7;7]]$, $[[10,2,6;5]]$, $[[10,2,5;3]]$, $[[10,2,5;2]]$ $[[10,3,6;7]]$, $[[10,3,6;6]]$, $[[10,4,5;5]]$, $[[10,4,5;4]]$

is constructed by $\mathbf{a} = 001110101110$ with the simplified check matrix

$$\begin{bmatrix} 001110 & 101110 \\ 000111 & 010111 \\ 100011 & 101011 \\ 110001 & 110101 \\ 111000 & 111010 \\ 011100 & 011101 \end{bmatrix}.$$

We call this the *circulant* construction of EAQEC codes, which is used for regular stabilizer codes in [27].

We examined the simplified check matrices cyclicly generated by every possible binary $2n$-tuple $\mathbf{a}$ by computer for $n = 4, \cdots, 10$ and $r \leq 2(n-1)$. Parameters of EAQEC codes not equivalent to any regular stabilizer codes are listed in Table VII. The parameters $[[5,1,4;3]]$, $[[5,1,4;2]]$, $[[5,1,5;4]]$, $[[5,2,3;2]]$, $[[6,2,3;1]]$, $[[6,2,4;3]]$, $[[6,1,5;4]]$, $[[7,1,6;5]]$, $[[7,1,7;6]]$, $[[7,2,5;5]]$, $[[7,3,4;4]]$, $[[7,3,4;4]]$, $[[7,4,3;2]]$, $[[8,2,6;6]]$, $[[8,3,5;5]]$, $[[8,5,3;2]]$, $[[8,3,4;3]]$, $[[9,1,9;8]]$, $[[9,5,3;1]]$, $[[10,3,6;7]]$, $[[10,3,6;6]]$, and $[[10,4,5;4]]$ are also optimal, for they saturate the upper bounds on the minimum distance [19].

V. DISCUSSION

This paper studied how entanglement can be used to increase the minimum distance of quantum error-correcting codes. We demonstrated the encoding optimization procedure for EAQEC codes obtained by adding ebits to standard quantum stabilizer codes. The four types of unitary row operators play an important role in this encoding optimization procedure, and also help to clarify the properties of EAQEC codes and their relationship to standard codes. Some applications of the encoding optimization procedure were found to have promising results: we constructed $[[7,1,5;2]]$ and $[[7,1,5;3]]$ EAQEC codes from quantum BCH codes; $[[8,3,5;5]]$ and $[[8,3,4;3]]$ EAQEC codes from Gottesman's 8-qubit code; and $[[9,1,7;4]]$ and $[[9,1,7;5]]$ EAQEC codes from Shor's 9-qubit code; together with a family of EA repetition codes, all of which are optimal. Several of the EAQEC codes found by this encoding optimization procedure are degenerate codes. This procedure serves as an EAQEC code construction method for given parameters n, k, c.

Some of our EAQEC codes use large numbers of ebits. However, it is still worthwhile to study EAQEC codes that use large entanglement. The one-shot father protocol is a random EA quantum code, and it achieves the EA hashing bound [9, 14–16]. Maximal-entanglement EA turbo codes come close the EA hashing bound within a few dB [17]. Asymptotically, maximal-entanglement codes achieve the EA capacity [15, 16].

The encoding optimization procedure has very high complexity. However, it might be useful to further investigate it for specific families of codes that have special algebraic structures, such as quantum BCH codes and quantum Reed-Muller codes. This is future work.

While the encoding optimization procedure in this paper applies to a standard quantum stabilizer code, it is possible to construct a similar encoding optimization algorithm for adding ebits to other EAQEC codes that use less than the maximum amount of entanglement. By adding a small amount of entanglement we may reduce the search space and make optimization more computationally tractable. It also might be possible to generate small or moderately sized EAQECCs randomly, by choosing random selections of simplified generators, and to search in this way for codes with desirable properties. Much work remains to be done in finding the best possible EAQEC codes for different applications.

ACKNOWLEDGMENTS

TAB and CYL acknowledge useful conversations with Mark M. Wilde. This work was supported in part by NSF Grants CCF-0448658 and CCF-0830801.

merlin.mbs apsrev4-1.bst 2010-07-25 4.21a (PWD, AO, DPC) hacked Control: key (0) Control: author (8) initials jnrlst Control: editor formatted (1) identically to author Control: production of article title (-1) disabled Control: page (0) single Control: year (1) truncated Control: production of eprint (0) enabled

[1] P. W. Shor, Phys. Rev. A **52**, 2493 (1995).

[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A.

Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inform. Theory **44**, 1369 (1998).
[4] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[5] D. Gottesman, *Stabilizer codes and quantum error correction*, Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997).
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambirdge University Pressr, Cambridge, UK, 2000).
[7] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[8] A. M. Steane, Proc. R. Soc. London A **452**, 2551 (1996).
[9] G. Bowen, Phys. Rev. A **66**, 052313 (2002).
[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[11] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[12] T. A. Brun, I. Devetak, and M.-H. Hsieh, Science **314**, 436 (2006).
[13] T. A. Brun, I. Devetak, and M.-H. Hsieh, (2006).
[14] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).
[15] I. Devetak, A. W. Harrow, and A. Winter, IEEE Trans. Inform. Theory **54**, 4587 (2008).
[16] I. Devetak, A. W. Harrow, and A. Winter, Phys. Rev. Lett. **93**, 230504 (2004).
[17] M. M. Wilde and M.-H. Hsieh, in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on* (31 2011-Aug. 5) pp. 445–449.
[18] M. M. Wilde, *Quantum Coding with Entanglement*, Ph.D. thesis, University of Southern California, Los Angeles, California (2008).
[19] C.-Y. Lai, T. A. Brun, and M. M. Wilde, (2010), arXiv:1010.5506.
[20] C.-Y. Lai, T. A. Brun, and M. M. Wilde, IEEE Trans. Inform. Theory 10.1109/TIT.2013.2246274, to be published.
[21] M. M. Wilde and T. A. Brun, Phys. Rev. A **77**, 064302 (2008).
[22] C.-Y. Lai and T. A. Brun, Phys. Rev. A **86**, 032319 (2012).
[23] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, The Netherlands, 1977).
[24] M. Grassl and T. Beth, in *Proc. X. International Symposium on Theoretical Electrical Engineering* (Magdeburg, 1999) pp. 207–212.
[25] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, IEEE Trans. Inform. Theory **53**, 1183 (2007).
[26] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Accessed on 2010-12-01.
[27] C.-Y. Lai and C.-C. Lu, IEEE Trans. Inform. Theory **57**, 7163 (2011)
.