Classical enhancement of quantum-error-correcting codes

Isaac Kremsky
Physics Department, University of Southern California, Los Angeles, California 90089, USA

Min-Hsiu Hsieh* and Todd A. Brun
Ming Hsieh Electrical Engineering Department, University of Southern California, Los Angeles, California 90089, USA

(Received 17 February 2008; published 21 July 2008)

We present a general formalism for quantum-error-correcting codes that encode both classical and quantum information (the EACQ formalism). This formalism unifies the entanglement-assisted coding theory and the classical coding theory in the sense that, after the encoding, error-correcting, and decoding steps, the encoded quantum and classical information can be correctly recovered by the receiver. We formally define this kind of quantum codes using stabilizer language, and derive the appropriate error-correcting conditions. We give several examples to demonstrate the construction of such codes.

DOI: 10.1103/PhysRevA.78.012341 PACS number(s): 03.67.Pp

I. INTRODUCTION

Since Shor proposed the first quantum-error-correcting code (QECC) [1], research in this field has progressed rapidly. A broad theory of QECCs was created under the stabilizer formalism and its symplectic formulation [2,3] that allow the systematic description of a large class of quantum codes and their error-correcting properties. In this formulation, a QECC is defined to be a subspace fixed by a stabilizer group. At the same time, a construction of QECCs from classical error-correcting codes was proposed separately by Calderbank, Shor, and Steane [4,5], the so-called CSS construction. Later this was generalized to give a stronger connection between quantum codes and classical symplectic codes; however, it seemed that this connection between quantum coding theory and classical coding theory was not universal, since only certain symplectic codes possessed quantum equivalents.

More recent developments in quantum coding theory have led to the development of the operator quantum-error-correcting formalism (OQECC) [6–12] and the entanglement-assisted quantum-error-correcting formalism (EAQECC) [13–15]; moreover, it is possible to produce a unified formalism (EAOQECC) [16] that combines both OQECCs and EAQECCs. This formalism demonstrates that a broader connection exists between classical and quantum coding theory. Good QECCs can be obtained by a generalized CSS construction from good classical codes. This opens the door, for example, to the construction of high-quality quantum codes from modern classical codes, such as TURBO and LDPC codes [17].

In this paper, we generalize this construction in a different way, by proposing quantum codes that can be used to transmit both classical and quantum information simultaneously. We call this scheme the entanglement-assisted, classically enhanced quantum-error-correcting formalism, but throughout the paper it will be referred to simply as the EACQ formalism. The EACQ formalism can be considered as a unification of the entanglement-assisted quantum coding theory [18] and the classical linear coding theory. This unification also makes contact with results in quantum information theory, where bounds exist on the asymptotic transmission of simultaneous classical and quantum information, including the use of entanglement assistance. It is believed that these bounds are better than simple time sharing between codes for transmitting quantum and classical information separately through a quantum channel [19]. It is our hope that it may be possible to construct classes of codes which achieve these rates in the limit of large block size.

This paper is organized as follows. We give a brief introduction of EAQECCs using the stabilizer formalism in Sec. II. In Sec. III, we formally define a quantum code (EACQ) that can transmit both classical and quantum information at the same time. Several properties of this kind of quantum codes are also discussed in this section. We provide several examples in Sec. IV to demonstrate the usefulness of this formalism. We conclude in Sec. V by examining some special cases, and arguing that the EACQ formalism is indeed a generalization and unification of both quantum and classical coding theory.

II. EAQECC

In this section, we will review the entanglement-assisted quantum-error-correcting formalism using the stabilizer language. Let $\mathcal{G}_n$ be the n-fold Pauli group [20]. Every operator in $\mathcal{G}_n$ has either eigenvalues ± 1 or $\pm i$. An $[[n,q,d;e]]$ EAQECC is a quantum code that encodes q logical quantum bits (qubits) into n physical qubits with the help of e maximally entangled pairs (e-bits) shared between sender and receiver, and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ single-qubit errors. Such an EAQECC is defined by a noncommuting group $\mathcal{S}_Q = \langle \bar{Z}_1, \ldots, \bar{Z}_s, \bar{Z}_{s+1}, \bar{X}_{s+1}, \ldots, \bar{Z}_{s+e}, \bar{X}_{s+e} \rangle \subset \mathcal{G}_n$ of size 2^{s+2e}, where $s+e+q=n$. We will continue to refer to the group $\mathcal{S}_Q$ as a "stabilizer," even though, being non-Abelian, it does not stabilize any state. The generators $\bar{Z}_i$ and $\bar{X}_i$ satisfy the following commutation relations:

*Author to whom correspondence should be addressed; minhsiuh@gmail.com

$$[\bar{Z}_i,\bar{Z}_j]=0 \quad \forall \quad i,j,$$
$$[\bar{X}_i,\bar{X}_j]=0 \quad \forall \quad i,j,$$
$$[\bar{X}_i,\bar{Z}_j]=0 \quad \forall \quad i\neq j, \tag{1}$$
$$\{\bar{X}_i,\bar{Z}_i\}=0 \quad \forall \quad i.$$

We define the isotropic subgroup $\mathcal{S}_{Q,I}$ of $\mathcal{S}_Q$ to be the group generated by $\{\bar{Z}_1,\ldots,\bar{Z}_s\}$; it is of size 2^s. Similarly, the symplectic subgroup $\mathcal{S}_{Q,S}$ of $\mathcal{S}_Q$ is of size 2^{2e} and is generated by $\{\bar{Z}_{s+1},\bar{X}_{s+1},\ldots,\bar{Z}_{s+e},\bar{X}_{s+e}\}$. The isotropic subgroup $\mathcal{S}_{Q,I}$ is Abelian; however, the symplectic subgroup $\mathcal{S}_{Q,S}$ is not. We can easily construct an Abelian extension of $\mathcal{S}_Q$ that acts on $n+e$ qubits, by specifying the following generators:

$$\bar{Z}_1\otimes I,$$
$$\vdots$$
$$\bar{Z}_s\otimes I,$$
$$\bar{Z}_{s+1}\otimes Z_1,$$
$$\bar{X}_{s+1}\otimes X_1,$$
$$\vdots$$
$$\bar{Z}_{s+e}\otimes Z_e,$$
$$\bar{X}_{s+e}\otimes X_e,$$

where the first n qubits are on the side of the sender (Alice) and the extra e qubits are taken to be on the side of the receiver (Bob). The operators Z_i or X_i to the right of the tensor product symbol above is the Pauli operator Z or X acting on Bob's ith qubit. The picture is that Alice and Bob initially share e e-bits; Alice encodes her q qubits together with her halves of the e entangled pairs and s ancilla qubits. Bob's qubits are his halves of the e entangled pairs. Because this code assumes pre-existing entanglement between Alice and Bob, it is an entanglement-assisted quantum-error-correcting code (EAQECC). We denote such an Abelian extension of the group $\mathcal{S}_Q$ by $\widetilde{\mathcal{S}}_Q$. This EAQECC can correct an error set $\mathbf{E}\subset\mathcal{G}_n$ if for all $E_1,E_2\in\mathbf{E}$, $E_2^\dagger E_1\in\mathcal{S}_{Q,I}\cup[\mathcal{G}_n-N(\mathcal{S}_Q)]$, where $N(\mathcal{S})$ is the normalizer of group $\mathcal{S}$.

III. CLASSICALLY ENHANCED QUANTUM-ERROR-CORRECTING CODES

In this section, we will present a quantum code that can transmit both classical and quantum information at the same time.

A. The stabilizer formalism

We define an $[[n,q:c,d;e]]$ entanglement-assisted, classically enhanced quantum-error-correcting code (EACQ) to be a quantum code which encodes q logical qubits and c classical bits into n physical qubits with the help of e e-bits. Our quantum information is given by the q-qubit state $|\phi\rangle\in(\mathcal{H}_2)^{\otimes q}$, and our classical information $i\in\{1,2,\ldots,2^c\}$ is represented by a vector $\mathbf{x}_i\in(\mathbb{Z}_2)^c$. Here, we keep the subscript i in $\mathbf{x}_i$ to remind the reader that $\mathbf{x}_i$ is the binary expression of i. Let us denote the q-dimensional Hilbert space of the original qubits by $\mathcal{H}\equiv(\mathcal{H}_2)^{\otimes q}$, and the subspaces of the n-dimensional encoded states by $\mathcal{C}^i$. Our encoding operations $\hat{U}^i_{\text{enc}}:\mathcal{H}\to\mathcal{C}^i$ consist of appending the ancilla states $|0\rangle^{\otimes s}$ and maximally entangled states $|\Phi_+\rangle^{\otimes e}$, where $s+e+q=n$ and $|\Phi_+\rangle\equiv\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$, to $|\phi\rangle$ followed by performing the unitary U_i. Thus, our encoded states, or "code words," are defined as

$$|\Psi_i\rangle\equiv U_i(|0\rangle^{\otimes s}\otimes|\Phi_+\rangle^{\otimes e}\otimes|\phi\rangle). \tag{2}$$

We require that $\langle\Psi_i|\Psi_j\rangle=\delta_{ij}$ so that the classical information is perfectly retrievable. We specify an $[[n,q:c,d;e]]$ EACQ by the pair of groups $(\mathcal{S}_Q,\mathcal{S}_C)$.

Theorem 1. The quantum stabilizer $\mathcal{S}_Q=\langle\mathcal{S}_{Q,I},\mathcal{S}_{Q,S}\rangle$ of the code is generated by $s+2e-c$ elements

$$\mathcal{S}_{Q,I}=\langle\bar{Z}_{c_1+1},\bar{Z}_{c_1+2},\ldots,\bar{Z}_s\rangle,$$
$$\mathcal{S}_{Q,S}=\langle\bar{Z}_{s+c_2+1},\bar{X}_{s+c_2+1},\ldots,\bar{Z}_{s+e},\bar{X}_{s+e}\rangle. \tag{3}$$

The classical stabilizer $\mathcal{S}_C=\langle\mathcal{S}_{C,I},\mathcal{S}_{C,S}\rangle$ of the code is generated by c elements

$$\mathcal{S}_{C,I}=\langle\bar{Z}_1,\bar{Z}_2,\ldots,\bar{Z}_{c_1}\rangle,$$
$$\mathcal{S}_{C,S}=\langle\bar{Z}_{s+1},\ldots,\bar{Z}_{s+c_2},\bar{X}_{s+1},\ldots,\bar{X}_{s+c_2}\rangle, \tag{4}$$

where $q+s+e=n$ and $c_1+2c_2=c$, such that $\forall\ g_j\in\widetilde{\mathcal{S}}_Q$,

$$g_j|\Psi_i\rangle=|\Psi_i\rangle, \tag{5}$$

and

$$g_j'|\Psi_i\rangle=(-1)^{x_{ij}}|\Psi_i\rangle, \tag{6}$$

where g_j' is the jth element of the generator set of $\widetilde{\mathcal{S}}_C$, which is the Abelian extension of $\mathcal{S}_C$ introduced in Sec. II, and x_{ij} is the jth element of $\mathbf{x}_i\in(\mathbb{Z}_2)^c$.

Proof. We begin with a canonical code that encodes the quantum information $|\phi\rangle\in(\mathcal{H}_2)^{\otimes q}$ together with classical information $\mathbf{x}_i$ in the following trivial way:

$$|\phi\rangle\overset{\mathbf{x}_i}{\rightarrow}|\psi_i\rangle=(X^{\mathbf{x}_a}|0\rangle^{\otimes c_1})|0\rangle^{\otimes(s-c_1)}\times[(X^{\mathbf{x}_{b_1}}Z^{\mathbf{x}_{b_2}}\otimes I^B)|\Phi_+\rangle^{\otimes c_2}]|\Phi_+\rangle^{\otimes e-c_2}|\phi\rangle, \tag{7}$$

where $\mathbf{x}_a\in(\mathbb{Z}_2)^{c_1}$ and $\mathbf{x}_{b_1}$, $\mathbf{x}_{b_2}\in(\mathbb{Z}_2)^{c_2}$, and I^B is the identity acting on Bob's qubits. Given a vector $\mathbf{u}\in(\mathbb{Z}_2)^k$, we define

$$X^{\mathbf{u}}=X^{u_1}\otimes\cdots\otimes X^{u_k},$$

and similarly for $Z^{\mathbf{v}}$ where $\mathbf{v}\in(\mathbb{Z}_2)^k$. The classical information $\mathbf{x}_i$ is encoded using elementary and superdense coding [14], respectively. Instead of encoding $\mathbf{x}_i$ as a whole, the first c_1 bits of $\mathbf{x}_i$ (denoted by $\mathbf{x}_a$) are encoded on the first c_1

ancillas using elementary encoding. The rest of $\mathbf{x}_i$ is further divided into two parts $\mathbf{x}_{b_1}$ and $\mathbf{x}_{b_2}$ of equal length, and are encoded on the first c_2 pairs of e-bits using superdense coding.

Clearly, the set $\{|\psi_i\rangle\}$ is stabilized by the Abelian extension of $\mathcal{S}'_Q=\langle\mathcal{S}'_{Q,I},\mathcal{S}'_{Q,S}\rangle$, where

$$\mathcal{S}'_{Q,I}=\langle Z_{c_1+1},Z_{c_1+2},\ldots,Z_s\rangle,$$

$$\mathcal{S}'_{Q,S}=\langle Z_{s+c_2+1},X_{s+c_2+1},\ldots,Z_{s+e},X_{s+e}\rangle. \quad (8)$$

Now let $\mathcal{S}'_C=\langle\mathcal{S}'_{C,I},\mathcal{S}'_{C,S}\rangle$, where

$$\mathcal{S}'_{C,I}=\langle Z_1,\ldots,Z_{c_1}\rangle, \quad \mathcal{S}'_{C,S}=\langle Z_{s+1},\ldots,Z_{s+c_2},X_{s+1},\ldots,X_{s+c_2}\rangle, \quad (9)$$

and let $\tilde{\mathcal{S}}'_C$ be the Abelian extension of $\mathcal{S}'_C$. Then it is easy to verify that

$$g'_j|\psi_i\rangle=(-1)^{x_{ij}}|\psi_i\rangle, \quad (10)$$

where g'_j is the jth generator of $\tilde{\mathcal{S}}'_C$.

Since $(\mathcal{S}'_Q,\mathcal{S}'_C)$ is isomorphic to $(\mathcal{S}_Q,\mathcal{S}_C)$, there exists a unitary U such that $\mathcal{S}_Q=U\mathcal{S}'_QU^\dagger$ and $\mathcal{S}_C=U\mathcal{S}'_CU^\dagger$ [14,21]. The code words $\{|\Psi_i\rangle\}$ can also be obtained by

$$U|\psi_i\rangle=|\Psi_i\rangle. \quad (11)$$

It is then easy to verify that Eqs. (5) and (6) hold. ■

Notice that $\langle\mathcal{S}_Q,\mathcal{S}_C\rangle$ is the stabilizer of an $[[n,q;e]]$ EAQECC code, and thus it fully specifies one of the code words from Eq. (2), $|\Psi_{\mathbf{0}}\rangle$. For $c>0$, the additional code words are just unitary transformations of $|\Psi_{\mathbf{0}}\rangle$. Theorem 1 confirms that $\mathcal{S}_C$ and $\mathcal{S}_Q$ together are sufficient to fully specify the code words.

Now that we have uniquely defined our code, we will consider the conditions that make a set of errors correctable, as well as the decoding procedure for a given set of correctable errors. We will consider here only error sets which are subsets of $\mathcal{G}^n$, since the ability to correct such a discrete error set implies the ability to correct any linear combination of errors in that set [14].

Theorem 2. A set of errors $\mathbf{E}\subset\mathcal{G}^n$ is correctable if for all E_m, $E_p\in\mathbf{E}$, $E_m^\dagger E_p\in\langle\mathcal{S}_{Q,I},\mathcal{S}_{C,I}\rangle\cup[\mathcal{G}^n-N(\mathcal{S}_Q)]$, where $N(\mathcal{S})$ is the normalizer of group $\mathcal{S}$.

Proof. We consider the following different cases.

(1) If $E_m^\dagger E_p\in\mathcal{G}^n-N(\mathcal{S}_Q)$, then by definition there is at least one element $g_j\in\mathcal{S}_Q$ such that

$$[E_m^\dagger E_p,g_j]\neq 0.$$

Then we are guaranteed that E_m and E_p have different error syndromes on the set of code words $\{|\Psi_i\rangle\}$. We can then perform a recovery operation based on the error syndrome. If it is determined that the error E_m occurred, the original code word may be recovered by simply performing the unitary E_m since $E_m\in\mathcal{G}^n$.

(2) If $E_m^\dagger E_p\in N(\mathcal{S}_Q)$, there are three cases. (a) If $E_m^\dagger E_p\in\mathcal{S}_{Q,I}$, then $E_m^\dagger E_p|\Psi_i\rangle=|\Psi_i\rangle$. The errors have the same syndrome, but they also act on the code space the same way. (This is the case of a degenerate code.) (b) If $E_m^\dagger E_p\in\mathcal{S}_{C,I}$, then by Eq. (6), $E_m^\dagger E_p|\Psi_i\rangle=\pm|\Psi_i\rangle$. The errors have the same syndrome, but their effects differ by a possible global phase without changing the classical information i embedded in the code word $|\Psi_i\rangle$. Therefore, we can still recover both the quantum and classical information (see Theorem 3). (c) For all the rest, the errors act nontrivially on the code words $\{|\Psi_i\rangle\}$, but do not have a unique syndrome. If this case applies to a pair of errors $E_m,E_p\in\mathbf{E}$ then the error set $\mathbf{E}$ is uncorrectable.

Combining these cases, we conclude that whenever $E_m^\dagger E_p\in\langle\mathcal{S}_{Q,I},\mathcal{S}_{C,I}\rangle\cup[\mathcal{G}^n-N(\mathcal{S}_Q)]$ $\forall\, E_m,E_p\in\mathbf{E}$, the code words $\{|\Psi_i\rangle\}$ can be recovered up to a possible global phase. ■

TABLE I. The error-correcting conditions of EAQECCs and EACQs.

EAQECC	EACQ
$E_m^\dagger E_p\notin N(\langle\mathcal{S}_{Q,I},\mathcal{S}_{Q,S}\rangle)$	$E_m^\dagger E_p\notin N(\langle\mathcal{S}_{Q,I},\mathcal{S}_{Q,S}\rangle)$
$E_m^\dagger E_p\in\mathcal{S}_{Q,I}$	$E_m^\dagger E_p\in\langle\mathcal{S}_{Q,I},\mathcal{S}_{C,I}\rangle$

Theorem 3. Once error recovery has been performed, the classical index i may be determined by measuring each of the $g'_k\in\tilde{\mathcal{S}}_C$ observables. The original quantum state $|\phi\rangle$ may be recovered by performing the unitary U_i^{-1} and then discarding the ancillae.

Proof. After we have performed error recovery, the state in our possession will be $\pm|\Psi_i\rangle$. Measuring the generator set $\{g'_k\}$ of $\tilde{\mathcal{S}}_C$ will guarantee proper identification of $\mathbf{x}_i$ by Eq. (6). Once the classical index has been identified, we can see from Eq. (2) that we may recover the original quantum state $|\phi\rangle$ by performing U_i^{-1} and discarding the states $\pm|0\rangle^{\otimes s}|\Phi_+\rangle^{\otimes e}$. ■

B. Properties of EACQs

Theorem 4. We can transform any $[[n,q+c,d_1;e]]$ EAQECC code $\mathcal{C}_1$ into an $[[n,q:c,d_2;e]]$ EACQ code $\mathcal{C}_2$, and transform any $[[n,q:c,d_2;e]]$ EACQ code $\mathcal{C}_2$ into an $[[n,q,d_3;e]]$ EAQECC code $\mathcal{C}_3$, where $d_1\le d_2\le d_3$.

Proof. The stabilizer group $\mathcal{S}_Q$ of $\mathcal{C}_1$ is of size 2^{s+2e}, where $s+q+c+e=n$. The isotropic subgroup $\mathcal{S}_{Q,I}$ and the symplectic subgroup $\mathcal{S}_{Q,S}$ of $\mathcal{S}_Q$ are of sizes 2^s and 2^{2e}, respectively. If we simply add an Abelian group $\mathcal{S}_C$ of size 2^c such that $\mathcal{S}_C\cap\mathcal{S}_Q=\{I\}$, then $(\mathcal{S}_Q,\mathcal{S}_C)$ defines an $[[n,q:c,d_2;e]]$ EACQ code $\mathcal{S}_2$ for some d_2, which follows from Theorem 1. Let $\mathbf{E}_1$ be the error set that can be corrected by $\mathcal{C}_1$, and $\mathbf{E}_2$ be the error set that can be corrected by $\mathcal{C}_2$. Clearly, $\mathbf{E}_1\subset\mathbf{E}_2$ (see Table I), so $\mathcal{C}_2$ can correct more errors than $\mathcal{C}_1$. Therefore, $d_2\ge d_1$.

In general, an $[[n,q:c,d_2;e]]$ EACQ code $\mathcal{C}_2$ is defined by $\mathcal{S}_Q=\langle\mathcal{S}_{Q,I},\mathcal{S}_{Q,S}\rangle$ and $\mathcal{S}_C=\langle\mathcal{S}_{C,I},\mathcal{S}_{C,S}\rangle$, where the isotropic subgroup $\mathcal{S}_{Q,I}$ and the symplectic subgroup $\mathcal{S}_{Q,S}$ of $\mathcal{S}_Q$ are of sizes 2^{s-c_1} and $2^{2(e-c_2)}$, respectively, and the isotropic subgroup $\mathcal{S}_{C,I}$ and the symplectic subgroup $\mathcal{S}_{C,S}$ of $\mathcal{S}_C$ are of sizes 2^{c_1} and 2^{2c_2}, respectively. Here the parameters satisfy $s+q+e=n$ and $c_1+2c_2=c$. Now let $\mathcal{S}'_{Q,I}=\langle\mathcal{S}_{Q,I},\mathcal{S}_{C,I}\rangle$ and $\mathcal{S}'_{Q,S}=\langle\mathcal{S}_{Q,S},\mathcal{S}_{C,S}\rangle$. Then $\mathcal{S}'_Q=\langle\mathcal{S}'_{Q,I},\mathcal{S}'_{Q,S}\rangle$ defines an $[[n,q,d_3;e]]$ EAQECC code $\mathcal{C}_3$. Let $\mathbf{E}_3$ be the error set that

TABLE II. The stabilizer $\mathcal{S}$ of the [[9,1,3]] Shor code.

	$\mathcal{S}$								
p_1	Z	Z	I	I	I	I	I	I	I
p_2	I	Z	Z	I	I	I	I	I	I
p_3	I	I	I	Z	Z	I	I	I	I
p_4	I	I	I	I	Z	Z	I	I	I
p_5	I	I	I	I	I	I	Z	Z	I
p_6	I	I	I	I	I	I	I	Z	Z
p_7	X	X	X	X	X	X	I	I	I
p_8	I	I	I	X	X	X	X	X	X

can be corrected by $\mathcal{C}_3$. Let $E \in \mathbf{E}_2$, then either $E \in \langle \mathcal{S}_{Q,I}, \mathcal{S}_{C,I} \rangle$ or $E \notin N(\mathcal{S}_Q)$. If $E \in \langle \mathcal{S}_{Q,I}, \mathcal{S}_{C,I} \rangle$, then $E \in \mathcal{S}'_{Q,I}$. Thus, $E \in \mathbf{E}_3$. Since $\mathcal{S}_Q \subset \mathcal{S}'_Q$, we have $N(\mathcal{S}'_Q) \subset N(\mathcal{S}_Q)$. If $E \notin N(\mathcal{S}_Q)$, then $E \notin N(\mathcal{S}'_Q)$. Thus, $E \in \mathbf{E}_3$. Putting these together we get $\mathbf{E}_2 \subset \mathbf{E}_3$. Therefore $d_3 \geq d_2$. ■

It is worth pointing out that the theory of EACQs naturally includes the set of classically enhanced quantum codes that do not require entanglement as a subclass. These would be codes for which there is no nontrivial symplectic subgroup for either $\mathcal{S}_Q$ or $\mathcal{S}_C$, so that both of these groups are purely isotropic. In terms of the parameters describing the code, this is the special case where $e=0$. Our first example in the next section is exactly such a code. To conclude this section, we list the different error-correcting criteria of an EAQECC and an EACQ.

IV. EXAMPLES

In the following, we will refer to a binary $(n-k)\times n$ matrix $H=[h_{i,j}]$ that defines a k-dimensional subspace over $(\mathbb{Z}_2)^n$ as a "parity check matrix." Let $\mathcal{S}\subset\mathcal{G}_m$, where $n<m$, be generated by $\{p_1,\ldots,p_n\}$. A new group $\mathcal{V}$ derived from $H\cdot\mathcal{S}$ means that the ith generator g_i of $\mathcal{V}$ is

$$g_i = \prod_{j=1}^{n} p_j^{h_{i,j}}.$$

A. [[9,1:2,3;0]] EACQ

We first give an example of a code that starts from an overly redundant quantum code, and exploits that redundancy to encode additional classical information. The example we pick is the well-known nine-qubit Shor code. The modified Shor code presented here encodes one qubit and two classical bits into nine physical qubits, and it is still able to correct an arbitrary error on a single qubit.

The code is a combination of the [9,1,3] Shor code defined by the stabilizer given in Table II, and the [8,2] classical code with parity check matrix H

TABLE III. The stabilizer $(\mathcal{S}_Q,\mathcal{S}_C)$ of the [[9,1:2,3;0]] EACQ that encodes one qubit and two classical bits into nine physical qubits.

	$\mathcal{S}_Q$								
g_1	Z	Z	I	Z	Z	I	Z	Z	I
g_2	I	Z	Z	I	Z	Z	I	Z	Z
g_3	Z	Z	I	I	Z	Z	I	I	I
g_4	I	Z	Z	Z	I	Z	I	I	I
g_5	X	X	X	X	X	X	I	I	I
g_6	I	I	I	X	X	X	X	X	X
	$\mathcal{S}_C$								
g'_1	Z	Z	I	I	I	I	I	I	I
g'_2	I	Z	Z	I	I	I	I	I	I

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (12)$$

The generators of $\mathcal{S}_Q$ and $\mathcal{S}_C$ as in Eqs. (5) and (6) for the code are given in Table III such that $g_i=\Pi_{j=1}^{8}p_j^{h_{i,j}}$ and g'_k is the kth generator of $\mathcal{S}_C=\mathcal{S}\backslash\mathcal{S}_Q$, where $h_{i,j}$ is the (i,j)th element of H, g_i is the ith generator of $\mathcal{S}_Q$, and p_j is the jth generator of $\mathcal{S}$.

Remark. Though we have used the jargon of classical coding theory in referring to H as a "parity check matrix," this is not really necessary. What we need here is a matrix that specifies the subsystem degrees of freedom of the original quantum code. While H technically does define a classical code, we have not made explicit use of the error-correcting properties of this code (such as its distance).

Proposition 5. The modified Shor code presented above can correct an arbitrary error on a single qubit.

Proof. This modified Shor code is degenerate. A single-qubit Z error on any of the qubits in the same triplet (that is, on any of qubits 1, 2, 3, or any of qubits 4, 5, 6, or any of qubits 7, 8, 9) result in the same error syndrome, and can be corrected using the same recovery operation. However, it is easily verified that each of the single-qubit X errors gives a distinct error syndrome and can therefore be corrected. The syndromes are obtained by measuring $\{g_1,\ldots,g_6\}$, but we omit the syndrome list for brevity. Since this code is a CSS-type QECC, the single-qubit Y errors can therefore be corrected. ■

B. [[8,1:2,3;1]] EACQ

The following example comes from modifying the [[8,1,3;1]] EAQECC given in Ref. [16]. The [[8,1:2,3;1]] EACQ comes from a combination of the [[8,1,3;1]] EAQECC given in Table IV and the [8,2] classical code with parity check matrix H

TABLE IV. This [[8,1,3;e=1]] EAQECC encodes one qubit into eight physical qubits with the help of one e-bit (e=1).

p_1	Z	Z	I	I	I	I	I	I
p_2	I	Z	Z	I	I	I	I	I
p_3	I	I	I	Z	Z	I	I	I
p_4	I	I	I	I	Z	Z	I	I
p_5	I	I	I	I	I	I	Z	Z
p_6	X	X	X	X	X	X	I	I
p_7	I	I	I	I	I	I	I	Z
p_8	I	I	I	X	X	X	X	X

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

Table V gives generators of $(\mathcal{S}_Q,\mathcal{S}_C)$ for the [[8,1:2,3;1]] EACQ. The resulting EACQ encodes one qubit and two classical bits into eight physical qubits with the help of one e-bit. Since the [[8,1,3;1]] code is also derived from the Shor code, this EACQ is closely related to our first example.

C. EACQ codes from classical BCH codes

Here, we start from the [[63,21,9;6]] EAQECC shown in Ref. [16], which is constructed from a classical binary [63,39,9] BCH code [22]. This EAQECC has the interesting property that removing the symplectic pairs from the quantum parity check matrix only decreases the distance from $d=9$ to $d=7$, no matter how many pairs are removed. Therefore, if we switch all the e-bits from $\mathcal{S}_Q$ to $\mathcal{S}_C$, we will have a [[63,21:12,7;6]] EACQ. This example shows that it is possible to encode extra classical information using e-bits without degrading the distance performance too much.

V. CONCLUSIONS

In this paper, we have demonstrated yet another extension of the standard quantum-error-correcting scheme. The EACQ can transmit both classical and quantum information simultaneously. We consider this EACQ formalism as a generalization and unification of both entanglement-assisted quantum coding theory and classical coding theory, in the following sense.

For a purely quantum code (c=0), we have $\mathcal{S}_C=\{I\}$. This corresponds to the entanglement-assisted formalism. In this case, the classical parity check matrix H is chosen to be $I_{(n-q)\times(n-q)}$ such that the stabilizer of the code stays the same.

TABLE V. The stabilizer $(\mathcal{S}_Q,\mathcal{S}_C)$ of the [[8,1:2,3;1]] EACQ that encodes one qubit and two classical bits into eight physical qubits with the help of one e-bit.

				$\mathcal{S}_{Q,I}$				
g_1	Z	Z	I	Z	Z	I	Z	Z
g_2	Z	Z	I	I	Z	Z	I	I
g_3	I	Z	Z	Z	I	Z	I	I
g_4	X	X	X	X	X	X	I	I
				$\mathcal{S}_{Q,S}$				
g_5	I	Z	Z	I	Z	Z	I	Z
g_6	I	I	I	X	X	X	X	X
				$\mathcal{S}_C$				
g_1'	Z	Z	I	I	I	I	I	I
g_2'	I	Z	Z	I	I	I	I	I

For a purely classical code (q=0), we can assume that the original quantum stabilizer is $\mathcal{S}=\{Z_1,\ldots,Z_n\}$. Then given an arbitrary classical parity check matrix H and its corresponding generator matrix G, the resulting quantum and classical stabilizer is $\mathcal{S}_Q=H\cdot\mathcal{S}$ and $\mathcal{S}_C=G\cdot\mathcal{S}$, respectively. The classical code can be thought of as encoded in the Z basis.

On the other hand, the EACQ formalism provides further flexibility in the use of quantum-error-correcting codes. As shown in Sec. IV, EACQs can make use of extra redundancy in quantum codes to encode additional classical information. We also note that the passive error-correcting ability of an EACQ is increased, though at the cost of the quantum code rate of an EAQECC.

We are currently investigating the relation between EACQs and other extensions of standard quantum-error-correcting codes, such as OQECCs or "operator algebra quantum error-correcting" codes (OAQECs) [23]. Recently we have become aware of Ref. [24], which also allows correction of hybrid classical-quantum information based on operator algebra. Given the wider variety of resources in quantum information theory compared to classical information theory, we can expect a correspondingly richer set of families of quantum-error-correcting codes.

ACKNOWLEDGMENTS

We wish to acknowledge enlightening discussions with Igor Devetak and Cedric Beny. We also want to thank the anonymous referee for pointing out that our first example could be done using stabilizer generators with a CSS structure. T.A.B. received financial support from NSF Grant No. CCF-0448658, and T.A.B. and M.-H.H. both received support from NSF Grant No. ECS-0507270. I.K. and M.-H.H. received financial support from NSF Grant No. CCF-0524811 and NSF Grant No. CCF-0545845.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[3] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997 (unpublished).
[4] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[5] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[6] S. Aly, A. Klappenecker, and P. K. Sarvepalli, e-print arXiv:quant-ph/0610153.
[7] D. Bacon, Phys. Rev. A **73**, 012340 (2006).
[8] A. Klappenecker and P. K. Sarvepalli, e-print arXiv:quant-ph/0604161.
[9] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).
[10] D. W. Kribs and R. W. Spekkens, Phys. Rev. A **74**, 042329 (2006).
[11] M. A. Nielsen and D. Poulin, Phys. Rev. A **75**, 064304 (2007).
[12] D. Poulin, Phys. Rev. Lett. **95**, 230504 (2005).
[13] G. Bowen, Phys. Rev. A **66**, 052313 (2002).
[14] T. Brun, I. Devetak, and M. H. Hsieh, e-print arXiv:quant-ph/0608027.
[15] T. Brun, I. Devetak, and M. H. Hsieh, Science **314**, 436 (2006).
[16] M.-H. Hsieh, I. Devetak, and T. Brun, Phys. Rev. A **76**, 062313 (2007).
[17] M.-H. Hsieh, T. Brun, and I. Devetak, e-print arXiv:0803.0100.
[18] M.-H. Hsieh (unpublished).
[19] I. Devetak, P. Hayden, and D. Leung (unpublished).
[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2000).
[21] S. Bravyi, D. Fattal, and D. Gottesman, J. Math. Phys. **47**, 062106 (2006).
[22] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes* (Elsevier, Amsterdam, 1977).
[23] C. Bény, A. Kempf, and D. W. Kribs, Phys. Rev. Lett. **98**, 100502 (2007).
[24] C. Beny, A. Kempf, and D. W. Kribs, e-print arXiv:0705.1574.