General entanglement-assisted quantum error-correcting codes

Min-Hsiu Hsieh,* Igor Devetak,† and Todd Brun‡
Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, California 90089, USA
(Received 16 August 2007; published 19 December 2007)

Entanglement-assisted quantum error-correcting codes (EAQECCs) make use of preexisting entanglement between the sender and receiver to boost the rate of transmission. It is possible to construct an EAQECC from any classical linear code, unlike standard QECCs, which can only be constructed from dual-containing codes. Operator quantum error-correcting codes allow certain errors to be corrected (or prevented) *passively*, reducing the complexity of the correction procedure. We combine these two extensions of standard quantum error correction into a unified entanglement-assisted quantum error-correction formalism. This new scheme, which we call entanglement-assisted operator quantum error correction (EAOQEC), is the most general and powerful quantum error-correcting technique known, retaining the advantages of both entanglement-assistance and passive correction. We present the formalism, show the considerable freedom in constructing EAOQECCs from classical codes, and demonstrate the construction with examples.

DOI: 10.1103/PhysRevA.76.062313 PACS number(s): 03.67.Lx

I. INTRODUCTION

Conventional quantum error-correcting codes are simultaneous eigenspaces of a group of commuting operators, the stabilizer group. A construction of Calderbank and Shor and Steane [1,2] showed that it was possible to construct quantum codes from classical binary codes—the CSS codes—thereby drawing on the well-studied theory of classical error correction. Later on, it was shown that [3,4] the construction of quantum codes from classical codes can be put in a more general framework, the stabilizer formalism. This gave, among other important benefits, a strong connection between quantum error-correcting codes and classical symplectic codes, which are closely related to linear quaternary codes [that is, linear codes over $GF(4)$].

This connection between classical codes and quantum codes is not universal, however. Rather, only classical codes that satisfy a dual-containing constraint (i.e., that have self-orthogonal parity-check matrices) can be used to construct standard quantum codes. While this constraint is not too difficult to satisfy for relatively small codes, it is a substantial barrier to the use of highly efficient modern codes, such as turbo codes and low-density parity check (LDPC) codes, in quantum information theory. These codes are capable of achieving the classical capacity; but the difficulty of constructing dual-containing versions of them has made progress toward quantum versions very slow.

Recently, there have been two major breakthroughs in quantum error-correction theory. The first was the discovery of operator quantum error-correcting codes (OQECCs) [5–12]. These provide a general theory which combines passive error-avoiding schemes, such as decoherence-free subspaces [13] and noiseless subsystems [14], with conventional (active) quantum error correction. In a certain sense, OQECC does not lead to new codes, but instead provides a new kind of decoding procedure: it is not necessary to actively correct all errors, but rather only to perform correction modulo on the subsystem structure. One potential benefit of the new decoding procedure is to improve the threshold of fault-tolerant quantum computation [6].

The second breakthrough was the development of a theory of entanglement-assisted quantum error-correcting codes [15–17]. In this theory, it is assumed that in addition to a quantum channel, the sender and receiver share a certain amount of preexisting entanglement. The entanglement-assisted quantum error-correcting codes (EAQECC) formalism can be applied to any classical quaternary code, not just dual-containing ones, and the performance of the resulting quantum code (that is, its minimum distance and net rate) is determined by the performance of the classical code. (OQECCs also allow quantum codes to be constructed from classical codes which do not obey the dual-containing constraint, but in this case the performance of the quantum codes cannot be predicted from the performance of the classical codes).

Within the framework of EAQECCs, the existing theory of quantum error becomes a special case in which the needed entanglement is zero. Classical dual-containing codes give rise to standard quantum codes, while all other classical codes give rise to EAQECCs. In a similar way, standard QECCs can also be thought of as a special of OQECCs, where the protected subsystem is the entire system. In this paper, we move one step further, by incorporating both operator quantum error correction and entanglement-assisted quantum error correction into a single unified formalism. This unified scheme is the most general theory of quantum error correction currently known.

We now briefly outline the structure of this paper. In Sec. II, we review the construction of EAQECCs and OQECCs as extensions of the usual stabilizer formalism. In Sec. III, we provide the theoretical derivation of EAOQECCs, and briefly discuss the relationship between conventional QECCs, OQECCs, EAQECCs, and EAOQECCs. In Sec. IV, we give some examples of EAOQECCs, and show how one can make trade-offs between entanglement-assistance and passive error correction. Finally, in Sec. V, we conclude with a

*minhsiuh@usc.edu
†devetak@usc.edu
‡tbrun@usc.edu

discussion of how the entanglement-assisted operator formalism allows us to construct versatile classes of EAOQECCs from classical linear codes, with varying powers of passive versus active error correction.

II. REVIEW OF EAQECCS AND OQECCS

First, let us recall the stabilizer formalism for conventional quantum error-correcting codes. Let $\mathcal{G}_n$ be the n-fold Pauli group [18]. Every operator in $\mathcal{G}_n$ has either eigenvalues ± 1 or $\pm i$. Let $\mathcal{S}\subset\mathcal{G}_n$ be an Abelian subgroup which does not contain $-I$. Then this subgroup has a common eigenspace $C(\mathcal{S})$ of $+1$ eigenvectors, which we call the *code space* determined by the stabilizer $\mathcal{S}$. Later on, we will just use C to denote the code space. Typically, the stabilizer is represented by a minimal generating set $\{g_1,\ldots,g_m\}$, which makes this a very compact way to specify a code (analogous to specifying a classical linear code by its parity-check matrix). We write $\mathcal{S}=\langle g_1,\ldots,g_m\rangle$ to denote that $\mathcal{S}$ is generated by $\{g_1,\ldots,g_m\}$.

Let $\mathbf{E}\subset\mathcal{G}_n$ be a set of possible errors. If a particular error $E_1\in\mathbf{E}$ anticommutes with any of the generators of $\mathcal{S}$, then the action of that error can be detected by measuring the generators; if the measurement returns -1 instead of 1, we know an error has occurred. On the other hand, if the error is actually *in* the stabilizer $\mathcal{S}$, then it leaves all the states in C unchanged. We can conclude that the code C can correct any error in $\mathbf{E}$ if either $E_2^\dagger E_1\notin\mathcal{Z}(\mathcal{S})$ or $E_2^\dagger E_1\in\mathcal{S}$ for all pairs of errors E_1 and E_2 in $\mathbf{E}$, where $\mathcal{Z}(\mathcal{S})$ is the *centralizer* of $\mathcal{S}$.

We can now generalize this description to the entanglement-assisted case. Given a *nonabelian* subgroup $\mathcal{S}\subset\mathcal{G}_n$ of size 2^m, there exists a set of generators $\{\bar{Z}_1,\ldots,\bar{Z}_{s+c},\bar{X}_{s+1},\ldots,\bar{X}_{s+c}\}$ for $\mathcal{S}$ with the following commutation relations:

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

The parameters s and c satisfy $s+2c=m$. Let $\mathcal{S}_I$ be the *isotropic* subgroup generated by $\{\bar{Z}_1,\ldots,\bar{Z}_s\}$ and $\mathcal{S}_E$ be the *entanglement* subgroup generated by $\{\bar{Z}_{s+1},\ldots,\bar{Z}_{s+c},\bar{X}_{s+1},\ldots,\bar{X}_{s+c}\}$. The sizes of $\mathcal{S}_I$ and $\mathcal{S}_E$ describe the number of ancillas and the number of ebits needed to construct EAQECCs, respectively. (An ebit is one copy of a maximally entangled pair.) The pair of subgroups $(\mathcal{S}_I,\mathcal{S}_E)$ defines an $[[n,k;c]]$ EAQECCC^{EA} that encodes $k=n-s-c$ logical qubits into n physical qubits, with the help of c ebits shared between sender and receiver and s ancillas. These n qubits are transmitted from Alice (the sender) to Bob (the receiver), who measures them together with his half of the c ebits in order to correct any errors and decode the k logical qubits. We define $(k-c)/n$ as the net rate of the code. This EAQECC C^{ea} can correct an error set $\mathbf{E}$ if for all $E_1,E_2\in\mathbf{E}$, $E_2^\dagger E_1\in\mathcal{S}_I\cup[\mathcal{G}_n-\mathcal{Z}(\langle\mathcal{S}_I,\mathcal{S}_E\rangle)]$.

The starting point for OQECCs is similar to that for EAQECCs. Let the nonabelian group $\mathcal{S}\subset\mathcal{G}_n$ of size 2^m be generated by $\{\bar{Z}_1,\ldots,\bar{Z}_{s+r},\bar{X}_{s+1},\ldots,\bar{X}_{s+r}\}$, where $\bar{Z}$'s and $\bar{X}$'s obey the same commutation relations as in Eq. (1), and the parameters s and r satisfy $s+2r=m$. Let $\mathcal{S}_I=\langle\bar{Z}_1,\ldots,\bar{Z}_s\rangle$ be the isotropic subgroup, and let $\mathcal{S}_G=\langle\bar{Z}_{s+1},\ldots,\bar{Z}_{s+r},\bar{X}_{s+1},\ldots,\bar{X}_{s+r}\rangle$ be the *gauge* subgroup. The size of $\mathcal{S}_I$ and $\mathcal{S}_G$ describes the number of ancillas and the number of gauge qubits (gauge qubits can be thought of as redundant logical qubits to accommodate more errors) needed to construct OQECCs, respectively. Then the pair of subgroups $(\mathcal{S}_I,\mathcal{S}_G)$ defines an $[[n,k;r]]$ OQECC C^{op} that fixes a 2^{r+k}-dimensional code space, where $s+k+r=n$. Furthermore, the gauge subgroup $\mathcal{S}_G$ defines an equivalence between pairs of states inside the code space: the two states ρ and ρ' are considered to carry the same information if they differ by the action of a quantum operation in the algebra generated by $\mathcal{S}_G$. These r logical gauge qubits provide extra power of passive error correction. This OQECC C^{op} can correct an error set $\mathbf{E}$ if for all $E_1,E_2\in\mathbf{E}$, $E_2^\dagger E_1\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle\cup[\mathcal{G}_n-\mathcal{Z}(\mathcal{S}_I)]$.

III. ENTANGLEMENT-ASSISTED OPERATOR QUANTUM ERROR-CORRECTING CODES

A. Canonical code

We illustrate the idea of EAOQECCs by the following canonical code. Consider the trivial encoding operation $\mathcal{E}_0$ defined by

$$\mathcal{E}_0:|\psi\rangle\langle\psi|\to|\mathbf{0}\rangle\langle\mathbf{0}|\otimes|\Phi\rangle\langle\Phi|\otimes\sigma\otimes|\psi\rangle\langle\psi|. \tag{2}$$

The operation simply appends s ancilla qubits in the state $|\mathbf{0}\rangle$, c copies of $|\Phi\rangle$ (a maximally entangled state shared between sender Alice and receiver Bob), and an arbitrary state σ of size r qubits, to the initial register containing the state $|\psi\rangle$ of size k qubits, where $s+k+r+c=n$. These r extra qubits are the gauge qubits. Two states of this form, which differ only in σ, are considered to encode the same quantum information.

Proposition 1. The encoding given by $\mathcal{E}_0$ and a suitably defined decoding map $\mathcal{D}_0$ can correct the error set

$$
\begin{aligned}
\mathbf{E}_0=\{&X^{\mathbf{a}}Z^{\mathbf{b}}\otimes Z^{\mathbf{a}_1}X^{\mathbf{a}_2}\otimes X^{\mathbf{c}}Z^{\mathbf{d}}\otimes X^{\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}Z^{\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}:\mathbf{a},\mathbf{b}\\
&\in(\mathbb{Z}_2)^s,\mathbf{a}_1,\mathbf{a}_2\in(\mathbb{Z}_2)^c,\mathbf{c},\mathbf{d}\in(\mathbb{Z}_2)^r\},
\end{aligned}
\tag{3}
$$

for any fixed functions $\alpha,\beta:(\mathbb{Z}_2)^s\times(\mathbb{Z}_2)^c\times(\mathbb{Z}_2)^c\to(\mathbb{Z}_2)^k$.

Proof. After applying an error $E\in\mathbf{E}_0$, the channel output becomes (up to a phase factor)

$$
\begin{aligned}
&(X^{\mathbf{a}}Z^{\mathbf{b}})|\mathbf{0}\rangle\langle\mathbf{0}|(X^{\mathbf{a}}Z^{\mathbf{b}})^\dagger\\
&\quad\otimes(Z^{\mathbf{a}_1}X^{\mathbf{a}_2}\otimes I^B)|\Phi\rangle\langle\Phi|(Z^{\mathbf{a}_1}X^{\mathbf{a}_2}\otimes I^B)^\dagger\otimes(X^{\mathbf{c}}Z^{\mathbf{d}})\sigma(X^{\mathbf{c}}Z^{\mathbf{d}})^\dagger\\
&\quad\otimes(X^{\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}Z^{\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)})|\psi\rangle\langle\psi|(X^{\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}Z^{\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)})^\dagger\\
&\quad=|\mathbf{a}\rangle\langle\mathbf{a}|\otimes=|\mathbf{a}_1,\mathbf{a}_2\rangle\langle\mathbf{a}_1,\mathbf{a}_2|\otimes\sigma'\otimes|\psi'\rangle\langle\psi'|,
\end{aligned}
\tag{4}
$$

where $|\mathbf{a}\rangle=X^{\mathbf{a}}|\mathbf{0}\rangle$, $|\mathbf{a}_1,\mathbf{a}_2\rangle=(Z^{\mathbf{a}_1}X^{\mathbf{a}_2}\otimes I^B)|\Phi\rangle^{\otimes c}$, $\sigma'=(X^{\mathbf{c}}Z^{\mathbf{d}})\sigma(X^{\mathbf{c}}Z^{\mathbf{d}})^\dagger$, and $|\psi'\rangle=(X^{\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}Z^{\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)})|\psi\rangle$. Here we write, e.g.,

$$X^{\mathbf{a}} \equiv X^{a_1} \otimes X^{a_2} \otimes \cdots X^{a_s},$$

where $\mathbf{a}=(a_1,\ldots,a_s)\in(\mathbb{Z}_2)^s$, $X^0=I$, and $X^1=X$. As the vector $(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2,\mathbf{b},\mathbf{c},\mathbf{d})$ completely specifies the error operator E, it is called the *error syndrome*. However, in order to correct this error, only the *reduced syndrome* $(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)$ matters. Here two kinds of passive error correction are involved. The errors that come from vector $\mathbf{b}$ are passively corrected because they do not affect the encoded state given in Eq. (2). The errors that come from vector $(\mathbf{c},\mathbf{d})$ are passively corrected because of the subsystem structure inside the code space: $\rho\otimes\sigma$ and $\rho\otimes\sigma'$ represent the same information, differing only by a gauge operation.

The decoding operation $\mathcal{D}_0$ is constructed based on the reduced syndrome, and is also known as *collective measurement*. Bob can recover the state $|\psi\rangle$ by performing the decoding $\mathcal{D}_0$ as follows:

$$\mathcal{D}_0=\sum_{\mathbf{a},\mathbf{a}_1,\mathbf{a}_2}|\mathbf{a}\rangle\langle\mathbf{a}|\otimes|\mathbf{a}_1,\mathbf{a}_2\rangle\langle\mathbf{a}_1,\mathbf{a}_2|\otimes I\otimes X^{-\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}Z^{-\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}, \tag{5}$$

followed by discarding the unwanted systems. ■

We can rephrase the above error-correcting procedure in terms of the stabilizer formalism. Let $\mathcal{S}_0=\langle\mathcal{S}_{0,I},\mathcal{S}_{0,S}\rangle$, where $\mathcal{S}_{0,I}=\langle Z_1,\ldots Z_s\rangle$ is the isotropic subgroup of size 2^s and $\mathcal{S}_{0,S}=\langle Z_{s+1},\ldots,Z_{s+c+r},X_{s+1},\ldots,X_{s+c+r}\rangle$ is the *symplectic* subgroup of size $2^{2(c+r)}$. We can further divide the symplectic subgroup $\mathcal{S}_{0,S}$ into an entanglement subgroup

$$\mathcal{S}_{0,E}=\langle Z_{s+1},\ldots,Z_{s+c},X_{s+1},\ldots,X_{s+c}\rangle$$

of size 2^{2c} and a gauge subgroup

$$\mathcal{S}_{0,G}=\langle Z_{s+c+1},\ldots,Z_{s+c+r},X_{s+c+1},\ldots,X_{s+c+r}\rangle$$

of size 2^{2r}, respectively. The generators of $(\mathcal{S}_{0,I},\mathcal{S}_{0,E},\mathcal{S}_{0,G})$ are arranged in the following form:

$$\begin{array}{cccc} Z^{\mathbf{e}_i} & I & I & I \\ I & Z^{\mathbf{e}_j} & I & I \\ I & X^{\mathbf{e}_j} & I & I \\ I & I & Z^{\mathbf{e}_l} & I \\ I & I & X^{\mathbf{e}_l} & I \\ \overleftrightarrow{s} & \overleftrightarrow{c} & \overleftrightarrow{r} & \overleftrightarrow{k} \end{array}, \tag{6}$$

where $\{\mathbf{e}_i\}_{i\in[s]}$, $\{\mathbf{e}_j\}_{j\in[c]}$, and $\{\mathbf{e}_l\}_{l\in[r]}$ are the set of standard bases in $(\mathbb{Z}_2)^s$, $(\mathbb{Z}_2)^c$, and $(\mathbb{Z}_2)^r$, respectively, and $[k]\equiv\{1,\ldots,k\}$.

It follows that the three subgroups $(\mathcal{S}_{0,I},\mathcal{S}_{0,E},\mathcal{S}_{0,G})$ define the canonical EAOQECC given in Eq. (2). The subgroups $\mathcal{S}_{0,I}$ and $\mathcal{S}_{0,E}$ define a 2^{k+r}-dimensional code space $C_0^{\text{EAO}}\subset\mathcal{H}^{\otimes(n+c)}$, and the gauge subgroup $\mathcal{S}_{0,G}$ specifies all possible operations that can happen on the gauge qubits. Thus we can use $\mathcal{S}_{0,G}$ to define an equivalence class between two states in the code space of the form $\rho\otimes\sigma$ and $\rho\otimes\sigma'$, where ρ is a state on $\mathcal{H}^{\otimes k}$, and σ,σ' are states on $\mathcal{H}^{\otimes r}$. Consider the parameters of the canonical code. The number of ancillas s is equal to the number of generators for the isotropic subgroup $\mathcal{S}_{0,I}$. The number of ebits c is equal to the number of symplectic pairs that generate the entanglement subgroup $\mathcal{S}_{0,E}$. The number of gauge qubits r is equal to the number of symplectic pairs for the gauge subgroup $\mathcal{S}_{0,G}$. Finally, the number of logical qubits k that can be encoded in C_0^{EAO} is equal to $n-s-c-r$. To sum up, C_0^{eao} defined by $(\mathcal{S}_{0,I},\mathcal{S}_{0,E},\mathcal{S}_{0,G})$ is an $[[n,k;r,c]]$ EAOQECC that fixes a 2^{k+r}-dimensional code space, within which $\rho\otimes\sigma$ and $\rho\otimes\sigma'$ are considered to carry the same information. Notice that there is a trade-off between the number of encoded bits and gauge bits, in that we can reduce the rate by improving the error-avoiding ability or vice versa.

Proposition 2. The EAOQECC C_0^{EAO} defined by $(\mathcal{S}_{0,I},\mathcal{S}_{0,E},\mathcal{S}_{0,G})$ can correct an error set $\mathbf{E}_0$ if for all $E_1,E_2\in\mathbf{E}_0$, $E_2^{\dagger}E_1\in\langle\mathcal{S}_{0,I},\mathcal{S}_{0,G}\rangle\cup[\mathcal{G}_n-\mathcal{Z}(\langle\mathcal{S}_{0,I},\mathcal{S}_{0,E}\rangle)]$.

Proof. Since the vector $(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2,\mathbf{b},\mathbf{c},\mathbf{d})$ completely specifies the error operator E, we consider the following two different cases:

(1) If two error operators E_1 and E_2 have the same reduced syndrome $(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)$, then the error operator $E_2^{\dagger}E_1$ gives us all-zero reduced syndrome with some vector $(\mathbf{b},\mathbf{c},\mathbf{d})$. Therefore, $E_2^{\dagger}E_1\in\langle\mathcal{S}_{0,I},\mathcal{S}_{0,G}\rangle$. This error $E_2^{\dagger}E_1$ has no effect on the logical state $|\psi\rangle\langle\psi|$.

(2) If two error operators E_1 and E_2 have different reduced syndromes, and let $(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)$ be the reduced syndrome of $E_2^{\dagger}E_1$, then $E_2^{\dagger}E_1\notin Z(\langle\mathcal{S}_{0,I},\mathcal{S}_{0,E}\rangle)$. This error $E_2^{\dagger}E_1$ can be corrected by the decoding operation given in Eq. (5). ■

B. General case

Before giving the theorem, we first state two lemmas that lead directly to the result.

Lemma 1. Let $\mathcal{V}$ be an arbitrary subgroup of $\mathcal{G}_n$ with size 2^m. Then there exists a set of generators $\{\bar{Z}_1,\ldots,\bar{Z}_{p+q},\bar{X}_{p+1},\ldots,\bar{X}_{p+q}\}$ that generates $\mathcal{V}$ such that $\bar{Z}$'s and $\bar{X}$'s obey the same commutation relations as in Eq. (1), for some $p,q\geqslant 0$ and $p+2q=m$.

Proof. The idea of this proof comes from Gram-Schmidt orthogonality. By performing a Gram-Schmidt-type procedure, we can obtain a set of generators satisfying the commutation relations as in Eq. (1). See Ref. [16] for more detail. ■

Consider an arbitrary nonabelian group $\mathcal{S}$ of size $2^{s+2(c+r)}$, for some $s,c,r\geqslant 0$, Lemma 1 says that there exists a set of generators $\{\bar{Z}_1,\ldots,\bar{Z}_{s+c+r},\bar{X}_{s+1},\ldots,\bar{X}_{s+c+r}\}$ such that $\mathcal{S}=\langle\mathcal{S}_I,\mathcal{S}_S\rangle$, where $\mathcal{S}_I=\langle\bar{Z}_1,\ldots,\bar{Z}_s\rangle$ is the isotropic subgroup, and $\mathcal{S}_S=\langle\bar{Z}_{s+1},\ldots,\bar{Z}_{s+c+r},\bar{X}_{s+1},\ldots,\bar{X}_{s+c+r}\rangle$ is the symplectic subgroup. Furthermore, the symplectic subgroup $\mathcal{S}_S$ can be divided into the entanglement subgroup $\mathcal{S}_E$ of size 2^{2c} and the gauge subgroup $\mathcal{S}_G$ of size 2^{2r}.

Lemma 2. If there is a one-to-one map between $\mathcal{V}$ and $\mathcal{S}$ which preserves their commutation relations, which we denote $\mathcal{V}\sim\mathcal{S}$, then there exists a unitary U such that for each $V_i\in\mathcal{V}$, there is a corresponding $S_i\in\mathcal{S}$ such that $V_i=US_iU^{-1}$, up to a phase which can differ for each generator.

Proof. This lemma holds if two groups are isomorphic. We provide an independent proof in Ref. [16]. ■

This lemma enables us to link the group $\mathcal{S}$ to $\mathcal{S}_0$ [in other words, map $(\mathcal{S}_I,\mathcal{S}_E,\mathcal{S}_G)$ to $(\mathcal{S}_{0,I},\mathcal{S}_{0,E},\mathcal{S}_{0,G})$] by some unitary U such that

$$Z_i = U\bar{Z}_i U^{-1} \quad \forall \;\; i \in \{1,2,\ldots,s+c+r\},$$

$$X_j = U\bar{X}_j U^{-1} \quad \forall \;\; j \in \{s+1,\ldots,s+c+r\}. \tag{7}$$

Let U also denote the trivial extension of U that acts as the identity on the qubits on Bob's side. We can now define an $[[n,k;r,c]]$ EAOQECC C^{EAO} by $(\mathcal{S}_I,\mathcal{S}_S,\mathcal{S}_G)$, that incorporates both entanglement-assistance and passive error-avoiding ability.

We now reach our main theorem in this paper.

Theorem 1. Given the subgroups $(\mathcal{S}_I,\mathcal{S}_E,\mathcal{S}_G)$, there exists an $[[n,k;r,c]]$ entanglement-assisted operator quantum error-correcting code C^{EAO} defined by the encoding and decoding pair: $(\mathcal{E},\mathcal{D})$. The code C^{EAO} can correct the error set $\mathbf{E}$ if for all $E_1,E_2\in\mathbf{E}$, $E_2^\dagger E_1\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle\cup[\mathcal{G}_n-\mathcal{Z}(\langle\mathcal{S}_I,\mathcal{S}_E\rangle)]$.

Proof. Since $\mathcal{S}\sim\mathcal{S}_0$, there exists a unitary matrix U that preserves the commutation relations. Define $\mathcal{E}=U^{-1}\circ\mathcal{E}_0$ and $\mathcal{D}=\mathcal{D}_0\circ U$, where $\mathcal{E}_0$ and $\mathcal{D}_0$ are given in Eqs. (2) and (5), respectively. Since

$$\mathcal{D}_0\circ E_0\circ\mathcal{E}_0=\text{id}^{\otimes k}$$

for any $E_0\in\mathbf{E}_0$, then

$$\mathcal{D}\circ E\circ\mathcal{E}=\text{id}^{\otimes k}$$

follows for any $E\in\mathbf{E}$. Thus, the encoding and decoding pair $(\mathcal{E},\mathcal{D})$ corrects $\mathbf{E}$. ∎

C. Properties of EAOQECCs

Conventionally, the performance of a code is characterized by its distance d. Define the *weight* of a Pauli operator to be the number of single-qubit operators that are not the identity. We say that the $[[n,k,d;r,c]]$ EAOQECC C^{EAO} has distance d if it can correct any error set $\mathbf{E}$ such that for each operator $E\in\mathbf{E}$, the weight t of E satisfies $2t+1\leqslant d$.

In the description earlier in this section, we assumed that the gauge subgroup was generated by a set of symplectic pairs of generators. In some cases, it may make sense to start with a gauge subgroup which itself has both an isotropic (i.e., commuting) and a symplectic subgroup. In this case, we can arbitrarily add a symplectic partner for each generator in the isotropic subgroup of the gauge group. This can be useful in constructing EAOQECCs from EAQECCs, in a way analogous to how OQECCs can be constructed by starting from standard QECCs. Poulin shows in Ref. [12] that it is possible to move generators from the stabilizer group into the gauge subgroup, together with their symplectic partners, without changing the essential features of the original code. We provide an example of such a construction in Sec. IV A. There is further flexibility in trading between active error correction ability and passive noise avoiding ability [5]. This is captured by the following theorem:

Theorem 2. We can transform any $[[n,k+r,d_1;0,c]]$ code C_1 into an $[[n,k,d_2;r,c]]$ code C_2, and transform the $[[n,k,d_2;r,c]]$ code C_2 into an $[[n,k,d_3;0,c]]$ code C_3, where $d_1\leqslant d_2\leqslant d_3$.

Proof. There exists an isotropic subgroup $\mathcal{S}_I$ and an entanglement subgroup $\mathcal{S}_E$ associated with C_1 of size 2^s and 2^{2c}, respectively. These parameters satisfy $s+c+k+r=n$. This code C_1 corresponds to an $[[n,k+r,d_1;0,c]]$ EAQECC for some d_1. If we add the gauge subgroup $\mathcal{S}_G$ of size 2^{2r}, then $(\mathcal{S}_I,\mathcal{S}_E,\mathcal{S}_G)$ defines an $[[n,k,d_2;r,c]]$ EAOQECC C_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 the following table), so $\mathcal{C}_2$ can correct more errors than $\mathcal{C}_1$. By sacrificing part of the transmission rate, we have gained additional passive correction, and $d_2\geqslant d_1$.

If we now throw away half of each symplectic pair in $\mathcal{S}_G$ and include the remaining generators in $\mathcal{S}_I$, which becomes $\mathcal{S}_I'$, the size of the isotropic subgroup increases by a factor of 2^r. Then $(\mathcal{S}_I',\mathcal{S}_E)$ defines an $[[n,k,d_3;0,c]]$ EAQECC C_3. Let $\mathbf{E}_3$ be the error set that can be corrected by C_3. Let $E\in\mathbf{E}_2$, then either $E\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle$ or $E\notin\mathcal{Z}(\langle\mathcal{S}_I,\mathcal{S}_E\rangle)$.

(1) If $E\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle$, then either $E\in\mathcal{S}_I'$ or $E\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle/\mathcal{S}_I'$. If $E\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle/\mathcal{S}_I'$, this implies $E\notin\mathcal{Z}(\mathcal{S}_I')$. Thus, $E\in\mathbf{E}_3$.

(2) Since $\langle\mathcal{S}_I,\mathcal{S}_E\rangle\subset\langle\mathcal{S}_I',\mathcal{S}_E\rangle$, we have $\mathcal{Z}(\langle\mathcal{S}_I',\mathcal{S}_E\rangle)\subset\mathcal{Z}(\langle\mathcal{S}_I,\mathcal{S}_E\rangle)$. If $E\notin\mathcal{Z}(\langle\mathcal{S}_I,\mathcal{S}_E\rangle)$, then $E\notin\mathcal{Z}(\langle\mathcal{S}_I',\mathcal{S}_E\rangle)$. Thus, $E\in\mathbf{E}_3$.

Putting these together we get $\mathbf{E}_2\subset\mathbf{E}_3$. Therefore $d_3\geqslant d_2$. ∎

To conclude this section, we list the different error-correcting criteria of a conventional stabilizer code (QECC), an EAQECC, an OQECC, and an EAOQECC as follows:

QECC	EAQECC
$E_2^\dagger E_1\notin\mathcal{Z}(\mathcal{S}_I)$	$E_2^\dagger E_1\notin\mathcal{Z}(\langle\mathcal{S}_I,\mathcal{S}_E\rangle)$
$E_2^\dagger E_1\in\mathcal{S}_I$	$E_2^\dagger E_1\in\mathcal{S}_I$

OQECC	EAOQECC
$E_2^\dagger E_1\notin\mathcal{Z}(\mathcal{S}_I)$	$E_2^\dagger E_1\notin\mathcal{Z}(\langle\mathcal{S}_I,\mathcal{S}_E\rangle)$
$E_2^\dagger E_1\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle$	$E_2^\dagger E_1\in\langle\mathcal{S}_I,\mathcal{S}_G\rangle$

IV. EXAMPLES

A. EAOQECC from EAQECC

Our first example constructs an $[[8,1,3;c=1,r=2]]$ EAOQECC from an [[8,1,3;1]] EAQECC. Consider the EAQECC code defined by the group $\mathcal{S}$ generated by the operators in Table I. Here $\bar{Z}$ and $\bar{X}$ refer to the logical Z and X operation on the codeword, respectively. The isotropic subgroup is $\mathcal{S}_I=\langle S_1,S_2,S_3,S_4,S_5,S_8\rangle$, the entanglement subgroup is $\mathcal{S}_E=\langle S_6,S_7\rangle$, and together they generate the full group $\mathcal{S}=\langle\mathcal{S}_I,\mathcal{S}_E\rangle$. This code $C(\mathcal{S}_I,\mathcal{S}_E)$ encodes one qubit into eight physical qubits with the help of one ebit, and therefore is an $[[8,1;1]]$ code. It can be easily checked that this code can correct an arbitrary single-qubit error, and it is degenerate.

By inspecting the group structure of $\mathcal{S}$, we can recombine the first four stabilizers of the code to give two isotropic generators (which we retain in $\mathcal{S}_I$), and two generators which we include, together with their symplectic partners, in the subgroup $\mathcal{S}_G$, for two qubits of gauge symmetry. This yields an $[[8,1,3;c=1,r=2]]$ EAOQECC whose generators are

TABLE I. This [[8,1,3;$c=1$]] EAQECC encodes one qubit into eight physical qubits with the help of one ebit ($c=1$).

	Alice								Bob
S_1	Z	Z	I	I	I	I	I	I	I
S_2	Z	I	Z	I	I	I	I	I	I
S_3	I	I	I	Z	Z	I	I	I	I
S_4	I	I	I	Z	I	Z	I	I	I
S_5	I	I	I	I	I	I	Z	Z	I
S_6	I	I	I	I	I	I	I	Z	Z
S_7	X	X	X	I	I	I	X	X	X
S_8	X	X	X	X	X	X	I	I	I
$\bar{Z}$	Z	I	I	Z	I	I	I	Z	I
$\bar{X}$	I	I	I	X	X	X	I	I	I

given in Table II where $\mathcal{S}_I=\langle S_1',S_2',S_3',S_6'\rangle$, $\mathcal{S}_E=\langle S_4',S_5'\rangle$, and $\mathcal{S}_G=\langle g_1^z,g_1^x,g_2^z,g_2^x\rangle$.

B. EAOQECCs from classical BCH codes

EAOQECCs can also be constructed directly from classical binary codes. Before we give examples, however, we need one more theorem:

Theorem 3. Let H be any binary parity check matrix with dimension $(n-k)\times n$. We can obtain the corresponding $[[n,2k-n+c;c]]$ EAQECC, where $c=\text{rank}(HH^T)$ is the number of ebits needed.

Proof. By the CSS construction, let $\widetilde{H}$ be

$$\widetilde{H}=\left(\begin{array}{c|c} H & \mathbf{0} \\ \mathbf{0} & H \end{array}\right). \tag{8}$$

Let $\mathcal{S}$ be the group generated by $\widetilde{H}$, then $\mathcal{S}=\langle Z^{\mathbf{r}_1},\ldots,Z^{\mathbf{r}_{n-k}},X^{\mathbf{r}_1},\ldots,X^{\mathbf{r}_{n-k}}\rangle$, where $\mathbf{r}_i$ is the ith row vector of H. Now we need to determine how many symplectic pairs are in group $\mathcal{S}$. Since $\text{rank}(HH^T)=c$, there exists a matrix P such that

$$PHH^TP^T=\begin{pmatrix} I_{p\times p} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_{q\times q} & \mathbf{0} \\ \mathbf{0} & I_{q\times q} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix}_{(n-k)\times(n-k)},$$

where $p+2q=c$. Let $\mathbf{r}_i'$ be the ith row vector of the new matrix PH, then $\mathcal{S}=\langle Z^{\mathbf{r}_1'},\ldots,Z^{\mathbf{r}_{n-k}'},X^{\mathbf{r}_1'},\ldots,X^{\mathbf{r}_{n-k}'}\rangle$.

Using the fact that $\{Z^{\mathbf{a}},X^{\mathbf{b}}\}=0$ if and only if $\mathbf{a}\cdot\mathbf{b}=1$, we know that the operators $Z^{\mathbf{r}_i'},X^{\mathbf{r}_i'}$ for $1\le i\le p$, and the operators $Z^{\mathbf{r}_{p+j}'},X^{\mathbf{r}_{p+q+j}'}$ for $1\le j\le q$, generate a symplectic subgroup in $\mathcal{S}$ of size 2^{2c}. ■

Definition 1 [19]. A cyclic code of length n over $\text{GF}(p^m)$ is a BCH code of designed distance d if, for some number $b\geqslant 0$, the generator polynomial $g(x)$ is

$$g(x)=\text{lcm}\{M^b(x),M^{b+1}(x),\ldots,M^{b+d-2}(x)\},$$

where $M^k(x)$ is the minimal polynomial of α^k over $\text{GF}(p^m)$. I.e., $g(x)$ is the lowest degree monic polynomial over $\text{GF}(p^m)$ having $\alpha^b,\alpha^{b+1},\ldots,\alpha^{b+d-2}$ as zeros. When $b=1$, we call such BCH codes narrow-sense BCH codes. When $n=p^m-1$, we call such BCH codes primitive.

Consider the primitive narrow-sense BCH code over $\text{GF}(2^6)$. This code has the following parity check matrix:

$$H_q=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & \cdots & \alpha^{5(n-1)} \\ 1 & \alpha^7 & \alpha^{14} & \cdots & \alpha^{7(n-1)} \end{pmatrix}, \tag{9}$$

where $\alpha\in\text{GF}(2^6)$ satisfies $\alpha^6+\alpha+1=0$ and $n=63$. Since all finite fields of order p^m are *isomorphic*, there exists a one-to-one correspondence between elements in $\{\alpha^j:j=0,1,\ldots,p^m-2,\infty\}$ and elements in $\{a_0a_1\ldots,a_m:a_i\in\text{GF}(p)\}$. If we replace $\alpha^j\in\text{GF}(2^6)$ in Eq. (9) with its binary representation, this gives us a binary $[63,39,9]$ BCH code whose parity check matrix H_2 is of size 24×63. If we carefully inspect the binary parity check matrix H_2, we will find that the first 18 rows of H_2 give a $[63,45,7]$ dual-containing BCH code.

TABLE II. The resulting [[8,1,3;$c=1$,$r=2$]] EAOQECC encodes one qubit into eight physical qubits with the help of one ebit ($c=1$), and has two gauge qubits ($r=2$) for passive error correction.

	Alice								Bob
S_1'	Z	Z	I	Z	Z	I	I	I	I
S_2'	Z	I	Z	Z	I	Z	I	I	I
S_3'	I	I	I	I	I	I	Z	Z	I
S_4'	I	I	I	I	I	I	I	Z	Z
S_5'	X	X	X	I	I	I	X	X	X
S_6'	X	X	X	X	X	X	I	I	I
$\bar{Z}$	Z	I	I	Z	I	I	I	Z	I
$\bar{X}$	I	I	I	X	X	X	I	I	I
g_1^z	Z	Z	I	I	I	I	I	I	I
g_1^x	I	X	I	I	X	I	I	I	I
g_2^z	I	I	I	Z	I	Z	I	I	I
g_2^x	I	I	X	I	I	X	I	I	I

TABLE III. Parameters of the EAOQECCs constructed from a classical [63,39,9] BCH code, where r represents the number of gauge qubits and c represents the number of ebits needed.

n	k	d	r	c
63	21	9	0	6
63	21	7	1	5
63	21	7	2	4
63	21	7	3	3
63	21	7	4	2
63	21	7	5	1
63	21	7	6	0

TABLE IV. Stabilizer generators of the [[15,9,4;c=4]] EAQECC derived from the classical code given by Eq. (10). The code uses c=4 ebits, and the size of $\mathcal{S}_E$ is equal to 2^{2c}=256.

$\mathcal{S}_E$	I	I	Y	I	Z	X	Y	Z	Y	I	I	Z	Y	X	Z
	I	Y	I	I	Y	I	Z	X	Y	Z	I	I	Y	Z	Y
	I	Z	Y	I	I	X	Z	X	X	X	I	Z	X	I	I
	I	I	X	I	Y	Z	X	Y	X	I	I	Y	X	Z	Y
	I	I	I	I	I	I	I	I	I	I	Z	I	I	I	I
	I	I	I	I	I	I	I	I	I	I	Y	I	I	I	I
	I	Z	Z	Z	X	I	Y	I	Y	I	I	Z	Z	Z	I
	I	Y	Y	Y	Z	I	X	I	X	I	I	Y	Y	Y	I
$\mathcal{S}_I$	Z	Z	Y	I	Z	Y	X	X	Y	Z	I	Y	Z	Z	I
	Y	Y	X	I	Y	X	Z	Z	X	Y	I	X	Y	Y	I

From Theorem 3, it is easy to check that $c=\text{rank}(H_2H_2^T)=6$. Thus by the CSS construction [17], this binary $[63,39,9]$ BCH code will give us a corresponding $[[63,21,9;6]]$ EAQECC.

If we further explore the group structure of this EAQECC, we will find that the six symplectic pairs that generate the entanglement subgroup $\mathcal{S}_E$ come from the last six rows of H_2. (Remember that we are using the CSS construction.) If we remove one symplectic pair at a time from $\mathcal{S}_E$ and adding it to the gauge subgroup $\mathcal{S}_G$, we get EAOQECCs with parameters given in Table III.

In general, there could be considerable freedom in which one of the symplectic pairs is to be removed. There are plenty of choices in the generators of $\mathcal{S}_E$. In fact, it does not matter which symplectic pair we remove first in this example, due to the algebraic structure of this BCH code. The distance is always lower bounded by 7.

One final remark: this example gives EAOQECCs with positive net rate, so they could be used as catalytic codes.

C. EAOQECCs from classical quaternary codes

In the following, we will show how to use MAGMA [20] to construct EAOQECCs from classical quaternary codes with positive net yield and without too much distance degradation. Consider the following parity check matrix H_4 of a $[15,10,4]$ quaternary code:

$$H_4=\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & \omega^2 & 0 & 1 & \omega^2 & 0 & \omega & \omega^2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & \omega & \omega^2 & 1 & \omega & 0 & 0 & 1 & \omega & 1 \\ 0 & 0 & 1 & 0 & \omega & \omega^2 & 1 & \omega & 1 & 0 & 0 & \omega & 1 & \omega^2 & \omega \\ 0 & 0 & 0 & 1 & 1 & \omega^2 & 0 & 1 & \omega^2 & \omega & 0 & \omega^2 & 1 & 0 & \omega^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad (10)$$

TABLE V. Stabilizer generators of the [[15,9,3;c=3,r=1]] EAOQECC derived from the EAQECC given by Table V. The number of ebits has been reduced to c=3, and r=1 gauge qubit has been added. The sizes of $\mathcal{S}_E$ and $\mathcal{S}_G$ are 2^{2c}=64 and 2^{2r}=4, respectively.

$\mathcal{S}_E$	I	I	Y	I	Z	X	Y	Z	Y	I	I	Z	Y	X	Z
	I	Y	I	I	Y	I	Z	X	Y	Z	I	I	Y	Z	Y
	I	Z	Y	I	I	X	Z	X	X	X	I	Z	X	I	I
	I	I	X	I	Y	Z	X	Y	X	I	I	Y	X	Z	Y
	I	I	I	I	I	I	I	I	I	I	Z	I	I	I	I
	I	I	I	I	I	I	I	I	I	I	Y	I	I	I	I
$\mathcal{S}_G$	I	Z	Z	Z	X	I	Y	I	Y	I	I	Z	Z	Z	I
	I	Y	Y	Y	Z	I	X	I	X	I	I	Y	Y	Y	I
$\mathcal{S}_I$	X	X	Z	I	X	Z	Y	Y	Z	X	I	Z	X	X	I
	Z	Z	Y	I	Z	Y	X	X	Y	Z	I	Y	Z	Z	I

where $\{0,1,\omega,\omega^2\}$ are elements of GF(4) that satisfy $1+\omega+\omega^2=0$ and $\omega^3=1$. This quaternary code has the largest minimum weight among all known $[n=15,k=10]$ linear quaternary codes. By the construction given in Ref. [17], this code gives a corresponding $[[15,9,4;c=4]]$ EAQECC with the stabilizers given in Table IV.

The entanglement subgroup $\mathcal{S}_E$ of this EAQECC has $c=4$ symplectic pairs. Our goal is to construct an EAOQECC from this EAQECC such that the power of error correction is largely retained, but the amount of entanglement needed is reduced. In this example, the choice of which symplectic pair is removed strongly affects the distance d of the resulting EAOQECC. By using MAGMA to perform a random search of all the possible sympletic pairs in $\mathcal{S}_E$, and then putting them into the gauge subgroup $\mathcal{S}_G$, we can obtain a $[[15,9,3;c=3,r=1]]$ EAOQECC with stabilizers given in Table V. The distance is reduced by one, which still retains the ability to correct all one-qubit errors; the amount of entanglement needed is reduced by one ebit; and we gain some extra power of passive error correction, due to the subsystem structure inside the code space, given by the gauge subgroup $\mathcal{S}_G$.

V. CONCLUSION

We have shown a very general quantum error-correction scheme that combines two extensions of standard stabilizer codes. This scheme includes the advantages of both entanglement-assisted and operator quantum error correction.

In addition to presenting the formal theory of EAOQECCs, we have given several examples of code construction. The methods of constructing OQECCs from standard QECCs can be applied directly to the construction of EAOQECCs from EAQECCs. We can also construct EAOQECCs directly from classical linear codes.

We also show that, by exploring the structure of the symplectic subgroup, we can construct versatile classes EAOQECCs with varying powers of passive versus active error correction. Starting with good classical codes, this entanglement-assisted operator formalism can be used to construct quantum codes tailored to the needs of particular applications. The study of such classes of good quantum codes is the subject of ongoing research.

ACKNOWLEDGMENTS

We wish to acknowledge enlightening discussions with David Poulin and Graeme Smith. T.B. received financial support from NSF Grant No. CCF-0448658, and T.B. and M.H.H. both received support from NSF Grant No. ECS-0507270. I.D. and M.H.H. received financial support from NSF Grants No. CCF-0524811 and No. CCF-0545845.

[1] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[2] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[4] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997 (unpublished).
[5] S. Aly, A. Klappenecker, and P. K. Sarvepalli, e-print arXiv:quant-ph/0610153.
[6] D. Bacon, Phys. Rev. A **73**, 012340 (2006).
[7] D. Bacon and A. Casaccino, e-print arXiv:quant-ph/0610088.
[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] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[14] P. Zanardi, Phys. Rev. A **60**, R729 (1999).
[15] G. Bowen, Phys. Rev. A **66**, 052313 (2002).
[16] T. Brun, I. Devetak, and M. H. Hsieh, e-print arXiv:quant-ph/0608027.
[17] T. Brun, I. Devetak, and M. H. Hsieh, Science **314**, 436 (2006).
[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2000).
[19] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes* (Elsevier, Amsterdam, 1977).
[20] W. Bosma, J. Cannon, and C. Playoust, J. Symb. Comput. **24**, 235 (1997).