Open access • Journal Article • DOI:10.1109/TIT.2014.2313559

Catalytic Quantum Error Correction — Source link

Todd A. Brun, Igor Devetak, Min-Hsiu Hsieh

Institutions: University of Southern California

Published on: 25 Mar 2014 - IEEE Transactions on Information Theory (IEEE)

Topics: Quantum convolutional code, Linear code, Block code, Quantum error correction and Error detection and correction

Catalytic quantum error correction

Todd Brun, Igor Devetak, and Min-Hsiu Hsieh

***Abstract*—We develop the theory of *entanglement-assisted quantum error correcting* (EAQEC) *codes*, a generalization of the stabilizer formalism to the setting in which the sender and receiver have access to pre-shared entanglement. Conventional stabilizer codes are equivalent to self-orthogonal symplectic codes. In contrast, EAQEC codes do not require self-orthogonality, which greatly simplifies their construction. We show how any classical binary or quaternary block code can be made into an EAQEC code. We provide a table of best known EAQEC codes with code length up to 10. With the self-orthogonality constraint removed, we see that the distance of an EAQEC code can be better than any standard QEC code with the same fixed net yield. In a quantum computation setting, EAQEC codes give rise to *catalytic* quantum codes, which assume a subset of the qubits are noiseless. We also give an alternative construction of EAQEC codes by making classical entanglement-assisted codes coherent.**

***Index Terms*—quantum error-correcting code, entanglement, quantum information theory, and father protocol.**

I. Introduction

Information theory and the theory of error-correcting codes (coding theory) are intimately connected. Both address the problem of sending information over noisy channels. The sender Alice encodes her message as a codeword, sends it through the channel, and the receiver Bob tries to infer the intended message based on the channel output.

Information theory (or rather the subfield of Shannon theory) deals with the *asymptotic* setting of increasingly long codes, with asymptotically vanishing error probability. The noisy channel is typically assumed to act independently on the codeword bits. The fundamental quantity of interest is the *capacity* of the channel: the optimal rate (in bits per channel use) of information transfer. Claude Shannon [1] gave a remarkable characterization of the channel capacity in terms of mutual information. Unfortunately, the capacity is achieved by random coding, which means highly inefficient encoding and decoding algorithms.

Coding theory deals with the practical *finite* setting, characterized by a fixed code length, number of encoded bits and correctable error set. The most popular codes have simple mathematical properties, such as linearity (a linear combination of codewords is another codeword), which allows for efficient encoding. The performance of these codes is then measured against the optimal performance set by Shannon theory.

The authors were all originally with the Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089. Min-Hsiu Hsieh is now with the Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, P.O. Box 123, Broadway NSW 2007, Australia (email: Min-Hsiu.Hsieh@uts.edu.au).

This paper was presented in part in New Trends in Mathematical Physics, Selected contributions of the XVth International Congress on Mathematical Physics, 161-172, 2009, and at the 2006 Asian Conference on Quantum Information Science, Beijing, China.

This relationship carries over to quantum information processing. The basic communication task is sending quantum information over noisy quantum channels. This setting is also relevant for fault-tolerant quantum computation, because decoherence can be regarded as a quantum channel connecting two points in time (rather than space). The first quantum error-correcting (QEC) code was discovered by Shor [2], leading to an explosion of research in subsequent years [3], [4], [5], [6], [7], [8], [9], [10]. Calderbank and Shor [10] and Steane [7] gave the first systematic way to construct quantum "CSS" codes from self-orthogonal classical codes over $\mathbb{Z}_2$. These efforts culminated in a general theory of linear quantum codes, also known as *stabilizer codes* [8], [11], [12], [13]. Stabilizer codes are equivalent to classical codes which are self-orthogonal with respect to the symplectic bilinear form. These in turn may be constructed from self-orthogonal classical codes over $\mathbb{F}_4$, generalizing the CSS construction [9], [8].

In [2] Shor also raised the information theoretical question of characterizing the capacity of a quantum channel for sending quantum information, subsequently answered by [14], [15], [16] in terms of *coherent information*. It comes as no surprise that coding theory and information theory continue to inform each other in the quantum setting. The capacity-achieving quantum codes of [16] have a structure akin to CSS codes (thanks to their common connection to cryptography). Concatenated stabilizer codes achieve rates equal to the coherent information evaluated on density operators corresponding to maximally mixed qubit states encoded by a stabilizer code [4], [17].

Research has since taken us beyond this most obvious quantum communication setting. Apart from quantum communication channels, there are other resources to consider, such as entanglement and classical communication. Great progress has been made in characterizing optimal tradeoffs between these resources. For example, the capacity of a quantum channel for sending classical information assisted by entanglement (EA capacity) is a simple single letter expression involving quantum mutual information [18]. In [19] (see also [20], [21]) a remarkable duality was discovered between entanglement-assisted quantum communication (the "father" protocol) and quantum-communication-assisted entanglement distillation (the "mother" protocol). The two were shown to generate a whole family of protocols when combined with the more elementary protocols of superdense coding [22], quantum teleportation [23] and entanglement distribution [19].

The father side of the family is shown in Figure 1. Quantum capacity-achieving protocols can be obtained from the father protocol by combining it with entanglement distribution. In conjunction with superdense coding, the father protocol gives rise to EA capacity-achieving protocols. Moreover, the latter

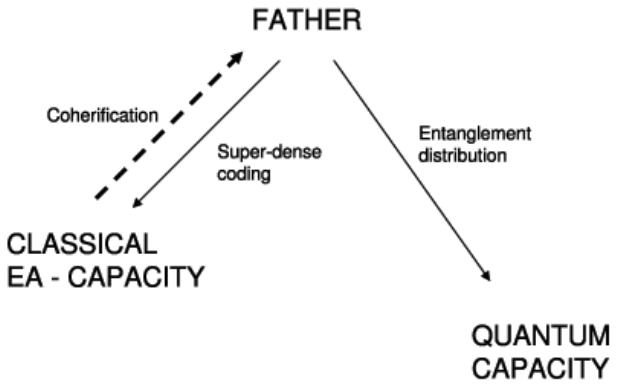

Fig. 1. The male side of the family tree of quantum Shannon theory [19].

can be made coherent [16], [19], [24], [25], [26] to recover the father protocol.

Can we reproduce the family in the finite setting of coding theory? Is it beneficial to do so? In this paper we give an affirmative answer to these two questions. We develop a general theory of linear "father" codes or entanglement-assisted quantum error-correcting (EAQEC) codes. EAQEC codes turn out to be a rather natural generalization of the usual stabilizer codes, equivalent to classical symplectic codes. These codes need not be self-orthogonal: the degree to which they are not self-orthogonal measures the required amount of entanglement assistance. Consequently, *any* linear classical code can be made into an EAQEC code. This provides a drastic simplification, allowing the classical theory of error correction to be imported wholesale [27], [49], [28], [29], [30], [31], [32], [33], [34], [35].

The idea of using entanglement to assist construction of QEC codes was proposed in [4], [36]. The authors in [4] showed how to link a one-way entanglement purification protocol (1-EPP)—specifically, the one-way hashing protocol—to the problem of preserving quantum states though quantum channels, the same goal as standard QEC codes. Analogously, in [37] the 1-EPP assisted by pure entanglement, or *breeding protocol*, can also be linked to EAQEC codes. The authors of [4] described a technique to turn the entanglement purification problem (and therefore, also the QEC problem) into an entirely classical exercise; however, this paper did not provide any such constructive method relating classical coding theory to actual QEC codes, due to the mathematical difficulty of keeping everything in the EPP language. It was only with the development of the stabilizer formalism that the connection between classical linear codes and standard QEC codes became clear. Because of this connection, in fact, entanglement purification protocols are now generally derived from QEC codes, rather than the other way around, since QEC codes can be constructed using ideas from the well-developed classical theory of error-correcting codes.

The first attempt to construct EAQEC codes in the stabilizer formalism was by Bowen [38]. He constructed an EAQEC code from the $[[5, 1, 3]]$ QEC code using two pure maximally entangled pairs. Still the connection of EAQEC codes to the stabilizer formalism (equivalently the classical symplectic codes) is very vague, and this stimulates the work presented in this paper. We continue the study of [10], [7], [11], [9], [8] where those papers can not link arbitrary classical linear codes to QEC codes.

The paper is organized as follows. Section II provides background on the Pauli group and symplectic algebra. It also reviews basic quantum strategies for sending classical information. Section III defines EAQEC codes and determines the set of errors they can correct. Section IV generalizes the code construction method of [9], [8] based on classical codes over $\mathbb{F}_4$. Section V regards the right branch of Figure 1: constructing *catalytic* QEC codes from EAQEC codes. Section VI regards the left branch of Figure 1: constructing entanglement-assisted codes for sending classical information (EACEC codes). These are then made coherent [25], providing an alternative construction of EAQEC codes. Section VII discusses bounds on the performance of EAQEC codes. Section VIII recovers Bowen's result in our framework. Section IX updates the table of known codes from [8]. We discuss our results in Section X.

II. Background

In this section we review the properties of Pauli matrices, and relate them to symplectic binary and quaternary vector spaces. Our presentation follows Forney et al. [39] and Hamada [17].

A. Single qubit Pauli group

A *qubit* is a quantum system corresponding to a two dimensional complex Hilbert space $\mathcal{H}$. Fixing a basis for $\mathcal{H}$, the set Π of *Pauli matrices* is defined as

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

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

The Pauli matrices are Hermitian unitary matrices with eigenvalues belonging to the set $\{1, -1\}$. The multiplication table of these matrices is given by:

$\times$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	iZ	$-iY$
Y	Y	$-iZ$	I	iX
Z	Z	iY	$-iX$	I

Observe that the Pauli matrices either commute or anticommute. Let $[A] = \{\beta A \mid \beta \in \mathbb{C}, |\beta| = 1\}$ be the equivalence class of matrices equal to A up to a phase factor.[1] Then the set $[\Pi] = \{[I], [X], [Y], [Z]\}$ is readily seen to form a commutative group under the multiplication operation defined by $[A][B] = [AB]$. It is called the Pauli group.

[1]It makes good physical sense to neglect this overall phase, which has no observable consequence.

We are interested in relating the Pauli group to the additive group $(\mathbb{Z}_2)^2 = \{00, 01, 10, 11\}$ of binary words of length 2 described by the table:

$+$	00	01	11	10
00	00	01	11	10
01	01	00	10	11
11	11	10	00	01
10	10	11	01	00

This group is also a two-dimensional vector space over the field $\mathbb{Z}_2$. A bilinear form can be defined over this vector space, called the *symplectic form* or *symplectic product*[2] $\odot : (\mathbb{Z}_2)^2 \times (\mathbb{Z}_2)^2 \to \mathbb{Z}_2$, given by the table

$\odot$	00	01	11	10
00	0	0	0	0
01	0	0	1	1
11	0	1	0	1
10	0	1	1	0

In what follows we will often write elements of $(\mathbb{Z}_2)^2$ as $u = (z|x)$, with $z, x \in \mathbb{Z}_2$. For instance, 01 becomes $(0|1)$. For $u = (z|x), v = (z'|x') \in (\mathbb{Z}_2)^2$ the symplectic product is equivalently defined by

$$u \odot v = zx' + z'x.$$

Define the map $N : (\mathbb{Z}_2)^2 \to \Pi$ by the following table:

$(\mathbb{Z}_2)^2$	Π
00	I
01	X
11	Y
10	Z

This map is defined in such a way that $N_{(z|x)}$ and $Z^z X^x$ are equal up to a phase factor, i.e.

$$[N_{(z|x)}] = [Z^z X^x].$$

We make two key observations

1) The map $[N] : (\mathbb{Z}_2)^2 \to [\Pi]$ induced by N is an isomorphism:

$$[N_u][N_v] = [N_{u+v}].$$

2) The commutation relations of the Pauli matrices are captured by the symplectic product

$$N_u N_v = (-1)^{u \odot v} N_v N_u.$$

Both properties are readily verified from the tables.

B. Multi-qubit Pauli group

Consider an n-qubit system corresponding to the tensor product Hilbert space $\mathcal{H}^{\otimes n}$. Define an n-qubit Pauli matrix $\mathbf{A}$ to be of the form $\mathbf{A} = A_1 \otimes A_2 \otimes \cdots \otimes A_n$, where $A_j \in \Pi$. The set of all 4^n n-qubit Pauli matrices is denoted by Π^n. The product of elements of Π^n is an element of Π^n up to a phase factor. Define as before the equivalence class $[\mathbf{A}] = \{\beta \mathbf{A} \mid \beta \in \mathbb{C}, |\beta| = 1\}$. Then

$$[\mathbf{A}][\mathbf{B}] = [A_1 B_1] \otimes [A_2 B_2] \otimes \cdots \otimes [A_n B_n] = [\mathbf{AB}].$$

Thus the set $[\Pi^n] = \{[\mathbf{A}] : \mathbf{A} \in \Pi^n\}$ is a commutative multiplicative group.

Now consider the group/vector space $(\mathbb{Z}_2)^{2n}$ of binary vectors of length $2n$. Its elements may be written as $\mathbf{u} = (\mathbf{z}|\mathbf{x})$, $\mathbf{z} = z_1 \dots z_n \in (\mathbb{Z}_2)^n$, $\mathbf{x} = x_1 \dots x_n \in (\mathbb{Z}_2)^n$. We shall think of $\mathbf{u}$, $\mathbf{z}$ and $\mathbf{x}$ as row vectors. The symplectic product of $\mathbf{u} = (\mathbf{z}|\mathbf{x})$ and $\mathbf{v} = (\mathbf{z}'|\mathbf{x}')$ is given by

$$\mathbf{u} \odot \mathbf{v}^T = \mathbf{z}\,\mathbf{x}'^T + \mathbf{z}'\,\mathbf{x}^T.$$

The right hand side are binary inner products and T denotes the transpose. This should be thought of as a kind of matrix multiplication of a row vector and a column vector. We use $\mathbf{u} \odot \mathbf{v}^T$ rather than the more standard $\mathbf{u}\,\mathbf{v}^T$ to emphasize that the symplectic form is used rather than the binary inner product. Equivalently,

$$\mathbf{u} \odot \mathbf{v}^T = \sum_i u_i \odot v_i$$

where $u_i = (z_i|x_i), v_i = (z_i'|x_i')$ and this sum represents Boolean addition. Observe that if $\mathbf{u} \odot \mathbf{u}^T = 0$, these two vectors are "orthogonal" to each other with respect to the symplectic inner product.

The map $N : (\mathbb{Z}_2)^{2n} \to \Pi^n$ is now defined as

$$N_{\mathbf{u}} = N_{u_1} \otimes \cdots \otimes N_{u_n}.$$

Writing

$$X^{\mathbf{x}} = X^{x_1} \otimes \cdots \otimes X^{x_n},$$

$$Z^{\mathbf{z}} = Z^{z_1} \otimes \cdots \otimes Z^{z_n},$$

as in the single qubit case, we have

$$[N_{(\mathbf{z}|\mathbf{x})}] = [Z^{\mathbf{z}} X^{\mathbf{x}}].$$

The two observations made for the single qubit case also hold:

1) The map $[N] : (\mathbb{Z}_2)^{2n} \to [\Pi^n]$ induced by N is an isomorphism:

$$[N_{\mathbf{u}}][N_{\mathbf{v}}] = [N_{\mathbf{u}+\mathbf{v}}]. \tag{1}$$

Consequently, if $\{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ is a linearly independent set then the elements of the Pauli group subset $\{[N_{\mathbf{u}_1}], \dots, [N_{\mathbf{u}_m}]\}$ are independent in the sense that no element can be written as a product of others.

2) The commutation relations of the n-qubit Pauli matrices are captured by the symplectic product

$$N_{\mathbf{u}} N_{\mathbf{v}} = (-1)^{\mathbf{u} \odot \mathbf{v}^T} N_{\mathbf{v}} N_{\mathbf{u}}. \tag{2}$$

C. Properties of the symplectic form

In this subsection we present two well-known results which will play a major role in the construction of EAQEC codes. Together they will enable us to conclude that any independent subset of the n-qubit Pauli group can be transformed via a unitary operation into a canonical set whose elements act non-trivially only on single qubits. Independent proofs of Theorem 1 and 2 are provided in Appendix A and B, respectively, for

[2]Strictly speaking it is not an inner product.

completeness. The reader is advised that the proofs can be skipped on a first reading without impairing understanding of the rest of the paper.

A subspace V of $(\mathbb{Z}_2)^{2n}$ is called *symplectic* [40] if there is no $\mathbf{v} \in V \backslash \{\mathbf{0}\}$ such that

$$\mathbf{v} \odot \mathbf{u}^T = 0, \ \ \forall \mathbf{u} \in V. \tag{3}$$

$(\mathbb{Z}_2)^{2n}$ is itself a symplectic subspace. Consider the standard basis for $(\mathbb{Z}_2)^{2n}$, consisting of $\mathbf{g}_i = (\mathbf{e}_i|\mathbf{0})$ and $\mathbf{h}_i = (\mathbf{0}|\mathbf{e}_i)$ for $i = 1, \ldots, n$, where $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ [1 in the ith position] are the standard basis vectors of $(\mathbb{Z}_2)^n$. Observe that

$$\mathbf{g}_i \odot \mathbf{g}_j^T = 0, \quad \text{for all } i, j \tag{4}$$
$$\mathbf{h}_i \odot \mathbf{h}_j^T = 0, \quad \text{for all } i, j \tag{5}$$
$$\mathbf{g}_i \odot \mathbf{h}_j^T = 0, \quad \text{for all } i \neq j \tag{6}$$
$$\mathbf{g}_i \odot \mathbf{h}_i^T = 1, \quad \text{for all } i. \tag{7}$$

Thus, the basis vectors come in n *hyperbolic pairs* $(\mathbf{g}_i, \mathbf{h}_i)$ such that only the symplectic product between hyperbolic partners is nonzero. The matrix $J = [\mathbf{g}_i \odot \mathbf{h}_j^T]$ defining the symplectic product with respect to this basis is given by

$$J = \begin{pmatrix} 0_{n\times n} & I_{n\times n} \\ I_{n\times n} & 0_{n\times n} \end{pmatrix}, \tag{8}$$

where $I_{n\times n}$ and $0_{n\times n}$ are the $n \times n$ identity and zero matrices, respectively. A basis for $(\mathbb{Z}_2)^{2n}$ whose symplectic product matrix J is given by (8) is called a *symplectic basis*. In the Pauli picture, the hyperbolic pairs $(\mathbf{g}_i, \mathbf{h}_i)$ correspond to $(Z^{\mathbf{e}_i}, X^{\mathbf{e}_i})$ – the anticommuting Z and X Pauli matrices acting on the ith qubit.

In contrast, a subspace V of $(\mathbb{Z}_2)^{2n}$ is called *isotropic* if (3) holds for *all* $\mathbf{v} \in V$. The largest isotropic subspace of $(\mathbb{Z}_2)^{2n}$ is n-dimensional. The span of the $\mathbf{g}_i$, $i = 1, \ldots, n$, is an example of a subspace saturating this bound.

A general subspace of $(\mathbb{Z}_2)^{2n}$ is neither symplectic nor isotropic. The following theorem, stated in [40] and rediscovered in Pauli language in [41], says that an arbitrary subspace V can be decomposed as a direct sum of a symplectic part and an isotropic part.

Theorem 1: Let V be an m-dimensional subspace of $(\mathbb{Z}_2)^{2n}$. Then there exists a symplectic basis of $(\mathbb{Z}_2)^{2n}$ consisting of hyperbolic pairs $(\mathbf{u}_i, \mathbf{v}_i)$, $i = 1, \ldots, n$, such that $\{\mathbf{u}_1, \ldots, \mathbf{u}_{c+\ell}, \mathbf{v}_1, \ldots, \mathbf{v}_c\}$ is a basis for V, for some $c, \ell \geq 0$ with $2c + \ell = m$.

Equivalently,

$$V = \mathrm{symp}(V) \oplus \mathrm{iso}(V)$$

where $\mathrm{symp}(V) = \mathrm{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_c, \mathbf{v}_1, \ldots, \mathbf{v}_c\}$ is symplectic and $\mathrm{iso}(V) = \mathrm{span}\{\mathbf{u}_{c+1}, \ldots, \mathbf{u}_{c+\ell}\}$ is isotropic.

Proof: The proof is given in Appendix A where we describe an algorithm which, by induction, yields the basis from the statement of the theorem. The idea of the algorithm comes from Gram-Schmidt orthogonalization procedure for linear space. ∎

Remark It is readily seen that the space $\mathrm{iso}(V)$ is unique, given V. In contrast, $\mathrm{symp}(V)$ is not. For instance, replacing $\mathbf{v}_1$ by $\mathbf{v}_1' = \mathbf{v}_1 + \mathbf{u}_{c+1}$ in the above definition of $\mathrm{symp}(V)$ does not change its symplectic property.

A *symplectomorphism* $\Upsilon : (\mathbb{Z}_2)^{2n} \to (\mathbb{Z}_2)^{2n}$ is a linear isomorphism which preserves the symplectic form, namely

$$\Upsilon(\mathbf{u}) \odot \Upsilon(\mathbf{v})^T = \mathbf{u} \odot \mathbf{v}^T. \tag{9}$$

The following theorem relates symplectomorphisms on $(\mathbb{Z}_2)^{2n}$ to unitary maps on $\mathcal{H}^{\otimes n}$. It appears, for instance, in [42].

Theorem 2: For any symplectomorphism Υ on $(\mathbb{Z}_2)^{2n}$ there exists a unitary map U_Υ on $\mathcal{H}^{\otimes n}$ such that for all $\mathbf{u} \in (\mathbb{Z}_2)^{2n}$,

$$[N_{\Upsilon(\mathbf{u})}] = [U_\Upsilon N_{\mathbf{u}} U_\Upsilon^{-1}].$$

Proof: An independent proof is given in Appendix B for completeness. ∎

Remark. The unitary map U_Υ may be viewed as a map on $[\Pi]$ given by $[\mathbf{A}] \mapsto [U_\Upsilon \mathbf{A} U_\Upsilon^{-1}]$. The theorem says that the following diagram commutes

$$\begin{array}{ccc} (\mathbb{Z}_2)^{2n} & \xrightarrow{\Upsilon} & (\mathbb{Z}_2)^{2n} \\ {\scriptstyle [N]}\downarrow & & \downarrow{\scriptstyle [N]} \\ [\Pi] & \xrightarrow{U_\Upsilon} & [\Pi] \end{array}$$

D. Encoding classical information into quantum states

In this subsection we review two schemes for sending classical information over quantum channels: elementary coding and superdense coding. These will be used later in the context of quantum error correction to convey information to the decoder about which error happened.

In the first scheme, Alice and Bob are connected by a perfect qubit channel. Alice can send an arbitrary bit $a \in \mathbb{Z}_2$ over the qubit channel in the following way:

- Alice locally prepares a state $|0\rangle$ in $\mathcal{H}$. This state is the $+1$ eigenstate of the Z operator. Based on her message a, she performs the encoding operation X^a, producing the state $|a\rangle = X^a|0\rangle$.
- Alice sends the encoded state to Bob through the qubit channel.
- Bob decodes by performing the von Neumann measurement in the $\{|0\rangle, |1\rangle\}$ basis. As this is the unique eigenbasis of the Z operator, this is equivalently called "measuring the Z observable".

We call this protocol "elementary coding" and write it symbolically as a *resource inequality* [19], [25], [43], [21], [20][3]

$$[q \to q] \geq [c \to c].$$

Here $[q \to q]$ represents a perfect qubit channel and $[c \to c]$ represents a perfect classical bit channel. The inequality $\geq$ signifies that the resource on the left hand side can be used in a protocol to simulate the resource on the right hand side.

Elementary coding immediately extends to m qubits. Alice prepares the simultaneous $+1$ eigenstate of the $Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m}$ operators $|\mathbf{0}\rangle$, and encodes the message $\mathbf{a} \in (\mathbb{Z}_2)^m$ by applying $X^{\mathbf{a}}$, producing the encoded state $|\mathbf{a}\rangle = X^{\mathbf{a}}|\mathbf{0}\rangle$.

[3] In [25] resource inequalities were used in the asymptotic sense. Here they refer to finite protocols, and are thus slightly abusing their original intent.

Bob decodes by simultaneously measuring the $Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m}$ observables. We could symbolically represent this protocol by

$$m\,[q \to q] \geq m\,[c \to c].$$

In the second scheme, Alice and Bob share the ebit state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \tag{10}$$

in addition to being connected by the qubit channel. In (10) Alice's state is to the left and Bob's is to the right of the $\otimes$ symbol.

The state $|\Phi\rangle$ is the simultaneous $(+1, +1)$ eigenstate of the commuting operators $Z \otimes Z$ and $X \otimes X$. Again, the operator to the left of the $\otimes$ symbol acts on Alice's system and the operator to the right of the $\otimes$ symbol acts on Bob's system. Alice can send a two-bit message $(a_1, a_2) \in (\mathbb{Z}_2)^2$ to Bob using "superdense coding" [22]:

- Based on her message (a_1, a_2), Alice performs the encoding operation $Z^{a_1}X^{a_2}$ on her part of the state $|\Phi\rangle$, producing the state $|a_1, a_2\rangle = (Z^{a_1}X^{a_2} \otimes I)|\Phi\rangle$.
- Alice sends her part of the encoded state to Bob through the perfect qubit channel.
- Bob decodes by performing the von Neumann measurement in the $\{(Z^{a_1}X^{a_2} \otimes I)|\Phi\rangle : (a_1, a_2) \in (\mathbb{Z}_2)^2\}$ basis, i.e., by simultaneously measuring the $Z \otimes Z$ and $X \otimes X$ observables.

The protocol is represented by the resource inequality

$$[q \to q] + [q\,q] \geq 2\,[c \to c], \tag{11}$$

where $[q\,q]$ now represents the shared ebit. It can also be extended to m copies. Alice and Bob share the state $|\Phi\rangle^{\otimes m}$ which is the simultaneous $+1$ eigenstate of the $Z^{\mathbf{e}_1} \otimes Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m} \otimes Z^{\mathbf{e}_m}$ and $X^{\mathbf{e}_1} \otimes X^{\mathbf{e}_1}, \ldots, X^{\mathbf{e}_m} \otimes X^{\mathbf{e}_m}$ operators. Alice encodes the message $(\mathbf{a}_1, \mathbf{a}_2) \in (\mathbb{Z}_2)^{2m}$ by applying $Z^{\mathbf{a}_1}X^{\mathbf{a}_2}$, producing the encoded state $|\mathbf{a}_1, \mathbf{a}_2\rangle = (Z^{\mathbf{a}_1}X^{\mathbf{a}_2} \otimes I)|\Phi\rangle^{\otimes m}$. Bob decodes by simultaneously measuring the $Z^{\mathbf{e}_1} \otimes Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m} \otimes Z^{\mathbf{e}_m}$ and $X^{\mathbf{e}_1} \otimes X^{\mathbf{e}_1}, \ldots, X^{\mathbf{e}_m} \otimes X^{\mathbf{e}_m}$ observables. The corresponding resource inequality is

$$m\,[q \to q] + m\,[q\,q] \geq 2m\,[c \to c].$$

Superdense coding provides the simplest illustration of how entanglement can increase the power of information processing.

III. Entanglement-assisted quantum error correction

In this section we formally introduce entanglement-assisted quantum error-correcting codes and prove our main result, Theorem 6, which gives sufficient error-correcting conditions.

A. The model

Denote by $\mathcal{L}$ the space of linear operators defined on the qubit Hilbert space $\mathcal{H}$. We will often encounter isometric operators $U : \mathcal{H}^{\otimes n_1} \to \mathcal{H}^{\otimes n_2}$. The corresponding *superoperator*, or completely positive, trace preserving (CPTP) map, is marked by a hat $\hat{U} : \mathcal{L}^{\otimes n_1} \to \mathcal{L}^{\otimes n_2}$ and defined by

$$\hat{U}(\rho) = U\rho U^\dagger.$$

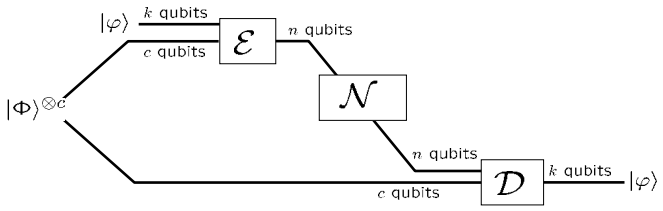

Fig. 2. A generic entanglement-assisted quantum code.

Observe that $\hat{U}$ is independent of any phase factors multiplying U. Thus, for a Pauli operator $N_{\mathbf{u}}$, $\hat{N}_{\mathbf{u}}$ only depends on the equivalence class $[N_{\mathbf{u}}]$.

Our communication scenario involves two spatially separated parties, Alice and Bob, as depicted in Figure 2. The resources at their disposal are

- a noisy channel defined by a CPTP map $\mathcal{N} : \mathcal{L}^{\otimes n} \to \mathcal{L}^{\otimes n}$ taking density operators on Alice's system to density operators on Bob's system;
- the c ebit state $|\Phi\rangle^{\otimes c}$ shared between Alice and Bob.

Alice wishes to send k qubits *perfectly* to Bob using the above resources. An $[[n, k; c]]$ EAQEC code consists of

- An encoding isometry $\mathcal{E} = \hat{U}_{\text{enc}} : \mathcal{L}^{\otimes k} \otimes \mathcal{L}^{\otimes c} \to \mathcal{L}^{\otimes n}$
- A decoding CPTP map $\mathcal{D} : \mathcal{L}^{\otimes n} \otimes \mathcal{L}^{\otimes c} \to \mathcal{L}^{\otimes k}$

such that

$$\mathcal{D} \circ \mathcal{N} \circ \hat{U}_{\text{enc}} \circ \hat{U}_{\text{app}} = \text{id}^{\otimes k},$$

where U_{app} is the isometry which appends the state $|\Phi\rangle^{\otimes c}$,

$$U_{\text{app}}|\varphi\rangle = |\varphi\rangle|\Phi\rangle^{\otimes c},$$

and $\text{id} : \mathcal{L} \to \mathcal{L}$ is the identity map on a single qubit. The protocol thus uses up c ebits of entanglement and generates k perfect qubit channels. We represent it by the resource inequality (with a slight abuse of notation [25], [20])

$$\langle \mathcal{N} \rangle + c\,[q\,q] \geq k\,[q \to q].$$

Even though a qubit channel is a strictly stronger resource than its static analogue, an ebit of entanglement, the parameter $k-c$ is still a good (albeit pessimistic) measure of the net noiseless quantum resources gained. It should be borne in mind that a negative value of $k - c$ still refers to a non-trivial protocol.

To make contact with classical error correction it is necessary to discretize the errors. It is well known that for standard quantum error correction (i.e., that unassisted by entanglement) it suffices to consider errors from the Pauli group (see e.g. [13].) We will show this for entanglement-assisted quantum error correction. This is done in two steps. First, the CPTP map $\mathcal{N}$ may be (non-uniquely) written in terms of its Kraus representation

$$\mathcal{N}(\rho) = \sum_i A_i \rho A_i^\dagger.$$

Second, each A_i may be expanded in the Pauli operators

$$A_i = \sum_{\mathbf{u} \in (\mathbb{Z}_2)^{2n}} \alpha_{i,\mathbf{u}} N_{\mathbf{u}}.$$

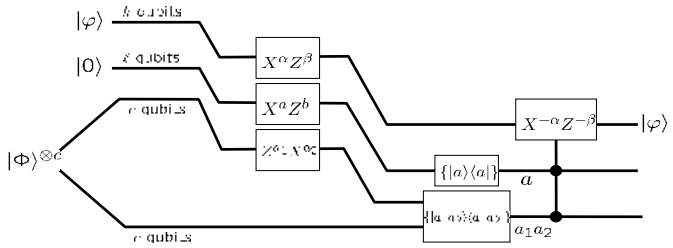

Fig. 3. The canonical code.

Define the support of $\mathcal{N}$ by $\mathrm{supp}(\mathcal{N}) = \{\mathbf{u} \in (\mathbb{Z}_2)^{2n} : \exists i, \alpha_{i,\mathbf{u}} \neq 0\}$. The following theorem allows us, absorbing U_{app} into U_{enc}, to replace the continuous map $\mathcal{N}$ by the error set $S = \mathrm{supp}(\mathcal{N})$.

Theorem 3: If $\mathcal{D} \circ \hat{N}_{\mathbf{u}} \circ \hat{U}_{\mathrm{enc}} = \mathrm{id}^{\otimes k}$ for all $\mathbf{u} \in \mathrm{supp}(\mathcal{N})$, then $\mathcal{D} \circ \mathcal{N} \circ \hat{U}_{\mathrm{enc}} = \mathrm{id}^{\otimes k}$.

Proof: The proof, which follows straightforwardly from the discretization proof in standard QEC case, is given in Appendix C. ∎

B. The canonical code and syndrome coding

By the results of the previous subsection, we are now interested in EAQEC codes which correct a particular error set $S \subset (\mathbb{Z}_2)^{2n}$. We first restrict attention to a simple error set, which will turn out to be generic due to the results of Section II-C.

Consider the following trivial encoding operation $\hat{U}_0$ defined by

$$U_0 : |\varphi\rangle|\Phi\rangle^{\otimes c} \mapsto |\varphi\rangle|\mathbf{0}\rangle|\Phi\rangle^{\otimes c}. \tag{12}$$

In other words, the register containing $|\mathbf{0}\rangle$ (of size $\ell = n-k-c$ qubits) is appended to the registers containing $|\varphi\rangle$ (of size k qubits) and $|\Phi\rangle^{\otimes c}$ (of size c qubits each for Alice and Bob). We call the encoded state in (12) the canonical code. What errors can this canonical code correct with such a simple-minded encoding?

Proposition 4: The code given by U_0 and a suitably defined decoding map $\mathcal{D}_0$ can correct the error set $S_0 \in (\mathbb{Z}_2)^{2n}$,

$$S_0 = \{(\alpha(\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2), \mathbf{b}, \mathbf{a}_1 | \beta(\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2), \mathbf{a}, \mathbf{a}_2) : \mathbf{b}, \mathbf{a} \in (\mathbb{Z}_2)^\ell, \mathbf{a}_1, \mathbf{a}_2 \in (\mathbb{Z}_2)^c\}, \tag{13}$$

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

Proof: The protocol is shown in Figure 3. Consider an error vector $\mathbf{u} \in S_0$:

$$\mathbf{u} = (\alpha(\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2), \mathbf{b}, \mathbf{a}_1 | \beta(\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2), \mathbf{a}, \mathbf{a}_2). \tag{14}$$

After applying $N_{\mathbf{u}}$ on the encoded state $|\varphi\rangle|\mathbf{0}\rangle|\Phi\rangle^{\otimes c}$, the state received by Bob becomes (up to a phase factor)

$$\begin{aligned} &N_{\mathbf{u}}\big(|\varphi\rangle|\mathbf{0}\rangle|\Phi\rangle^{\otimes c}\big) \\ &= Z^{\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)} X^{\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)} |\varphi\rangle \otimes X^{\mathbf{a}} Z^{\mathbf{b}} |\mathbf{0}\rangle \otimes (Z^{\mathbf{a}_1} X^{\mathbf{a}_2} \otimes I)|\Phi\rangle^{\otimes c} \\ &= |\varphi'\rangle \otimes |\mathbf{a}\rangle \otimes |\mathbf{a}_1, \mathbf{a}_2\rangle, \end{aligned} \tag{15}$$

where

$$\begin{aligned} |\varphi'\rangle &= Z^{\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)} X^{\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)} |\varphi\rangle & (16)\\ |\mathbf{a}\rangle &= X^{\mathbf{a}} Z^{\mathbf{b}} |\mathbf{0}\rangle = X^{\mathbf{a}} |\mathbf{0}\rangle & (17)\\ |\mathbf{a}_1, \mathbf{a}_2\rangle &= (Z^{\mathbf{a}_1} X^{\mathbf{a}_2} \otimes I)|\Phi\rangle^{\otimes c}. & (18) \end{aligned}$$

As the vector $(\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{b})^T$ completely specifies the error $\mathbf{u}$, it is called the *error syndrome*. The state (15) only depends on the *reduced syndrome* $\mathbf{r} = (\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2)^T$. In effect, $\mathbf{a}$ and $(\mathbf{a}_1, \mathbf{a}_2)$ have been encoded using elementary and superdense coding, respectively. Bob, who holds the entire state (15), may identify the reduced syndrome using the results of section II-D. Bob simultaneously measures the $Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_\ell}$ observables to decode $\mathbf{a}$, the $Z^{\mathbf{e}_1} \otimes Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_c} \otimes Z^{\mathbf{e}_c}$ observables to decode $\mathbf{a}_1$, and the $X^{\mathbf{e}_1} \otimes X^{\mathbf{e}_1}, \ldots, X^{\mathbf{e}_c} \otimes X^{\mathbf{e}_c}$ observables to decode $\mathbf{a}_2$. He then performs $Z^{-\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)} X^{-\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)}$ on the remaining k qubit system $|\varphi'\rangle$, recovering it back to the original state $|\varphi\rangle$.

Since the goal is the transmission of quantum information, no actual measurement is necessary. Instead, Bob can perform the CPTP map $\mathcal{D}_0$ consisting of the controlled unitary

$$U_{0,\mathrm{dec}} = \sum_{\mathbf{a},\mathbf{a}_1,\mathbf{a}_2} Z^{-\alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)} X^{-\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)} \otimes |\mathbf{a}\rangle\langle\mathbf{a}| \otimes |\mathbf{a}_1, \mathbf{a}_2\rangle\langle\mathbf{a}_1, \mathbf{a}_2|,$$

followed by discarding the last two subsystems. ∎

The above code is *degenerate* with respect to the error set S_0, which means that the error can be corrected without knowing the full error syndrome.

We can characterize the canonical code in terms of the *parity check matrix* F given by

$$F = \begin{pmatrix} F_I \\ F_S \end{pmatrix}, \tag{19}$$

$$F_I = \left(\begin{array}{ccc|ccc} \mathbf{0}_{\ell\times k} & \mathbf{I}_{\ell\times\ell} & \mathbf{0}_{\ell\times c} & \mathbf{0}_{\ell\times k} & \mathbf{0}_{\ell\times\ell} & \mathbf{0}_{\ell\times c} \end{array}\right), \tag{20}$$

$$F_S = \left(\begin{array}{ccc|ccc} \mathbf{0}_{c\times k} & \mathbf{0}_{c\times\ell} & \mathbf{I}_{c\times c} & \mathbf{0}_{c\times k} & \mathbf{0}_{c\times\ell} & \mathbf{0}_{c\times c} \\ \mathbf{0}_{c\times k} & \mathbf{0}_{c\times\ell} & \mathbf{0}_{c\times c} & \mathbf{0}_{c\times k} & \mathbf{0}_{c\times\ell} & \mathbf{I}_{c\times c} \end{array}\right), \tag{21}$$

with $\ell = n - k - c$.

The vector space $\mathrm{rowspace}(F)$ decomposes into a direct sum of the isotropic subspace $\mathrm{rowspace}(F_I)$ and symplectic subspace $\mathrm{rowspace}(F_S)$, as in Theorem 1. Define the *symplectic code* corresponding to F by

$$C_0 = \mathrm{rowspace}(F)^\perp$$

where

$$V^\perp = \{\mathbf{w} : \mathbf{w} \odot \mathbf{u}^T = 0,\ \forall \mathbf{u} \in V\}.$$

Note that $(V^\perp)^\perp = V$. Then $C_0^\perp = \mathrm{rowspace}(F)$, $\mathrm{iso}(C_0^\perp) = \mathrm{rowspace}(F_I)$ and $\mathrm{symp}(C_0^\perp) = \mathrm{rowspace}(F_S)$.

The number of ebits used in the code is

$$c = \frac{1}{2} \dim \mathrm{rowspace}(F_S)$$

and the number of encoded qubits is

$$k = n - \dim \mathrm{rowspace}(F_I) - \frac{1}{2} \dim \mathrm{rowspace}(F_S).$$

The code parameter $\hat{k} := k-c$ which is the number of encoded qubits minus the number of ebits used is independent of the symplectic structure of F:

$$\hat{k} = n - \dim \mathrm{rowspace}(F).$$

The error set S_0 can be described in terms of F:

Proposition 5: The set S_0 of errors correctable by the code $\mathcal{C}_0$ is such that, if $\mathbf{u}, \mathbf{u}' \in S_0$ and $\mathbf{u} \neq \mathbf{u}'$, then either

1) $\mathbf{u} - \mathbf{u}' \notin C_0$ (equivalently: $F \odot (\mathbf{u} - \mathbf{u}')^T \neq \mathbf{0}^T$), or
2) $\mathbf{u} - \mathbf{u}' \in \mathrm{iso}(C_0^\perp)$ (equivalently: $\mathbf{u} - \mathbf{u}' \in \mathrm{rowspace}(F_I)$).

Proof: If $\mathbf{u}$ is given by (14) then $F \odot \mathbf{u}^T = \mathbf{r} = (\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2)^T$, the reduced error syndrome. By definition (13), two distinct elements of S_0 either have different reduced syndromes $(\mathbf{a}, \mathbf{a}_1, \mathbf{a}_2)$ (condition 1) or they differ by a vector of the form $(\mathbf{0}, \mathbf{b}, \mathbf{0} | \mathbf{0}, \mathbf{0}, \mathbf{0})$ (condition 2). Observe that condition 1 is analogous to the usual error-correcting condition for classical codes [44]. ∎

The parity check matrix F also specifies the encoding and decoding operations. The space $\mathcal{H}^{\otimes k}$ is encoded into the *codespace* defined by

$$\mathcal{C}_0 = \{U_0 |\varphi\rangle |\Phi\rangle^{\otimes c} : |\varphi\rangle \in \mathcal{H}^{\otimes k}\}.$$

It is not hard to see that the codespace is the simultaneous $+1$ eigenspace of the commuting operators:

1) $I \otimes Z^{\mathbf{e}_i} \otimes I \otimes I,\ i = 1, \ldots, \ell$;
2) $I \otimes I \otimes Z^{\mathbf{e}_j} \otimes Z^{\mathbf{e}_j},\ j = 1, \ldots, c$;
3) $I \otimes I \otimes X^{\mathbf{e}_j} \otimes X^{\mathbf{e}_j},\ j = 1, \ldots, c$.

Above, the first three operators act on Alice's qubits and the fourth on Bob's. Define the matrix

$$B = \left(\begin{array}{c|c} \mathbf{0}_{\ell \times c} & \mathbf{0}_{\ell \times c} \\ \mathbf{I}_{c \times c} & \mathbf{0}_{c \times c} \\ \mathbf{0}_{c \times c} & \mathbf{I}_{c \times c} \end{array} \right). \tag{22}$$

Define the *augmented* parity check matrix

$$F_{\mathrm{aug}} = (F, B) = \left(\begin{array}{cccc|cccc} \mathbf{0}_{\ell \times k} & \mathbf{I}_{\ell \times \ell} & \mathbf{0}_{\ell \times c} & \mathbf{0}_{\ell \times c} & \mathbf{0}_{\ell \times k} & \mathbf{0}_{\ell \times \ell} & \mathbf{0}_{\ell \times c} & \mathbf{0}_{\ell \times c} \\ \mathbf{0}_{c \times k} & \mathbf{0}_{c \times \ell} & \mathbf{I}_{c \times c} & \mathbf{I}_{c \times c} & \mathbf{0}_{c \times k} & \mathbf{0}_{c \times \ell} & \mathbf{0}_{c \times c} & \mathbf{0}_{c \times c} \\ \mathbf{0}_{c \times k} & \mathbf{0}_{c \times \ell} & \mathbf{0}_{c \times c} & \mathbf{0}_{c \times c} & \mathbf{0}_{c \times k} & \mathbf{0}_{c \times \ell} & \mathbf{I}_{c \times c} & \mathbf{I}_{c \times c} \end{array} \right).$$

Observe that $\mathrm{rowspace}(F_{\mathrm{aug}})$ is purely isotropic. The codespace is now described as the simultaneous $+1$ eigenspace of $\{N_{\mathbf{w}} : \mathbf{w} \in \mathrm{rowspace}(F_{\mathrm{aug}})\}$, or, equivalently that of

$$\mathcal{G}_0 = \{N_{\mathbf{w}} : \mathbf{w} \text{ is a row of } F_{\mathrm{aug}}\}.$$

The decoding operation $\mathcal{D}_0$ is also described in terms of F. The reduced syndrome $\mathbf{r} = F \odot \mathbf{u}^T$ is obtained by simultaneously measuring the observables in $\mathcal{G}_0$. The reduced error syndrome corresponds to a number of possible errors $\mathbf{u} \in S_0$ which all have an identical effect on the codespace. Bob performs $\hat{N}_{\mathbf{u}} = \hat{N}_{-\mathbf{u}}$ to undo the error.

C. The general case

We now present our main result: how to convert an arbitrary $(n + \hat{k})$-dimensional subspace C of $(\mathbb{Z}_2)^{2n}$ into an EAQEC code. Consider the $(n - \hat{k})$-dimensional subspace $C^\perp$. By Theorem 1, there exists a symplectic basis of $(\mathbb{Z}_2)^{2n}$ consisting of hyperbolic pairs $(\mathbf{u}_i, \mathbf{v}_i)$, $i = 1, \ldots, n$, such that the ordered set $\mathcal{R} = \{\mathbf{u}_{k+1}, \ldots, \mathbf{u}_n, \mathbf{v}_{k+\ell+1}, \ldots, \mathbf{v}_n\}$ is a basis for $C^\perp$, for some $c, \ell \geq 0$ with $2c + \ell = n - \hat{k}$, and $k - c = \hat{k}$. Let H be the matrix whose rows consist of the elements of $\mathcal{R}$ in the order given from top to bottom. Let Υ be the symplectomorphism defined by

$$\Upsilon(\mathbf{u}_i) = \mathbf{g}_i \tag{23}$$
$$\Upsilon(\mathbf{v}_i) = \mathbf{h}_i. \tag{24}$$

Recall the matrix F given by (19)-(21). Observe that, with a slight abuse of notation,

$$\Upsilon(H) = F$$

in the sense that Υ takes the ith row of H to the ith row of F. We may extend Υ to act on $(\mathbb{Z}_2)^{2(n+c)}$, including a trivial action on the bits corresponding to Bob's side. Then

$$\Upsilon(H_{\mathrm{aug}}) = F_{\mathrm{aug}}, \tag{25}$$

where $H_{\mathrm{aug}} = (H, B)$.

In terms of vector spaces

$$\Upsilon(C^\perp) = C_0^\perp, \tag{26}$$
$$\Upsilon(\mathrm{iso}(C^\perp)) = \mathrm{iso}(C_0^\perp). \tag{27}$$

Note that $c = \frac{1}{2} \dim \mathrm{symp}(C^\perp)$. We are now ready for our main result:

Theorem 6: There exists an $[[n, k; c]]$ EAQEC code defined by the encoding and decoding pair $(\hat{U}_{\mathrm{enc}}, \mathcal{D})$ with the following properties:

1) It can correct the error set S defined by: if $\mathbf{u}, \mathbf{u}' \in S$ and $\mathbf{u} \neq \mathbf{u}'$, then either
   a) $\mathbf{u} - \mathbf{u}' \notin C$ (equivalently: $H \odot (\mathbf{u} - \mathbf{u}')^T \neq \mathbf{0}^T$), or
   b) $\mathbf{u} - \mathbf{u}' \in \mathrm{iso}(C^\perp)$ (equivalently: $\mathbf{u} - \mathbf{u}' \in \mathrm{rowspace}(H_I)$).
2) The codespace $\mathcal{C} = \hat{U}_{\mathrm{enc}}(\mathcal{H}^{\otimes k})$ is a simultaneous eigenspace of the ordered set
   $$\mathcal{G} = \{N_{\mathbf{w}} : \mathbf{w} \text{ is a row of } H_{\mathrm{aug}}\},$$
   where $H_{\mathrm{aug}} = (H, B)$, with B given by (22).
3) To decode, the reduced error syndrome
   $$\mathbf{r} = H \odot \mathbf{u}^T \tag{28}$$
   is obtained by simultaneously measuring the observables from $\mathcal{G}$. Bob finds a $\mathbf{u}$ satisfying (28) and performs $\hat{N}_{\mathbf{u}}$ to undo the error.

Remark The above theorem generalizes the error correcting conditions of [11], [8] for quantum error correcting codes unassisted by entanglement. When $c = 0$ then $C^\perp = \mathrm{iso}(C^\perp)$ and no entanglement is used in the protocol. We call such codes *self-orthogonal*.

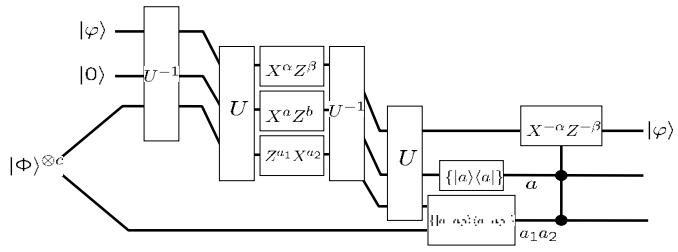

Fig. 4. Generalizing the canonical code construction.

Proof: By Theorem 2 there exists a unitary U_Υ such that for all $\mathbf{u} \in (\mathbb{Z}_2)^{2n}$

$$[N_{\Upsilon(\mathbf{u})}] = [U_\Upsilon N_\mathbf{u} U_\Upsilon^{-1}], \tag{29}$$

and hence

$$\hat{N}_{\Upsilon(\mathbf{u})} = \hat{U}_\Upsilon \circ \hat{N}_\mathbf{u} \circ \hat{U}_\Upsilon^{-1}.$$

The above also holds for Υ and $\hat{U}_\Upsilon$ extended to act trivially on Bob's side.

Our EAQEC code is defined by $U_{\text{enc}} = U_\Upsilon^{-1} U_0$ and $\mathcal{D} = \mathcal{D}_0 \circ \hat{U}_\Upsilon$, as shown in Figure 4.

1) Recall the error set S_0 defined in Proposition 5. From (26) and (27) it follows that $\Upsilon(S) = S_0$. By Proposition 5, for all $\mathbf{u} \in S$,

$$\mathcal{D}_0 \circ \hat{N}_{\Upsilon(\mathbf{u})} \circ \hat{U}_0 = \mathrm{id}^{\otimes k},$$

from which

$$\mathcal{D} \circ \hat{N}_\mathbf{u} \circ \hat{U}_{\text{enc}} = \mathrm{id}^{\otimes k}$$

follows. Thus, the code $(\hat{U}_{\text{enc}}, \mathcal{D})$ corrects the error set S.

2) The codespace is $\mathcal{C} = U_\Upsilon^{-1}(\mathcal{C}_0)$, by definition. According to (25), $\mathcal{C}_0$ is the simultaneous $+1$ eigenspace of

$$\mathcal{G}_0 = \{N_{\Upsilon(\mathbf{w})} : \mathbf{w} \text{ is a row of } H_{\text{aug}}\},$$

or by (29), the set

$$\mathcal{G}_0' = \{U_\Upsilon N_\mathbf{w} U_\Upsilon^{-1} : \mathbf{w} \text{ is a row of } H_{\text{aug}}\}.$$

Lemma 7 below implies that the codespace $\mathcal{C}$ is a simultaneous eigenspace of $\mathcal{G}$.

3) Assume that error $\mathbf{u} \in S$ occurs. The operation $\mathcal{D}_0$ involves
   a) measuring the set of operators given by $\mathcal{G}_0$, or equivalently $\mathcal{G}_0'$, yielding the reduced syndrome
   $$\mathbf{r} = F \odot \Upsilon(\mathbf{u})^T;$$
   b) performing $\hat{N}_{\Upsilon(\mathbf{u})}$, where $\Upsilon(\mathbf{u}) \in S_0$ is an error consistent with the observed syndrome $\mathbf{r}$.

(28) holds because

$$\mathbf{r} = \Upsilon(H) \odot \Upsilon(\mathbf{u})^T = H \odot \mathbf{u}^T.$$

By Lemma 8 below, performing $\mathcal{D} = \mathcal{D}_0 \circ \hat{U}_\Upsilon$ is equivalent to measuring the set $\mathcal{G}$, followed by performing $\hat{N}_\mathbf{u} = \hat{U}_\Upsilon^{-1} \circ \hat{N}_{\Upsilon(\mathbf{u})} \circ \hat{U}_\Upsilon$, followed by $\hat{U}_\Upsilon$ to undo the encoding. If the final $\hat{U}_\Upsilon$ is omitted, one recovers the encoded state rather than the original one.

■

Lemma 7: If $\mathcal{C}_0$ is a simultaneous eigenspace of Pauli operators from the set $\mathcal{G}_0'$ then $\mathcal{C} = U^{-1}(\mathcal{C}_0)$ is a simultaneous eigenspace of Pauli operators from the set $\mathcal{G} = \{U^{-1}\mathbf{A}U : \mathbf{A} \in \mathcal{G}_0'\}$.

Proof: Observe that if

$$\mathbf{A}|\psi\rangle = \alpha|\psi\rangle,$$

then

$$(U^{-1}\mathbf{A}U)U^{-1}|\psi\rangle = \alpha U^{-1}|\psi\rangle.$$

■

Lemma 8: Performing U followed by measuring the operator $\mathbf{A}$ is equivalent to measuring the operator $U^{-1}\mathbf{A}U$ followed by performing U.

Proof: Let Π_i be a projector onto the eigenspace corresponding to eigenvalue λ_i of $\mathbf{A}$. Performing U followed by measuring the operator $\mathbf{A}$ is equivalent to the instrument (generalized measurement) given by the set of operators $\{\Pi_i U\}$. The operator $U^{-1}\mathbf{A}U$ has the same eigenvalues as $\mathbf{A}$, and the projector onto the eigenspace corresponding to eigenvalue λ_i is $U^{-1}\Pi_i U$. Measuring the operator $U^{-1}\mathbf{A}U$ followed by performing U is equivalent to the instrument $\{U(U^{-1}\Pi_i U)\} = \{\Pi_i U\}$. ■

D. Distance

The notion of distance provides a convenient way to characterize the error-correcting properties of a code. We start by defining the *weight* of a vector $\mathbf{u} = (\mathbf{z}|\mathbf{x}) \in (\mathbb{Z}_2)^{2n}$ by $\mathrm{wt}(\mathbf{u}) = \mathrm{wt}(\mathbf{z} \vee \mathbf{x})$. Here $\vee$ denotes the bitwise logical "or", and $\mathrm{wt}(\mathbf{y})$ is the number of non-zero bits in $\mathbf{y} \in (\mathbb{Z}_2)^n$. In terms of the Pauli group, $\mathrm{wt}(\mathbf{u})$ is the number of single qubit Pauli matrices in $N_\mathbf{u}$ not equal to the identity I.

Consider a symplectic code C. The *distance* of C is the maximum d such that for each nonzero $\mathbf{u}$ of weight $< d$ either

1) $\mathbf{u} \notin C$, or
2) $\mathbf{u} \in \mathrm{iso}(C^\perp)$

It is called *non-degenerate* if the second condition is not invoked. A code is said to correct t errors if it corrects the error set $\{\mathbf{u} : \mathrm{wt}(\mathbf{u}) \le t\}$ but not $\{\mathbf{u} : \mathrm{wt}(\mathbf{u}) \le t+1\}$. Comparing these definitions with Theorem 6, a code with distance $d = 2t+1$ can correct t errors. An $[[n, k; c]]$ EAQEC code with distance d will be referred to as an $[[n, k, d; c]]$ code.

IV. Relation to quaternary codes

We shall now show how to construct non-degenerate EAQEC codes from classical codes over $\mathbb{F}_4$, generalizing the work of [8]. Following the presentation of Forney et al. [39], the addition table of the additive group of the quaternary field $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$ is given by

$+$	0	$\overline{\omega}$	1	ω
0	0	$\overline{\omega}$	1	ω
$\overline{\omega}$	$\overline{\omega}$	0	ω	1
1	1	ω	0	$\overline{\omega}$
ω	ω	1	$\overline{\omega}$	0

Comparing the above to the addition table of $(\mathbb{Z}_2)^2$ establishes the isomorphism $\gamma : \mathbb{F}_4 \to (\mathbb{Z}_2)^2$, given by the table

$\mathbb{F}_4$	$(\mathbb{Z}_2)^2$
0	00
$\overline{\omega}$	01
1	11
ω	10

The multiplication table for $\mathbb{F}_4$ is defined as

$\times$	0	$\overline{\omega}$	1	ω
0	0	0	0	0
$\overline{\omega}$	0	ω	$\overline{\omega}$	1
1	0	$\overline{\omega}$	1	ω
ω	0	1	ω	$\overline{\omega}$

Define the *traces* (Tr) of the elements $\{0, 1, \omega, \overline{\omega}\}$ of $\mathbb{F}_4$ as $\{0, 0, 1, 1\}$, and their *conjugates* ("$\dagger$") as $\{0, 1, \overline{\omega}, \omega\}$. Intuitively, $\operatorname{Tr} a$ measures the "ω-ness" of $a \in \mathbb{F}_4$. Observe that $a = 0$ if and only if both $\operatorname{Tr} \omega a = 0$ and $\operatorname{Tr} \overline{\omega} a = 0$. The *Hermitian inner product* of two elements $a, b \in \mathbb{F}_4$ is defined as $\langle a, b\rangle = a^\dagger b \in \mathbb{F}_4$. The *trace product* is defined as $\operatorname{Tr}\langle a, b\rangle \in \mathbb{F}_2$. The trace product table is readily found to be

$\operatorname{Tr}\langle\,,\rangle$	0	$\overline{\omega}$	1	ω
0	0	0	0	0
$\overline{\omega}$	0	0	1	1
1	0	1	0	1
ω	0	1	1	0

Comparing the above to the $\odot$ table of $(\mathbb{Z}_2)^2$ establishes the identity

$$\operatorname{Tr}\langle a, b\rangle = \gamma(a) \odot \gamma(b).$$

These notions can be generalized to n-dimensional vector spaces over $\mathbb{F}_4$. Thus, for $\mathbf{a}, \mathbf{b} \in (\mathbb{F}_4)^n$,

$$\operatorname{Tr}\langle \mathbf{a}, \mathbf{b}\rangle = \gamma(\mathbf{a}) \odot \gamma(\mathbf{b})^T. \tag{30}$$

Let $\operatorname{wt}_4(\mathbf{a})$ be the number of non-zero bits in $\mathbf{a} \in (\mathbb{F}_4)^n$. Then we have another identity

$$\operatorname{wt}(\gamma(\mathbf{a})) = \operatorname{wt}_4(\mathbf{a}), \tag{31}$$

where $\gamma(\mathbf{a}) \in (\mathbb{Z}_2)^{2n}$.

Proposition 9: If a classical $[n, k, d]_4$ code exists then an $[[n, 2k-n+c, d; c]]$ EAQEC code exists for some non-negative integer c.

Proof: Consider a classical $[n, k, d]_4$ code (the subscript 4 emphasizes that the code is over $\mathbb{F}_4$) with an $(n-k) \times n$ quaternary parity check matrix H_4. By definition, for each nonzero $\mathbf{a} \in (\mathbb{F}_4)^n$ such that $\operatorname{wt}_4(\mathbf{a}) < d$,

$$\langle H_4, \mathbf{a}\rangle \neq \mathbf{0}^T.$$

This is equivalent to the logical statement

$$\operatorname{Tr}\langle \omega H_4, \mathbf{a}\rangle \neq \mathbf{0}^T \ \vee \ \operatorname{Tr}\langle \overline{\omega} H_4, \mathbf{a}\rangle \neq \mathbf{0}^T.$$

This is further equivalent to

$$\operatorname{Tr}\langle \widetilde{H}_4, \mathbf{a}\rangle \neq \mathbf{0}^T,$$

where

$$\widetilde{H}_4 = \begin{pmatrix} \omega H_4 \\ \overline{\omega} H_4 \end{pmatrix}. \tag{32}$$

Define the $(2n-2k) \times 2n$ symplectic matrix $H = \gamma(\widetilde{H}_4)$. By the correspondences (30) and (31),

$$H \odot \mathbf{u}^T \neq \mathbf{0}^T,$$

holds for each nonzero $\mathbf{u} \in (\mathbb{Z}_2)^{2n}$ with $\operatorname{wt}(\mathbf{u}) < d$. Thus $C = \operatorname{rowspace}(H)^\perp$ defines a non-degenerate $[[n, 2k-n+c, d; c]]$ EAQEC code, where

$$c = \frac{1}{2} \dim \operatorname{symp}(C).$$

■

Any classical binary $[n, k, d]_2$ code may be viewed as a quaternary $[n, k, d]_4$ code. In this case, the above construction gives rise to a CSS-type code.

V. Catalytic quantum error-correcting codes

So far we have been considering *communication* scenarios involving two spatially separated parties Alice and Bob connected by a noisy channel $\mathcal{N}$. In this setting, entanglement between them is a meaningful resource. However, this might not always be the case. What if Alice and Bob are separated only in time—that is, what if the receiver is the same as the sender, but at a later time? This is the problem of storing quantum information. For example, $\mathcal{N}$ could represent the time evolution of the state of a quantum computer. This type of error correction is a key problem of quantum computation. In this case, the idea of pre-shared entanglement between Alice and Bob no longer makes sense.

It would therefore seem at first glance that EAQEC codes have no direct application to quantum computation, except possibly to protect internal communications within a quantum computer. However, we can connect EAQEC codes to the related idea of *catalytic* quantum error correction, which we will now show does make sense in the context of storing information. We thus map the storage problem, which is relevant to computation, back to a communication problem where EAQEC codes can be useful.

Consider the following scenario. Alice and Bob have access to a noiseless channel, through which they are allowed to send c qubits error-free, in addition to a regular noisy channel $\mathcal{N}$. This noiseless channel, however, only serves as a catalyst and is returned at the end of the protocol. We define such an $[[n, \hat{k} = k-c; c]]_C$ *catalytic* quantum error correcting (CQEC) code by:

- An encoding isometry $\mathcal{E} : \mathcal{L}^{\otimes k} \otimes \mathcal{L}^{\otimes c} \to \mathcal{L}^{\otimes n}$
- A decoding CPTP map $\mathcal{D} : \mathcal{L}^{\otimes n} \otimes \mathcal{L}^{\otimes c} \to \mathcal{L}^{\otimes k}$

such that

$$\mathcal{D} \circ (\mathcal{N} \otimes \mathrm{id}^{\otimes c}) \circ \mathcal{E} = \mathrm{id}^{\otimes k} = \mathrm{id}^{\otimes \hat{k}} \otimes \mathrm{id}^{\otimes c}. \tag{33}$$

Please note that we use the subscript C to distinguish $[[n, k; c]]$ EAQEC and $[[n, \hat{k}; c]]_C$ CQEC codes, to avoid confusion between the yield k and the net yield $\hat{k}$. The above may be written as a resource inequality

$$\langle \mathcal{N} \rangle + c\,[q \to q] \geq \hat{k}\,[q \to q] + c\,[q \to q]. \tag{34}$$

Figure 5 shows how any $[[n, k; c]]$ EAQEC code $(\mathcal{E}, \mathcal{D})$ gives rise to a $[[n, \hat{k}; c]]_C$ CQEC code. This construction may

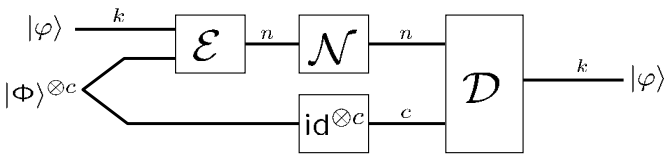

Fig. 5. A catalytic quantum error-correcting code.

be understood in terms of resource inequalities. The simple protocol called *entanglement distribution* written as

$$c\,[q \to q] \geq c\,[q\,q],$$

creates c ebits of entanglement by sending half of a locally prepared state $|\Phi\rangle^{\otimes c}$ through the channel $\mathrm{id}^{\otimes c}$. The CQEC code is obtained by combining entanglement distribution with the EAQEC code:

$$\begin{aligned} \langle\mathcal{N}\rangle + c\,[q \to q] &\geq \langle\mathcal{N}\rangle + c\,[q\,q] \\ &\geq k\,[q \to q] \\ &= \hat{k}\,[q \to q] + c\,[q \to q]. \end{aligned}$$

Assume now that Alice and Bob have access to m copies of the chanel $\mathcal{N}$. Performing the CQEC protocol m times in parallel (i.e. using the code $(\mathcal{E}^{\otimes m}, \mathcal{D}^{\otimes m})$) gives

$$m\langle\mathcal{N}\rangle + mc\,[q \to q] \geq m\hat{k}\,[q \to q] + mc\,[q \to q].$$

The size of the catalyst can actually be reduced from mc to c:

$$m\langle\mathcal{N}\rangle + c\,[q \to q] \geq m\hat{k}\,[q \to q] + c\,[q \to q]. \tag{35}$$

The proof is by induction. The statement is trivial for $m = 1$. For the inductive step, assume true for m. Then (35) holds for $m + 1$:

$$\begin{aligned} &(m+1)\langle\mathcal{N}\rangle + c\,[q \to q] \\ &\qquad = \langle\mathcal{N}\rangle + m\langle\mathcal{N}\rangle + c\,[q \to q] \\ &\qquad \geq \langle\mathcal{N}\rangle + m\hat{k}\,[q \to q] + c\,[q \to q] \\ &\qquad \geq m\hat{k}\,[q \to q] + \hat{k}\,[q \to q] + c\,[q \to q]. \end{aligned}$$

A more conventional formulation of this catalyst reduction is given in the lemma below.

Lemma 10: If (33) is satisfied then for any non-negative integer m there exists a CQEC code $(\mathcal{E}_m, \mathcal{D}_m)$ for the channel $\mathcal{N}^{\otimes m}$ in the sense that

$$\mathcal{D}_m \circ (\mathcal{N}^{\otimes m} \otimes \mathrm{id}^{\otimes c}) \circ \mathcal{E}_m = \mathrm{id}^{\otimes m\hat{k}} \otimes \mathrm{id}^{\otimes c}.$$

Proof: The inductive step is shown in the Figure 6. ∎

The above construction is rather sensitive to perturbations. If in any particular block a channel worse than $\mathcal{N}$ is experienced, the resulting channel will not be pure and the next block will start with an impure catalyst.

One may rightly ask about where one could obtain a catalyst to begin with. After all, perfect channels are not normally available, or we would not need error correction in the first place. The basic idea is to use an ordinary $c = 0$ QEC code. This is shown in Figure 7. An $[[n, \hat{k}; c]]_C$ CQEC code for

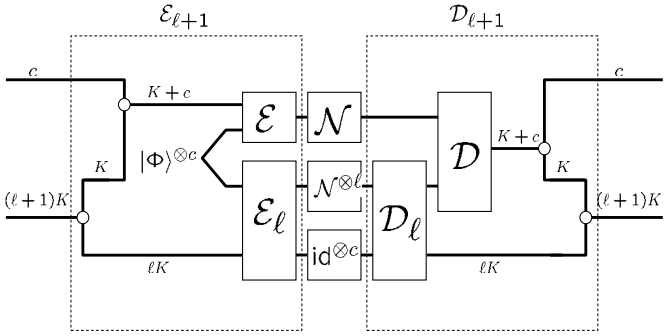

Fig. 6. The inductive step.

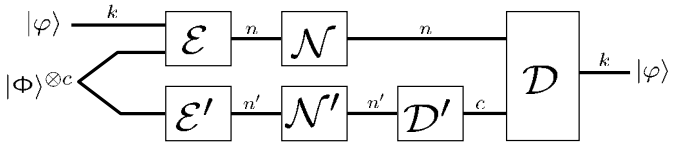

Fig. 7. Constructing a QEC code from a seed QEC code and a CQEC code.

the channel $\mathcal{N}$ combined with a $[[n', c; 0]]$ QEC code for the channel $\mathcal{N}'$ gives an $[[n + n', \hat{k} + c; 0]]$ QEC code for the channel $\mathcal{N} \otimes \mathcal{N}'$. The combined code can be used as a catalyst for an even larger code. In this way a sizeable catalyst can be built up pretty quickly.

It is worth looking at this construction from a purely mathematical point of view. Let $C \subset (\mathbb{Z}_2)^{2n}$ and $C' \subset (\mathbb{Z}_2)^{2n'}$ be the symplectic codes corresponding to the $[[n, \hat{k}; c]]_C$ CQEC code and $[[n', c; 0]]$ QEC code, respectively. Let H and H' be the respective parity check matrices, as in Section III-C. Note that $C'^{\perp} = \mathrm{iso}(C'^{\perp})$. Let $\mathbf{u}_i$, $i = 1, \ldots, c$, be vectors in $(\mathbb{Z}_2)^{2n'}$ which, together with a basis for $C'^{\perp}$, form a maximal n'-dimensional isotropic subspace of $(\mathbb{Z}_2)^{2n'}$. Recall the notation $\mathbf{g}_i = (\mathbf{e}_i|\mathbf{0}) \in (\mathbb{Z}_2)^{2c}$. Let Υ be a symplectomorphism such that $\Upsilon(\mathbf{g}_i) = \mathbf{u}_i$. Define the $(n - \hat{k}) \times 2n'$ matrix $B' = \Upsilon(B)$ with B defined as in (22) and $\ell = n - \hat{k} - 2c$. Note that the rows of B' are in C'. Then

$$\widetilde{H}_{\mathrm{aug}} = \begin{pmatrix} H, & B' \\ \mathbf{0}_{(n'-c)\times 2n}, & H' \end{pmatrix}$$

is the parity check matrix for the combined $[[n + n', \hat{k} + c; 0]]$ QEC code. By construction, it must be self-orthogonal. So we can think of the catalytic code construction as a way of using EAQEC codes—designed for communication protocols—to build up standard QEC codes, which can be useful for storage.

VI. A variation on EAQEC codes

One lesson learned from quantum Shannon theory [19] is that catalytic and non-catalytic codes have similar performance. In this section we mimic the quantum Shannon theoretical construction from [19]. First we construct codes for sending *classical* information with entanglement assistance. Then we make these protocols *coherent* in the sense of [19], [24] to obtain a variation on EAQEC codes in which entanglement is generated as well as quantum communication. The end result is what we will call "type II" EAQEC codes,

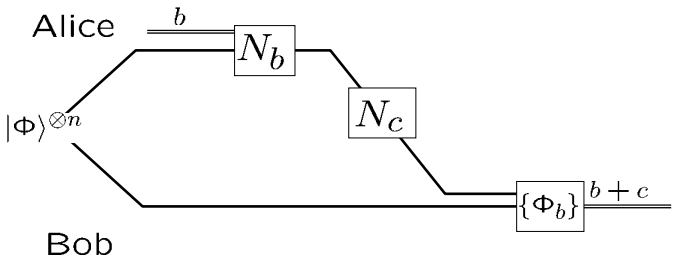

Fig. 8. Reduction from an EACEC code to a classical code over $\mathbb{F}_4$.

which can be constructed without the machinery of symplectic linear algebra.

A. EA-codes for sending classical information

The communication scenario again involves two spatially separated parties, Alice and Bob. The resources at their disposal are a noisy channel $\mathcal{N} : \mathcal{L}^{\otimes n} \to \mathcal{L}^{\otimes n}$ and the shared c ebit state $|\Phi\rangle^{\otimes c}$. Now Alice wishes to convey an element of $(\mathbb{F}_4)^k$ *perfectly* to Bob using the above resources. A protocol which does this is called an $[n, k; c]_4$ entanglement-assisted classical error correcting code, or EACEC code for short. We write the above as a resource inequality

$$\langle \mathcal{N} \rangle + c\,[q\,q] \geq 2k\,[c \to c]. \tag{36}$$

The factor of 2 accounts for the conversion from quaternary to binary.

Recall the isomorphism $\gamma : (\mathbb{F}_4)^n \to (\mathbb{Z}_2)^{2n}$. It allows us to, with a slight abuse of notation, speak of error sets $S \subset (\mathbb{F}_4)^n$, and Pauli matrices $N_{\mathbf{a}}$, $\mathbf{a} \in (\mathbb{F}_4)^n$. Let $S \subset (\mathbb{F}_4)^n$ be the support of $\mathcal{N}$. An easy modification of Theorem 3 ensures that correctly decoding the message for the set of channels $\{\hat{N}_{\mathbf{a}} : \mathbf{a} \in S\}$ suffices for the correct decoding of $\mathcal{N}$. The notion of distance for EACEC codes is equivalent to the one for classical quaternary codes. An $[n, k; c]_4$ EACEC code of distance d is called an $[n, k, d; c]_4$ EACEC code.

Proposition 11: If there exists an $[n, k]_4$ classical code (over $\mathbb{F}_4$) which corrects the error set $S \subset (\mathbb{F}_4)^n$, then there exists an $[n, k; n]_4$ EACEC code which corrects the same error set.

Proof: We will show that superdense coding establishes an equivalence between a quantum Pauli error $N_{\mathbf{c}}$ and a classical error $\mathbf{c}$.

Assume $\mathbf{c} = 0$, corresponding to no error. Alice superdense encodes $\mathbf{b}$ by performing $N_{\mathbf{b}}$ on her half of $|\Phi\rangle^{\otimes n}$. Bob performs a measurement in the $\{|\Phi_{\mathbf{b}}\rangle\langle\Phi_{\mathbf{b}}| : \mathbf{b} \in (\mathbb{F}_4)^n\}$ basis, where $|\Phi_{\mathbf{b}}\rangle = (N_{\mathbf{b}} \otimes I)|\Phi\rangle$, thus decoding $\mathbf{b}$.

If the channel is $\hat{N}_{\mathbf{c}}$ for some $\mathbf{c} \in S$, then Alice's effective encoding becomes $N_{\mathbf{c}} N_{\mathbf{b}}$ which is a representative of $[N_{\mathbf{b}+\mathbf{c}}]$. Bob's measurement will reveal $\mathbf{b} + \mathbf{c}$ instead of $\mathbf{b}$. This is the message with a classical error $\mathbf{c} \in S$. The encoding preparation, followed by quantum error $\hat{N}_{\mathbf{c}}$ and decoding measurement, simulates the noisy classical channel $\mathbf{b} \mapsto \mathbf{b}+\mathbf{c}$. The theorem now follows, since the classical code can correct any error $c \in S$. ∎

Thus there is a direct correspondence between $[n, k, d]_4$ classical codes and $[n, k, d; n]_4$ EACEC codes. On the other hand, in Section IV we saw that an $[n, k, d]_4$ classical code defines an $[[n, 2k - n + c, d; c]]$ EAQEC code. In the next subsection we show how to construct a variation on an $[[n, 2k-n+c, d; c]]$ EAQEC code from an $[n, k, d; n]_4$ EACEC code via "coherification."

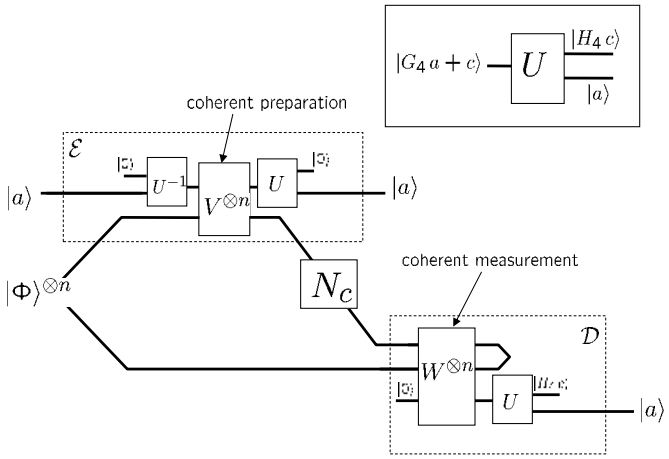

Fig. 9. The circuit implementing a coherent EACEC code. The upper right hand corner defines U in terms of the quaternary code with parity check matrix H_4 and generating matrix G_4.

B. Coherent EACEC codes

At this point we need to introduce one more resource, *coherent communication* [24]. Let $\{|0\rangle, |1\rangle\}$ denote a preferred basis for a qubit system. The isometric channel which implements the change of basis

$$\Delta_2 : |i\rangle^A \mapsto |i\rangle^A |i\rangle^B,\ i = 0, 1$$

is called the *coherent bit* (or *cobit*) channel. The superscript A denotes a system held by Alice and B denotes a system held by Bob. It is regarded as a coherent version of a classical bit channel. Viewing it as a resource, we use the symbol $[q \to q\,q]$. *Coherifying* a protocol is a broad notion marked by replacing classical communication by coherent communication [19], [24]. It was shown in [24] that superdense coding can be made coherent, i.e. that the following resource inequality holds:

$$[q \to q] + [q\,q] \geq 2[q \to q\,q]. \tag{37}$$

Consider an $[n, k, d; n]_4$ EACEC code, given by (36). It can also be made coherent thanks to its connection to superdense coding. In other words, (36) can be upgraded to

$$\langle \mathcal{N} \rangle + n\,[q\,q] \geq 2k\,[q \to q\,q]. \tag{38}$$

An explicit circuit implementing this resource inequality is given in Figure 9. The states $\{|\mathbf{a}\rangle : \mathbf{a} \in (\mathbb{F}_4)^k\}$ form a basis for a $2k$ qubit space. $\{N_{\mathbf{c}}\}$ is a Pauli matrix whose index $\mathbf{c} \in (\mathbb{F}_4)^n$ is in the support of $\mathcal{N}$. H_4 is the $(n - k) \times n$ quaternary parity check matrix for the classical $[n, k, d]_4$ code which corrects all such $\mathbf{c}$. G_4 is the corresponding $n \times k$ generator matrix such that $H_4 G_4 = \mathbf{0}_{(n-k)\times k}$. The box in the upper right hand corner defines the $4^n \times 4^n$ unitary matrix

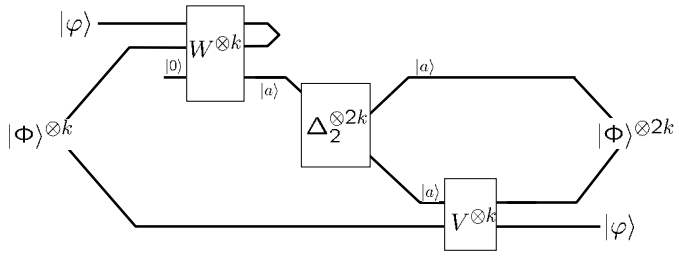

Fig. 10. The circuit implementing coherent teleportation.

U. There $G_4\mathbf{a} \in (\mathbb{F}_4)^n$ is an encoded element $\mathbf{a}$ of $(\mathbb{F}_4)^k$. The unitaries V and W are given by $V = \sum_{j\in\mathbb{F}_4} |j\rangle\langle j| \otimes N_j$ and

$$W(|\varphi\rangle|0\rangle) = \sum_{j\in\mathbb{F}_4} \langle\Phi_+|(N_j^\dagger \otimes I)|\varphi\rangle\,(|\Phi_+\rangle|j\rangle).$$

Harrow [24] also exhibited a coherent version of quantum teleportation [23], written as

$$2k\,[q \to q\,q] + k\,[q\,q] \geq k\,[q \to q] + 2k\,[q\,q]. \qquad (39)$$

Figure 10 depicts a circuit implementing this resource inequality.

Combining (38) with (39) gives

$$\langle\mathcal{N}\rangle + (n+k)\,[q\,q] \geq k\,[q \to q] + 2k\,[q\,q]. \qquad (40)$$

This differs from a hypothetical $[[n, k; n-k]]$ EAQEC code[4] given by

$$\langle\mathcal{N}\rangle + (n-k)\,[q\,q] \geq k\,[q \to q]$$

in that an extra $2k\,[q\,q]$ is needed as a catalyst. We call this a *type II* $[[n, k; n-k; 2k]]$ EAQEC code, and will refer to the EAQEC codes from Section III-C as *type I* EAQEC codes. A type II EAQEC code is not as versatile as regular type I EAQEC codes. The catalyst does not allow it to be converted into a catalytic QEC code, for example. Also, type II EAQEC codes appear to be limited to $\mathbb{F}_4$ construction.

As in the original Shannon theoretical result [19] (Figure 1), type II EAQEC codes (40) can be combined with superdense coding (11) to give a catalytic version of an EACEC code (36):

$$\langle\mathcal{N}\rangle + n\,[q\,q] + k\,[q\,q] \geq 2k\,[c \to c] + k\,[q\,q].$$

This does not hold for type I EAQEC codes of Section III, unless c equals its maximal value of $n-k$.

VII. Bounds on performance

In this section we shall see that the performance of EAQEC codes is comparable to the performance of QEC codes (which are a special case of EAQEC codes).

The two most important outer bounds for QEC codes are the quantum Singleton bound [5], [12] and the quantum Hamming bound [3]. Given an $[[n, k, d]]$ QEC code (which is an $[[n, k, d; 0]]$ EAQEC code), the quantum Singleton bound reads

$$n - k \geq 2(d-1).$$

[4] This EAQEC code has the maximum value of $c = n-k$.

The quantum Hamming bound holds only for non-degenerate codes and reads

$$\sum_{j=0}^{\lfloor\frac{d-1}{2}\rfloor} 3^j \binom{n}{j} \leq 2^{n-k}.$$

The proofs of these bounds [3], [12] are easily adapted to EAQEC codes. This was first noted by Bowen [38] in the case of the quantum Hamming bound. Consequently, an $[[n, k, d; c]]$ EAQEC code satisfies both bounds for any value of c. Note that the $\mathbb{F}_4$ construction connects the quantum Singleton bound to the classical Singleton bound $n - k \geq d - 1$. An $[n, k, d]_4$ code saturating the classical Singleton bound implies an $[[n, 2k-n+c, d; c]]$ EAQEC code saturating the quantum Singleton bound.

It is instructive to examine the asymptotic performance of quantum codes on a particular channel. A popular choice is the tensor power channel $\mathcal{N}^{\otimes n}$, where $\mathcal{N}$ is the depolarizing channel with Kraus operators $\{\sqrt{p_0}I, \sqrt{p_1}X, \sqrt{p_2}Y, \sqrt{p_3}Z\}$, for some probability vector $\mathbf{p} = (p_0, p_1, p_2, p_3)$.

It is well known that the maximal transmission rate $R = k/n$ achievable by a non-degenerate QEC code (in the sense of vanishing error for large n on the channel $\mathcal{N}^{\otimes n}$) is equal to the *hashing bound* $R = 1 - H(\mathbf{p})$. Here $H(\mathbf{p})$ is the Shannon entropy of the probability distribution $\mathbf{p}$. This bound is attained by picking a random self-orthogonal code. However no explicit constructions are known which achieve this bound.

Interestingly, the $\mathbb{F}_4$ construction also connects the hashing bound to the Shannon bound for quaternary channels. Consider the quaternary channel $a \mapsto a + t$, where t takes on values $0, \omega, 1, \overline{\omega}$, with respective probabilities p_0, p_1, p_2, p_3. The maximal achievable rate $R = k/n$ for this channel was proved by Shannon to equal $R = 2 - H(\mathbf{p})$. An $[n, k]_4$ code saturating the Shannon bound implies an $[[n, 2k-n+c; c]]$ EAQEC code, or CQEC code, achieving the hashing bound! The idea is to directly investigate the symplectic structure of such a *catalytic* QEC code, and then using the idea of bootstrapping the method from Figure 7 will enable us to construct a QEC code with similar properties.

VIII. The $[[3, 1, 3; 2]]$ EAQEC code

In this section, we will demonstrate our construction of the $[[3, 1, 3; 2]]$ EAQEC code and relate this code to Bowen's earlier result [38]. Consider the classical $[3, 1, 3]_4$ quaternary code with parity check matrix

$$H_4 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \qquad (41)$$

Then

$$H = \gamma(\widetilde{H}_4) = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right). \qquad (42)$$

Following the proof of Theorem 1, we have

$$\begin{array}{rcl} \mathbf{u}_1 = & (1 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 0) \\ \mathbf{u}_2 = & (0 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 0) \\ \mathbf{u}_3 = & (1 \;\; 1 \;\; 1 \;\; 0 \;\; 0 \;\; 0) \\ \mathbf{v}_1 = & (0 \;\; 0 \;\; 0 \;\; 1 \;\; 0 \;\; 1) \\ \mathbf{v}_2 = & (1 \;\; 0 \;\; 1 \;\; 0 \;\; 0 \;\; 0) \\ \mathbf{v}_3 = & (0 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 1), \end{array} \tag{43}$$

and the hyperbolic pairs $(\mathbf{u}_1, \mathbf{v}_1)$ and $(\mathbf{u}_2, \mathbf{v}_2)$ span the rowspace of H. The simultaneous $+1$ eigenstate of the commuting operators $N_{\mathbf{u}_i}$, $i = 1, 2, 3$, is

$$|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle).$$

Then

$$\begin{aligned} |\widetilde{000}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) \\ |\widetilde{001}\rangle &= N_{\mathbf{v}_1}|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(|101\rangle + |011\rangle) \\ |\widetilde{010}\rangle &= N_{\mathbf{v}_2}|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(|101\rangle - |011\rangle) \\ |\widetilde{011}\rangle &= N_{\mathbf{v}_1+\mathbf{v}_2}|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(-|101\rangle + |011\rangle) \\ |\widetilde{100}\rangle &= N_{\mathbf{v}_3}|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(|111\rangle + |001\rangle) \\ |\widetilde{101}\rangle &= N_{\mathbf{v}_1+\mathbf{v}_3}|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |100\rangle) \\ |\widetilde{110}\rangle &= N_{\mathbf{v}_2+\mathbf{v}_3}|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(-|111\rangle + |001\rangle) \\ |\widetilde{111}\rangle &= N_{\mathbf{v}_1+\mathbf{v}_2+\mathbf{v}_3}|\widetilde{000}\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |100\rangle). \end{aligned}$$

The encoding unitary U_Υ is therefore

$$U_\Upsilon = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \end{pmatrix}. \tag{44}$$

The logical 0 and 1 codewords are

$$\begin{aligned} |0_L\rangle &= U_\Upsilon|0\rangle|\Phi_+\rangle^{\otimes 2} \\ &= \frac{1}{2}\Big(|\widetilde{000}\rangle|00\rangle + |\widetilde{001}\rangle|01\rangle + |\widetilde{010}\rangle|10\rangle + |\widetilde{011}\rangle|11\rangle\Big) \\ |1_L\rangle &= U_\Upsilon|1\rangle|\Phi_+\rangle^{\otimes 2} \\ &= \frac{1}{2}\Big(|\widetilde{100}\rangle|00\rangle + |\widetilde{101}\rangle|01\rangle + |\widetilde{110}\rangle|10\rangle + |\widetilde{111}\rangle|11\rangle\Big). \end{aligned}$$

Bowen's code [38] can be obtained by applying the following unitary to the codewords given above

$$U_B = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 \end{pmatrix}.$$

IX. Table of codes

In [8] a table of best known QEC codes was given. Below we show an updated table which includes EAQEC codes.

The entries with an asterisk mark the improvements over the table from [8]. All these are obtained from Proposition 3.1. The corresponding classical quaternary code is available online at `http://www.win.tue.nl/~aeb/voorlincod.html`.

The general methods from [8] for constructing new codes from old also apply here. Moreover, new constructions are possible since the self-orthogonality condition is lifted. An example is given by the following theorem.

Theorem 12: a) Suppose an $[[n, k, d; c]]$ code exists, then an $[[n + 1, k - 1, d'; c']]$ code exists for some c' and $d' \geq d$; b) Suppose a non-degenerate $[[n, k, d; c]]$ code exists, then an $[[n - 1, k + 1, d - 1; c']]$ code exists for some c'.

Proof: a) Recall that the net yield is $\hat{k} = k - c$. Let H be the $(n - \hat{k} \times 2n)$ parity check matrix of the $[[n, k, d; c]]$ code. The parity check matrix of the new $[[n + 1, \hat{k} - 1, d'; c']]$ is then

$$H' = \left(\begin{array}{cc|cc} 0 \cdots 0 & 0 & 1 \cdots 1 & 1 \\ 1 \cdots 1 & 1 & 0 \cdots 0 & 0 \\ & 0 & & 0 \\ H_Z & \vdots & H_X & \vdots \\ & 0 & & 0 \end{array}\right). \tag{45}$$

This corresponds to the classical construction of adding a parity check at the end of the codeword [44]. The additional rows ensure that errors involving the last qubit are detected. Sometimes the distance actually increases: for instance, the $[[8, 0, 4]]$ is obtained from the $[[7, 1, 3]]$ code in this way.

b) We mimic the classical "puncturing" method [44]. Let C be the $(n+\hat{k})$-dimensional subspace of $(\mathbb{Z}_2)^{2n}$ corresponding to the $[[n, k, d; c]]$ EAQEC code. Puncturing C by deleting the first Z and X coordinate, we obtain a new "code" C' which is an $(n+\hat{k})$-dimensional subspace of $(\mathbb{Z}_2)^{2(n-1)}$. This corresponds to an $[[n-1, k+1, d-1; c']]$ EAQEC code, as the minimum distance between the "codewords" of C decreases by at most 1. ∎

X. Discussion

Motivated by recent developments in quantum Shannon theory, we have introduced a generalization of the stabilizer formalism to the setting in which the encoder Alice and decoder Bob pre-share entanglement (EAQEC codes) [27]. We have traced the male side of family tree of quantum

$n\backslash\hat{k}=k-c$	0	1	2	3	4	5	6	7	8	9	10
3	2	2^*	1	1							
4	3^*	2	2	1	1						
5	3	3	2	2^*	1	1					
6	4	3	2	2	2	1	1				
7	3	3	2	2	2	2^*	1	1			
8	4	3	3	3	2	2	2	1	1		
9	4	4^*	3	3	2	2	2	2^*	1	1	
10	5^*	4	4	3	3	2	2	2	2	1	1

TABLE I
TABLE OF CODES FOR CODE LENGTH UP TO 10

Shannon theory, from EAQEC codes (corresponding to the father protocol) to catalytic quantum codes (corresponding to the quantum capacity) and EACEC codes (corresponding to the classical EA-capacity). Moreover, EACEC codes can be made coherent, providing an alternative to the EAQEC construction from Section III. The most obvious question is whether we can do the same for the female side of the family tree [19]. Preliminary results [46] give a positive answer to this question: entanglement distillation protocols assisted by quantum and classical communication can be constructed based on non-orthogonal symplectic codes.

There are two practical advantages of EAQEC codes over standard QEC codes:

1) They are much easier to construct from classical codes because self-orthogonality is not required. In standard QEC codes, this would not work, because codes that are not self-orthogonal would give rise to noncommuting stabilizer generators. But we resolve this by using pre-shared entanglement (therefore adding extra Pauli operators on Bob's side) to make all the generators commute. This allows us to import the classical theory of error correction wholesale, including capacity-achieving modern codes [45], [49], [28], [29], [30], [31], [32], [33]. The attraction of these modern codes comes from the existence of efficient decoding algorithms that provide excellent trade-off between decoding complexity and decoding performance. In fact, these decoding algorithms, such as the sum-product algorithm, can be modified to decode the error syndromes effectively [47], [31], [48], [30]. The main problem in using these iterative decoding algorithms on quantum low-density parity-check (LDPC) codes comes from those shortest 4-cycles in the Tanner graph that are inevitably introduced because of the self-orthogonality constraint. However, we have demonstrated recently that by allowing entanglement assistance, those 4-cycles can be eliminated completely, and the performance of the iterative decoding improves dramatically in numerical simulations [28] (and subsequently in [31], [30], [33], [32]). We plan to further examine the performance of quantum LDPC codes and turbo codes in terms of the catalyst size for EAQEC codes.
2) The entanglement used in the protocol is a strictly weaker resource than quantum communication. Thus comparing the *net yield*, $k-c$, of $[[n,k,d;c]]$ EAQEC codes to $[[n,k,d;0]]$ QEC codes is not being entirely fair to former. Furthermore, the pre-shared entanglement can be obtained from a two-way entanglement distillation protocol that achieves higher rates than one-way schemes. In this sense, a large value of the catalyst c is advantageous, as it implies a higher qubit channel yield.

In the construction of EAQEC codes, the pre-shared ebits are assumed to be noiseless. However, recent investigation shows that EAQEC codes can be robust to noise on these pre-shared ebits [30], [35], [50]. Based on the entanglement-assisted stabilizer formalism proposed in this paper, we also can construct more general QEC codes that allow us to simultaneously transmit both classical and quantum messages [51], [52].

If one is interested in applications to fault-tolerant quantum computation, where the resource of entanglement between the sender and receiver is meaningless, high values of c are unwelcome because they require a long seed QEC code. We expect this obstacle to be overcome by bootstrapping. Another fruitful line of investigation connects to quantum cryptography. Quantum cryptographic protocols, such as BB84, are intimately related to CSS QEC codes. In [53] it is shown that EAQEC analogues of CSS codes give rise to key expansion protocols which do not rely on the existence of long self-orthogonal codes. This was demonstrated for a family of codes in [54].

APPENDIX A
PROOF OF THEOREM 1

Proof: Pick an arbitrary basis $\{\mathbf{w}_1,\ldots,\mathbf{w}_m\}$ for V and extend it to a basis $\{\mathbf{w}_1,\ldots,\mathbf{w}_{2n}\}$ for $(\mathbb{Z}_2)^{2n}$. The procedure consists of n rounds. In each round a new hyperbolic pair $(\mathbf{u}_i,\mathbf{v}_i)$ is generated; the index i is added to the set $\mathcal{U}$ ($\mathcal{V}$) if $\mathbf{u}_i\in V$ ($\mathbf{v}_i\in V$).

Initially set $i=1$, $m'=m$, and $\mathcal{U}=\mathcal{V}=\emptyset$. The i-th ($i>1$) round reads as follows.

1) We start with vectors $\mathbf{w}_1,\ldots,\mathbf{w}_{2(n-i+1)}$, and $\mathbf{u}_1,\ldots\mathbf{u}_{i-1},\mathbf{v}_1,\ldots\mathbf{v}_{i-1}$, such that
   a) $\mathbf{w}_1,\ldots,\mathbf{w}_{2(n-i+1)}$, $\mathbf{u}_1,\ldots\mathbf{u}_{i-1},\mathbf{v}_1,\ldots\mathbf{v}_{i-1}$ is a basis for $(\mathbb{Z}_2)^{2n}$,
   b) each of $\mathbf{u}_1,\ldots\mathbf{u}_{i-1},\mathbf{v}_1,\ldots\mathbf{v}_{i-1}$ has vanishing symplectic product with each of $\mathbf{w}_1,\ldots,\mathbf{w}_{2(n-i+1)}$,
   c) $V=\mathrm{span}\{\mathbf{w}_j:1\le j\le m'\}\oplus\mathrm{span}\{\mathbf{u}_j:j\in\mathcal{U}\}\oplus\mathrm{span}\{\mathbf{v}_j:j\in\mathcal{V}\}$.
2) Define $\mathbf{u}_i=\mathbf{w}_1$. If $m'\ge 1$ then and add i to $\mathcal{U}$. Let $j\ge 2$ be the smallest index for which $\mathbf{w}_1\odot\mathbf{w}_j^T=1$.

Such a j exists because of (a), (b) and the fact that there exists a $\mathbf{w} \in (\mathbb{Z}_2)^{2n}$ such that $\mathbf{u}_i \odot \mathbf{w}^T = 1$.
Set $\mathbf{v}_i = \mathbf{w}_j$.

3) If $j \leq m'$:
This means that there is a hyperbolic partner of $\mathbf{u}_i$ in V. Add i to $\mathcal{V}$; swap $\mathbf{w}_j$ with $\mathbf{w}_2$; for $k = 3, \ldots, 2(n-i+1)$ perform

$$\mathbf{w}'_{k-2} := \mathbf{w}_k - (\mathbf{v}_i \odot \mathbf{w}_k^T)\mathbf{u}_i - (\mathbf{u}_i \odot \mathbf{w}_k^T)\mathbf{v}_i,$$

so that

$$\mathbf{w}'_{k-2} \odot \mathbf{u}_i^T = \mathbf{w}'_{k-2} \odot \mathbf{v}_i^T = 0; \tag{46}$$

set $m' := m' - 2$.
If $j > m'$:
This means that there is no hyperbolic partner of $\mathbf{u}_i$ in V. Swap $\mathbf{w}_j$ with $\mathbf{w}_{2(n-i+1)}$; for $k = 2, \ldots, 2(n-i)+1$ perform

$$\mathbf{w}'_{k-1} := \mathbf{w}_k - (\mathbf{v}_i \odot \mathbf{w}_k^T)\mathbf{u}_i - (\mathbf{u}_i \odot \mathbf{w}_k^T)\mathbf{v}_i,$$

so that

$$\mathbf{w}'_{k-1} \odot \mathbf{u}_i^T = \mathbf{w}'_{k-1} \odot \mathbf{v}_i^T = 0; \tag{47}$$

if $m' \geq 1$ then set $m' := m' - 1$.

4) Let $\mathbf{w}_k := \mathbf{w}'_k$ for $1 \leq k \leq 2(n-i)$. We need to show that the conditions from item 1 are satisfied for the next round ($i := i+1$). Condition (a) holds because $\{\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}'_1, \ldots \mathbf{w}'_{2(n-i)}\}$ are related to the old $\{\mathbf{w}_1, \ldots \mathbf{w}_{2(n-i+1)}\}$ by an invertible linear transformation. Condition (b) follows from (46) and (47). Regarding condition (c), if $m' = 0$ then it holds because $\mathcal{U}$ and $\mathcal{V}$ did not change from the previous round. Otherwise, consider the two cases in item 3. If $j \leq m'$ then $\{\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}'_1, \ldots \mathbf{w}'_{m'-2}\}$ are related to the old $\{\mathbf{w}_1, \ldots \mathbf{w}_{m'}\}$ by an invertible linear transformation. If $j > m'$ then $\{\mathbf{u}_i, \mathbf{w}'_1, \ldots \mathbf{w}'_{m'-1}\}$ are related to the old $\{\mathbf{w}_1, \ldots \mathbf{w}_{m'}\}$ by an invertible linear transformation (the $(\mathbf{u}_i \odot \mathbf{w}_k^T)\mathbf{v}_i$ terms vanish for $1 \leq k \leq m'$ because there is no hyperbolic partner of $\mathbf{u}_i$ in V).

$0 \leq m' \leq 2(n-i)$ at the end of the ith round. Thus $m' = 0$ after n rounds and hence $V = \mathrm{span}\{\mathbf{u}_j : j \in \mathcal{U}\} \oplus \mathrm{span}\{\mathbf{v}_j : j \in \mathcal{V}\}$. The theorem follows by suitably reordering the $(\mathbf{u}_j, \mathbf{v}_j)$. ∎

Appendix B
Proof of Theorem 2

Proof: Consider the standard basis $\mathbf{g}_i = (\mathbf{e}_i|\mathbf{0})$, $\mathbf{h}_i = (\mathbf{0}|\mathbf{e}_i)$. Define the unique (up to a phase factor) state $|\mathbf{0}\rangle$ on $\mathcal{H}^{\otimes n}$ to be the simultaneous $+1$ eigenstate of the commuting operators $N_{\mathbf{g}_j}$, $j = 1, \ldots, n$. Define an orthonormal basis $\{|\mathbf{b}\rangle : \mathbf{b} = b_1 \ldots b_n \in (\mathbb{Z}_2)^n\}$ for $\mathcal{H}^{\otimes n}$ by

$$|\mathbf{b}\rangle = N_{\sum_i b_i \mathbf{h}_i}|\mathbf{0}\rangle.$$

The orthonormality follows from the observation that $|\mathbf{b}\rangle$ is a simultaneous eigenstate of $N_{\mathbf{g}_j}$, $j = 1, \ldots, n$ with respective eigenvalues $(-1)^{b_j}$:

$$\begin{aligned} N_{\mathbf{g}_j}|\mathbf{b}\rangle &= N_{\mathbf{g}_j} N_{\sum_i b_i \mathbf{h}_i}|\mathbf{0}\rangle \\ &= (-1)^{b_j} N_{\sum_i b_i \mathbf{h}_i} N_{\mathbf{g}_j}|\mathbf{0}\rangle \\ &= (-1)^{b_j} N_{\sum_i b_i \mathbf{h}_i}|\mathbf{0}\rangle \\ &= (-1)^{b_j}|\mathbf{b}\rangle. \end{aligned} \tag{48}$$

The second line is an application of (2).

Define $\widetilde{\mathbf{g}}_i := \Upsilon(\mathbf{g}_i)$. We repeat the above construction for this new basis. Define the unique (up to a phase factor) state $|\widetilde{\mathbf{0}}\rangle$ to be the simultaneous $+1$ eigenstate of the commuting operators $N_{\widetilde{\mathbf{g}}_i}$, $i = 1, \ldots, n$. Define an orthonormal basis $\{|\widetilde{\mathbf{b}}\rangle\}$ by

$$|\widetilde{\mathbf{b}}\rangle = N_{\sum_i b_i \widetilde{\mathbf{h}}_i}|\widetilde{\mathbf{0}}\rangle. \tag{49}$$

Defining $\mathbf{u} = \sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i$, $\widetilde{\mathbf{u}} = \sum_i z_i \widetilde{\mathbf{g}}_i + x_i \widetilde{\mathbf{h}}_i$ and $\mathbf{x} = x_1 \ldots x_n$, we have

$$\begin{aligned} N_{\widetilde{\mathbf{u}}}|\widetilde{\mathbf{b}}\rangle &= N_{\widetilde{\mathbf{u}}} N_{\sum_i b_i \widetilde{\mathbf{h}}_i}|\widetilde{\mathbf{0}}\rangle \\ &= (-1)^{\widetilde{\mathbf{u}} \odot (\sum_i b_i \widetilde{\mathbf{h}}_i)^T} N_{\sum_i b_i \widetilde{\mathbf{h}}_i} N_{\widetilde{\mathbf{u}}}|\widetilde{\mathbf{0}}\rangle \\ &= (-1)^{\widetilde{\mathbf{u}} \odot (\sum_i b_i \widetilde{\mathbf{h}}_i)^T} e^{i\theta(\widetilde{\mathbf{u}})} N_{\sum_i b_i \widetilde{\mathbf{h}}_i} N_{\sum_i x_i \widetilde{\mathbf{h}}_i} N_{\sum_i z_i \widetilde{\mathbf{g}}_i}|\widetilde{\mathbf{0}}\rangle \\ &= (-1)^{\widetilde{\mathbf{u}} \odot (\sum_i b_i \widetilde{\mathbf{h}}_i)^T} e^{i\theta(\widetilde{\mathbf{u}})} N_{\sum_i (b_i + x_i) \widetilde{\mathbf{h}}_i}|\widetilde{\mathbf{0}}\rangle \\ &= (-1)^{\widetilde{\mathbf{u}} \odot (\sum_i b_i \widetilde{\mathbf{h}}_i)^T} e^{i\theta(\widetilde{\mathbf{u}})} \widetilde{|\mathbf{b} + \mathbf{x}\rangle} \\ &= (-1)^{\mathbf{u} \odot (\sum_i b_i \mathbf{h}_i)^T} e^{i\theta(\widetilde{\mathbf{u}})} \widetilde{|\mathbf{b} + \mathbf{x}\rangle}, \end{aligned} \tag{50}$$

where $\theta(\widetilde{\mathbf{u}})$ is a phase factor which is independent of $\mathbf{b}$. The first equality follows from (49), the second from (2), the third from (1), the fourth from the definition of $|\widetilde{\mathbf{0}}\rangle$ and the fact that $X^{\mathbf{b}} X^{\mathbf{x}} = X^{\mathbf{b}+\mathbf{x}}$, the fifth from (49), and the sixth from (9). Similarly

$$N_{\mathbf{u}}|\mathbf{b}\rangle = (-1)^{\mathbf{u} \odot (\sum_i b_i \mathbf{h}_i)^T} e^{i\varphi(\mathbf{u})}|\mathbf{b} + \mathbf{x}\rangle, \tag{51}$$

where $\varphi(\mathbf{u})$ is a is a phase factor which is independent of $\mathbf{b}$.

Define U_Υ by the change of basis

$$U_\Upsilon = \sum_{\mathbf{b}} |\widetilde{\mathbf{b}}\rangle\langle \mathbf{b}|.$$

Combining (50) and (51) gives for all $|\mathbf{b}\rangle$

$$\begin{aligned} N_{\Upsilon(\mathbf{u})} U_\Upsilon |\mathbf{b}\rangle &= (-1)^{\mathbf{u} \odot (\sum_i b_i \mathbf{h}_i)^T} e^{i\theta(\widetilde{\mathbf{u}})} U_\Upsilon |\mathbf{b} + \mathbf{x}\rangle \\ &= e^{i[\theta(\widetilde{\mathbf{u}}) - \varphi(\mathbf{u})]} U_\Upsilon N_{\mathbf{u}}|\mathbf{b}\rangle. \end{aligned} \tag{52}$$

Therefore $[N_{\Upsilon(\mathbf{u})}] = [U_\Upsilon N_{\mathbf{u}} U_\Upsilon^{-1}]$. ∎

Appendix C
Proof of Theorem 3

Proof: We may extend the map $\mathcal{D}$ to its Stinespring dilation – an isometric map $\hat{U}_{\mathrm{dec}}$ with a larger target Hilbert space $\mathcal{L}^{\otimes k} \otimes \mathcal{L}'$, such that

$$\mathcal{D} = \mathrm{Tr}_{\mathcal{L}'} \circ \hat{U}_{\mathrm{dec}}.$$

The premise of the theorem is equivalent to saying that for all $\mathbf{u} \in \mathrm{supp}(\mathcal{N})$ and all pure states $|\varphi\rangle$ in $\mathcal{H}^{\otimes n}$,

$$U_{\mathrm{dec}} N_{\mathbf{u}} U_{\mathrm{enc}}|\varphi\rangle = |\varphi\rangle \otimes |\mathbf{u}\rangle$$

for some pure state $|\mathbf{u}\rangle\langle\mathbf{u}|$ on $\mathcal{L}'$. By linearity

$$U_{\rm dec} A_i U_{\rm enc} |\varphi\rangle = |\varphi\rangle \otimes |i\rangle,$$

with the unnormalized state $|i\rangle = \sum_{\mathbf{u}} \alpha_{i,\mathbf{u}} |\mathbf{u}\rangle$. Furthermore,

$$\begin{aligned}
&(\hat{U}_{\rm dec} \circ \mathcal{N} \circ \hat{U}_{\rm enc})(|\varphi\rangle\langle\varphi|) \\
&= U_{\rm dec} \left(\sum_i A_i U_{\rm enc} |\varphi\rangle\langle\varphi| U_{\rm enc}^\dagger A_i^\dagger \right) U_{\rm dec}^\dagger \\
&= |\varphi\rangle\langle\varphi| \otimes \sum_i |i\rangle\langle i|,
\end{aligned}$$

where the second subsystem corresponds to $\mathcal{L}'$. Tracing out the latter gives

$$(\mathcal{D} \circ \mathcal{N} \circ \hat{U}_{\rm enc})(|\varphi\rangle\langle\varphi|) = |\varphi\rangle\langle\varphi|,$$

concluding the proof. ∎

ACKNOWLEDGMENT

The authors would like to thank Graeme Smith for pointing us to references [41] and [42]. TAB acknowledges financial support from NSF Grant No. CCF-0448658, and TAB and MHH both received support from NSF Grant No. ECS-0507270. ID and MHH acknowledge financial support from NSF Grant No. CCF-0524811 and NSF Grant No. CCF-0545845. MHH was also supported by the UTS Chancellors postdoctoral research fellowship and UTS Early Career Researcher Grants Scheme.

REFERENCES

[1] C. E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., vol. 27, pp. 379–423, 623–656, 1948.

[2] P. W. Shor, "Scheme for Reducing Decoherence in Quantum Computer Memory," Phys. Rev. A, vol. 52, no. 4, pp. 2493–2496, 1995.

[3] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound.," Phys. Rev. A, vol. 54, no. 3, pp. 1862–1868, 1996.

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A, vol. 54, no. 5, pp. 3824–3851, 1996.

[5] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A, vol. 55, no. 2, pp. 900–911, 1997.

[6] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error-correcting code," Phys. Rev. Lett., vol. 77, no. 1, pp. 198–201, 1996.

[7] A. M. Steane, "error-correcting codes in quantum theory," Phys. Rev. Lett., vol. 77, no. 5, pp. 793–797, 1996.

[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inform. Theory, vol. 44, no. 4, pp. 1369–1387, 1998.

[9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett., vol. 78, no. 3, pp. 405–408, 1997.

[10] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol. 54, no. 2, pp. 1098–1105, 1996.

[11] D. Gottesman, "Theory of fault-tolerant quantum computation," Phys. Rev. A, vol. 57, no. 1, pp. 127–137, 1998.

[12] J. Preskill. Lecture notes for physics 229: Quantum information and computation, 1998. http://www.theory.caltech.edu/people/preskill/ph229.

[13] M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, New York, 2000.

[14] S. Lloyd, "Capacity of the noisy quantum channel," Phys. Rev. A, vol. 55, no. 3, pp. 1613–1622, 1997.

[15] P. W. Shor. The quantum channel capacity and coherent information. MSRI workshop on quantum computation, 2002.

[16] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," IEEE Trans. Inform. Theory, vol. 51, no. 1, pp. 44–55, 2005.

[17] M. Hamada, "Information rates achievable with algebraic codes on quantum discrete memoryless channels," IEEE Trans. Inform. Theory, vol. 51, no. 12, pp. 4263–4277, 2005.

[18] C. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," IEEE Trans. Inform. Theory, vol. 48, no. 10, pp. 2637–2655, 2002.

[19] I. Devetak, A. W. Harrow, and A. Winter, "A family of quantum protocols.," Phys. Rev. Lett., vol. 93, no. 23, p. 230504, 2004.

[20] M.-H. Hsieh and M. M. Wilde, "Trading Classical Communication, Quantum Communication, and Entanglement in Quantum Shannon Theory," IEEE Trans. Inform. Theory, vol. 56, no. 9, pp. 4705–4730, 2010.

[21] N. Datta and M.-H. Hsieh, "The apex of the family tree of protocols: optimal rates and resource inequalities," New J. Phys., vol. 13, no. 9, p. 093042, 2011.

[22] C. Bennett and S. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," Phys. Rev. Lett., vol. 69, no. 20, pp. 2881–2884, 1992.

[23] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett., vol. 70, no. 13, p. 1895–1899, 1993.

[24] A. Harrow, "Coherent communication of classical messages," Phys. Rev. Lett., vol. 92, no. 9, p. 097902, 2004.

[25] I. Devetak, A. W. Harrow, and A. Winter, "A Resource Framework for Quantum Shannon Theory," IEEE Trans. Inform. Theory, vol. 54, no. 10, pp. 4587–4618, 2008.

[26] M.-H. Hsieh and M. M. Wilde, "Entanglement-Assisted Communication of Classical and Quantum Information," IEEE Trans. Inform. Theory, vol. 56, no. 9, pp. 4682–4704, 2010.

[27] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," Science, vol. 314, no. 5798, pp. 436–439, 2006.

[28] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," Phys. Rev. A, vol. 79, no. 3, p. 032340, 2009.

[29] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," Phys. Rev. A, vol. 81, no. 4, p. 042333, 2010.

[30] M. M. Wilde, M.-H. Hsieh, and Z. Babar "Entanglement-assisted quantum turbo codes," IEEE Trans. Inform. Theory, vol. 60, no. 12, pp. 1203–1222, 2014.

[31] M.-H. Hsieh, W.-T. Yen, and L.-Y. Hsu, "High Performance Entanglement-Assisted Quantum LDPC Codes Need Little Entanglement," IEEE Trans. Inform. Theory, vol. 57, no. 3, pp. 1761–1769, 2011.

[32] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D. Tonchev, "Entanglement-assisted quantum low-density parity-check codes," Phys. Rev. A, vol. 82, no. 4, p. 042338, 2010.

[33] Y. Fujiwara and V. D. Tonchev, "A Characterization of Entanglement-Assisted Quantum Low-Density Parity-Check Codes," IEEE Trans. Inform. Theory, vol. 59, no. 6, pp. 3347–3353, 2013.

[34] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Duality in Entanglement-Assisted Quantum Error Correction," IEEE Trans. Inform. Theory, vol. 59, no. 6, pp. 4020–4024, 2013.

[35] C.-Y. Lai and T. A. Brun, "Entanglement-assisted quantum error-correcting codes with imperfect ebits," Phys. Rev. A, vol. 86, no. 3, p. 032319, 2012.

[36] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," Phys. Rev. Lett., vol. 78, no. 10, pp. 722–725, 1996.

[37] K. G. H. Vollbrecht and F. Verstraete, "Interpolation of recurrence and hashing entanglement distillation protocols," Phys. Rev. A, vol. 71, no. 6, p. 062325, 2005.

[38] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," Phys. Rev. A, vol. 66, no. 5, p. 052313, 2002.

[39] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," IEEE Trans. Inform. Theory, vol. 53, no. 3, pp. 865–880, 2007.

[40] A. C. da Silva. Lectures on symplectic geometry. Springer-Verlag, Berlin, 2001.

[41] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang. Entanglement in the stablizer formalism, 2004. quant-ph/0406168.

[42] S. Bravyi, D. Fattal, and D. Gottesman, "GHZ extraction yield for multipartite stabilizer states," J. Math. Phys., vol. 47, no. 6, p. 062106, 2006.
[43] I. Devetak and A. Winter, "Distilling common randomness from bipartite quantum states," IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 3183–3196, 2004.
[44] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Elsevier, Amsterdam, 1977.
[45] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," IEEE Trans. Inform. Theory, vol. 50, no. 10, pp. 23152330, 2004.
[46] Z. Luo, "Quantum error correcting codes based on privacy amplification," arXiv:0808.1392, 2008.
[47] D. Poulin and Y. Chung, "On the Iterative Decoding of Sparse Quantum Codes," Quantum Inf Comput, vol. 8, no. 10, pp. 987–1000, 2008.
[48] E. Pelchat and D. Poulin, "Degenerate Viterbi Decoding," IEEE Trans. Inform. Theory, vol. 59, no. 6, pp. 3915–3921, 2013.
[49] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum Serial Turbo Codes," IEEE Trans. Inform. Theory, vol. 55, no. 6, pp. 2776–2798, 2009.
[50] Y. Fujiwara, "Quantum Error Correction via Less Noisy Qubits.," Phys. Rev. Lett., vol. 110, no. 17, p. 170501, 2013.
[51] M.-H. Hsieh, I. Devetak, and T. A. Brun, "General entanglement-assisted quantum error-correcting codes," Phys. Rev. A, vol. 76, no. 6, p. 062313, 2007.
[52] I. Kremsky, M.-H. Hsieh, and T. A. Brun, "Classical enhancement of quantum-error-correcting codes," Phys. Rev. A, vol. 78, no. 1, p. 012341, 2008.
[53] Z. Luo and I. Devetak, "Efficiently implementable codes for quantum key expansion," Phys. Rev. A, vol. 75, no. 1, p. 010303, 2007.
[54] K.-C. Hsu and T. A. Brun, "Family of Finite Geometry Low-Density Parity-Check Codes for Quantum Key Expansion," Phys. Rev. A, vol. 87, p. 062332, 2013.

Todd A. Brun (SM10) was born in Hannibal, Missouri, USA. He received the A.B. degree in Physics from Harvard University in Cambridge, Massachusetts in 1989, the M.S. degree in Physics from Caltech in Pasadena, California in 1991, and the Ph.D. degree in Physics from Caltech in 1994. Currently, he is Professor of Electrical Engineering at the University of Southern California in Los Angeles, California. He is the author or co-author of more than 100 scientific papers, and co-editor (with Daniel A. Lidar) of the book Quantum Error Correction, published by Cambridge University Press in 2013. He does research on quantum computation, quantum information, error correction, and other aspects of quantum theory. Prof. Brun is also a member of the American Physical Society and the American Mathematical Society. He has been an associate editor of IEEE TRANSACTIONS ON COMPUTERS, and of the Journal of Computer and Systems Sciences, and served on the editorial boards of Physical Review A and Journal of Physics A. He has served extensively as a referee for journals and conferences, and written many reviews of articles and books for Mathematical Reviews.

Min-Hsiu Hsieh received his PhD degree in electrical engineering from the University of Southern California, Los Angeles, in 2008. From 2008-2010, he was a Researcher at the ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency, Tokyo, Japan. From 2010-2012, he was a Postdoctoral Researcher at the Statistical Laboratory, the Centre for Mathematical Sciences, the University of Cambridge, UK. He is now a Senior Lecturer at the Centre for Quantum Computation & Intelligent Systems (QCIS), Faculty of Engineering and Information Technology (FEIT), University of Technology, Sydney (UTS). His scientific interests include quantum Shannon theory, entanglement theory, and quantum coding theory.