Entanglement-assisted quantum error correction with linear optics

Mark M. Wilde,* Hari Krovi, and Todd A. Brun
Communication Sciences Institute, Department of Electrical Engineering, University of Southern California, Los Angeles, California 90089, USA

(Received 2 June 2007; published 9 November 2007)

We construct a theory of continuous-variable entanglement-assisted quantum error correction. We present an example of a continuous-variable entanglement-assisted code that corrects for an arbitrary single-mode error. We also show how to implement encoding circuits using passive optical devices, homodyne measurements, feedforward classical communication, conditional displacements, and off-line squeezers.

DOI: 10.1103/PhysRevA.76.052308 PACS number(s): 03.67.Pp, 03.67.Hk, 42.50.Dv

I. INTRODUCTION

Entanglement is a critical resource for quantum information processing. Shared entanglement between a sender and receiver enables several quantum communication protocols such as teleportation [1] and superdense coding [2]. Brun, Devetak, and Hsieh exploited the resource of shared entanglement to form a general theory of quantum error-correcting codes—the entanglement-assisted stabilizer formalism [3,4].

Standard quantum error-correcting codes protect a set of qubits from decoherence by encoding the qubits in a subspace of a larger Hilbert space [5–8]. These quantum codes protect a state against a particular error set. Quantum errors in the error set then either leave the set of qubits invariant or they take the state out of the subspace into an orthogonal subspace. Measurements can diagnose which subspace the state is in without disturbing the state. One can then reverse the effect of the error by rotating the state back into the original subspace.

Calderbank *et al.* figured out clever ways of importing classical codes for use in quantum error correction [9]. These methods translate the classical code to a quantum code. The problem is that the classical codes have to satisfy a dual-containing constraint. The dual-containing constraint is equivalent to the operators in the quantum code forming a commuting set. Few classical codes satisfy the dual-containing constraint so classical theory was only somewhat useful for quantum error correction after Calderbank *et al.*'s results.

Bowen constructed an example of a quantum error-correcting code exploiting shared entanglement [10]. Brun, Devetak, and Hsieh then established the entanglement-assisted stabilizer formalism [3,4].

Entanglement-assisted codes have several key benefits. One can construct an entanglement-assisted code from an arbitrary linear classical code. The classical code need not be dual-containing because an entanglement-assisted code does not require a commuting stabilizer. We turn anticommuting elements into commuting ones by employing shared entanglement. Thus we can use the whole of classical coding theory for quantum error correction. Additionally, a source of pre-established entanglement boosts the rate of an entanglement-assisted code. The performance of an entanglement-assisted quantum code follows from that of the imported classical code so that a good classical code translates to a good quantum code. Entanglement-assisted codes can also operate in a catalytic manner for quantum computation if a few qubits are immune to noise [3,4].

Continuous-variable quantum information has become increasingly popular due to the practicality of its experimental implementation [11]. Error correction routines are necessary for proper operation of a continuous-variable quantum communications system. Braunstein [12] and Lloyd and Slotine [13] independently proposed continuous-variable quantum error-correcting codes. Braunstein's scheme has the advantage that only linear optical devices and squeezed states prepared off-line implement the encoding circuit [12,14]. The performance of the code depends solely on the performance of the off-line squeezers, beamsplitters, and photodetectors. The disadvantage of Braunstein's scheme is that small errors accumulate as the computation proceeds if the performance of squeezers and photodetectors is not sufficient to detect these small errors [15].

In this paper, we extend the entanglement-assisted stabilizer formalism to continuous-variable quantum information [11]. Figure 1 illustrates how a continuous-variable entanglement-assisted code operates. Brun, Devetak, and Hsieh constructed the entanglement-assisted stabilizer formalism in terms of a sympletic space $\mathbb{Z}_2^{2n}$ over the field $\mathbb{Z}_2$. The theory behind continuous-variable entanglement-assisted quantum error-correcting codes exploits a symplectic vector space $\mathbb{R}^{2n}$ over the field $\mathbb{R}$.

We first review the relation between symplectic spaces, unitary operators, and the canonical operators for single and multiple modes. We present two theorems that play a crucial role in constructing continuous-variable entanglement-assisted codes. We then provide a canonical code and show how a symplectic transformation relates an arbitrary code to the canonical one. Our presentation parallels the approach for qubits [4]. The performance of our codes depends solely on the level of squeezing and photodetector efficiency that is technologically feasible. We give an example of a continuous-variable entanglement-assisted quantum error-correcting code that corrects a arbitrary single-mode error.

Our entanglement-assisted quantum error-correcting codes are vulnerable to finite squeezing effects and ineffi-

*mark.wilde@usc.edu

 ©2007 The American Physical Society

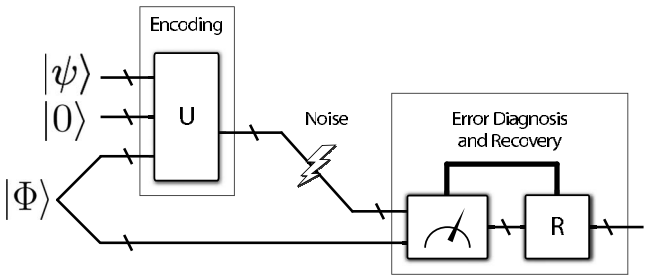

FIG. 1. The above figure demonstrates the operation of a continuous-variable entanglement-assisted code. Lines with bars through them denote multiple modes. Thin lines denote quantum information and thick lines denote classical information. Alice possesses states $|\psi\rangle$, $|0\rangle$, and half of the entangled modes $|\Phi\rangle$. Bob possesses the other half of entangled modes $|\Phi\rangle$. The unitary U encodes the multimode state $|\psi\rangle$ with the help of several position-quadrature squeezed ancillas $|0\rangle$ and entangled modes $|\Phi\rangle$. Alice sends her modes over a noisy quantum channel. The entanglement-assisted communication paradigm assumes that the noisy channel affects Alice's modes only. Bob measures all the modes to diagnose the errors and corrects them with a recovery operator R. Bob can perform these measurements with homodyne detection.

cient photodetectors for the same reasons as those given in [12]. Our scheme works well if the errors due to finite squeezing and inefficiencies in beamsplitters and photodetectors are smaller than the actual errors.

Our second contribution is an algorithm for constructing the encoding circuit using linear optics. We refer to any scheme implementing an optical circuit with passive optical elements, homodyne measurements, feedforward control, conditional displacements, and off-line squeezers as a linear-optical scheme. The algorithm exploits and extends previous techniques [16,17]. The algorithm employs a symplectic Gaussian elimination technique to decompose an arbitrary encoding circuit into a linear-optical circuit. The transmission amplitudes and phase shifts of passive beamsplitters encode all the logic rather than the interaction strength of nonlinear devices.

II. SYMPLECTIC ALGEBRA FOR CONTINUOUS VARIABLES

We first review some mathematical preliminaries. The notation we develop is useful for stating Theorems 1 and 2 precisely. Theorems 1 and 2 are relevant for constructing an entanglement-assisted quantum code and are analogous to the theorems in [3,4] for discrete variables.

We relate the n-mode phase-free Heisenberg-Weyl group $([\mathcal{W}^n],*)$ to the additive group $(\mathbb{R}^{2n},+)$. Let $X(x)$ be a single-mode position translation by x and let $Z(p)$ be a single-mode momentum kick by p where

$$X(x) \equiv \exp\{-i\pi x\hat{p}\},$$

$$Z(p) \equiv \exp\{i\pi p\hat{x}\}, \tag{1}$$

and $\hat{x}$ and $\hat{p}$ are the position-quadrature and momentum-quadrature operators, respectively. The canonical commutation relations are $[\hat{x},\hat{p}]=i$. Denote the single-mode Heisenberg-Weyl group by $\mathcal{W}$ where

$$\mathcal{W} \equiv \{X(x)Z(p)|x,p \in \mathbb{R}\}. \tag{2}$$

Let $\mathcal{W}^n$ be the set of all n-mode operators of the form $\mathbf{A} \equiv A_1 \otimes \cdots \otimes A_n$ where $A_j \in \mathcal{W}\ \forall j \in \{1,\ldots,n\}$. Define the equivalence class

$$[\mathbf{A}] \equiv \{\beta\mathbf{A}|\beta \in \mathbb{C}, |\beta| = 1\} \tag{3}$$

with representative operator having $\beta=1$. The above equivalence class is useful because global phases are not relevant in the formulation of our codes. The group operation $*$ for the above equivalence class is as follows:

$$[\mathbf{A}]*[\mathbf{B}] \equiv [A_1]*[B_1] \otimes \cdots \otimes [A_n]*[B_n] = [A_1B_1] \otimes \cdots \otimes [A_nB_n] = [\mathbf{AB}]. \tag{4}$$

The equivalence class $[\mathcal{W}^n]=\{[\mathbf{A}]:\mathbf{A} \in \mathcal{W}^n\}$ forms a commutative group $([\mathcal{W}^n],*)$. We name $([\mathcal{W}^n],*)$ the *phase-free Heisenberg-Weyl group*.

Consider the $2n$-dimensional real vector space $\mathbb{R}^{2n}$. It forms the commutative group $(\mathbb{R}^{2n},+)$ with operation + defined as vector addition. We employ the notation $\mathbf{u}=(\mathbf{p}|\mathbf{x}), \mathbf{v}=(\mathbf{p}'|\mathbf{x}')$ to represent any vectors $\mathbf{u},\mathbf{v} \in \mathbb{R}^{2n}$, respectively. Each vector $\mathbf{p}$ and $\mathbf{x}$ has elements $(p_1,\ldots,p_n)$ and $(x_1,\ldots,x_n)$, respectively, with similar representations for $\mathbf{p}'$ and $\mathbf{x}'$. The *symplectic product* $\odot$ of $\mathbf{u}$ and $\mathbf{v}$ is

$$\mathbf{u} \odot \mathbf{v} \equiv \mathbf{p}\cdot\mathbf{x}' - \mathbf{x}\cdot\mathbf{p}' = \sum_{i=1}^{n} p_i x_i' - x_i p_i', \tag{5}$$

where "$\cdot$" is the standard inner product. Define a map $\mathbf{D}:\mathbb{R}^{2n} \to \mathcal{W}^n$ as follows:

$$\mathbf{D}(\mathbf{u}) \equiv \exp\left\{ i\sqrt{\pi}\sum_{i=1}^{n} (p_i\hat{x}_i - x_i\hat{p}_i) \right\}. \tag{6}$$

Let

$$\mathbf{X}(\mathbf{x}) \equiv X(x_1) \otimes \cdots \otimes X(x_n),$$

$$\mathbf{Z}(\mathbf{p}) \equiv Z(p_1) \otimes \cdots \otimes Z(p_n), \tag{7}$$

so that $\mathbf{D}(\mathbf{p}|\mathbf{x})$ and $\mathbf{Z}(\mathbf{p})\mathbf{X}(\mathbf{x})$ belong to the same equivalence class:

$$[\mathbf{D}(\mathbf{p}|\mathbf{x})] = [\mathbf{Z}(\mathbf{p})\mathbf{X}(\mathbf{x})]. \tag{8}$$

The map $[\mathbf{D}]:\mathbb{R}^{2n} \to [\mathcal{W}^n]$ is an isomorphism

$$[\mathbf{D}(\mathbf{u}+\mathbf{v})] = [\mathbf{D}(\mathbf{u})][\mathbf{D}(\mathbf{v})], \tag{9}$$

where $\mathbf{u},\mathbf{v} \in \mathbb{R}^{2n}$. We use the Baker-Campbell-Hausdorff theorem $e^A e^B = e^B e^A e^{[A,B]}$ and the symplectic product to capture the commutation relations of any operators $\mathbf{D}(\mathbf{u})$ and $\mathbf{D}(\mathbf{v})$:

$$\mathbf{D}(\mathbf{u})\mathbf{D}(\mathbf{v}) = \exp\{i\pi(\mathbf{u}\odot\mathbf{v})\}\mathbf{D}(\mathbf{v})\mathbf{D}(\mathbf{u}). \tag{10}$$

The operators $\mathbf{D}(\mathbf{u})$ and $\mathbf{D}(\mathbf{v})$ commute if $\mathbf{u}\odot\mathbf{v}=2n$ and anticommute if $\mathbf{u}\odot\mathbf{v}=2n+1$ for any $n \in \mathbb{Z}$. The set of canonical operators $\hat{x}_i,\hat{p}_i$ for all $i \in \{1,\ldots,n\}$ have the canonical commutation relations

$$[\hat{x}_i,\hat{x}_j]=0,$$

$$[\hat{p}_i,\hat{p}_j]=0,$$

$$[\hat{x}_i,\hat{p}_j]=i\delta_{ij}.$$

Let $\mathcal{T}^n$ be the set of all linear combinations of the canonical operators:

$$\mathcal{T}^n \equiv \left\{ \sum_{i=1}^{n} \alpha_i \hat{x}_i + \beta_i \hat{p}_i : \forall\, i, \quad \alpha_i,\beta_i \in \mathbb{R} \right\}. \tag{11}$$

Define the map $\mathbf{M}:\mathbb{R}^{2n}\rightarrow\mathcal{T}^n$ as

$$\mathbf{M}(\mathbf{u}) \equiv \mathbf{u}\cdot\hat{\mathbf{R}}^n, \tag{12}$$

where $\mathbf{u}=(\mathbf{p}|\mathbf{x})\in\mathbb{R}^{2n}$,

$$\hat{\mathbf{R}}^n = [\,\hat{x}_1\cdots\hat{x}_n|\hat{p}_1\cdots\hat{p}_n]^T, \tag{13}$$

and "·" is the inner product. We can now write $\mathcal{T}^n \equiv \{\mathbf{M}(\mathbf{u}):\mathbf{u}\in\mathbb{R}^{2n}\}$. The symplectic product gives the commutation relations of elements of $\mathcal{T}^n$:

$$[\mathbf{M}(\mathbf{u}),\mathbf{M}(\mathbf{v})] = (\mathbf{u}\odot\mathbf{v})i. \tag{14}$$

The definitions given below provide terminology used in the statements of Theorems 1 and 2 and used in the construction of our continuous-variable entanglement-assisted codes.

Definition 1. A subspace V of a space W is symplectic if there is no $\mathbf{v}\in V$ such that $\forall\mathbf{u}\in V:\mathbf{u}\odot\mathbf{v}=0$.

Definition 2. A subspace V of a space W is isotropic if $\forall\mathbf{u}\in W,\mathbf{v}\in V:\mathbf{u}\odot\mathbf{v}=0$.

Definition 3. Two vectors $\mathbf{u},\mathbf{v}\in\mathbb{R}^{2n}$ form a hyperbolic pair $(\mathbf{u},\mathbf{v})$ if $\mathbf{u}\odot\mathbf{v}=1$.

Definition 4. The symplectic dual $V^{\perp}$ of a subspace V is $V^{\perp}\equiv\{\mathbf{w}:\mathbf{w}\odot\mathbf{u}=0, \quad \forall\mathbf{u}\in V\}$.

Definition 5. A symplectic matrix $\Upsilon:\mathbb{R}^{2n}\rightarrow\mathbb{R}^{2n}$ preserves the symplectic product:

$$\Upsilon\mathbf{u}\odot\Upsilon\mathbf{v}=\mathbf{u}\odot\mathbf{v}, \quad \forall\,\mathbf{u},\mathbf{v}\in\mathbb{R}^{2n}. \tag{15}$$

It satisfies the condition $\Upsilon^T\mathbf{J}\Upsilon=\mathbf{J}$ where

$$\mathbf{J}=\begin{bmatrix}\mathbf{0}_{n\times n} & \mathbf{I}_{n\times n}\\ -\mathbf{I}_{n\times n} & \mathbf{0}_{n\times n}\end{bmatrix}. \tag{16}$$

III. THEOREMS FOR ENTANGLEMENT-ASSISTED QUANTUM ERROR CORRECTION FOR CONTINUOUS-VARIABLE SYSTEMS

Theorem 1 applies to parity check matrices for our continuous-variable entanglement-assisted codes. The theorem gives an optimal way of decomposing an arbitrary subspace of $\mathbb{R}^{2n}$ into a purely isotropic subspace and a purely symplectic subspace. Thus we can decompose the rows of an arbitrary parity check matrix in this fashion. We later see that this theorem determines how much entanglement is necessary for the code.

Theorem 1. Let V be a subspace of $\mathbb{R}^{2n}$. Suppose $\dim(V)=m$. There exists a symplectic subspace $\mathrm{symp}(V)=\mathrm{span}\{\mathbf{u}_1,\ldots,\mathbf{u}_c,\mathbf{v}_1,\ldots,\mathbf{v}_c\}$ of $\mathbb{R}^{2n}$ where $\dim(\mathrm{symp}(V))=2c$. The hyperbolic pairs $(\mathbf{u}_i,\mathbf{v}_i)$ where $i=1,\ldots,c$ span $\mathrm{symp}(V)$. There exists an isotropic subspace $\mathrm{iso}(V)=\mathrm{span}\{\mathbf{u}_{c+1},\ldots,\mathbf{u}_{c+l}\}$ where $\dim(\mathrm{iso}(V))=l$. Subspace V has dimension $m=2c+l$ and is the direct sum of its isotropic and symplectic subspaces: $V=\mathrm{iso}(V)\oplus\mathrm{symp}(V)$.

A constructive proof of the above theorem is in [18]. The set of basis vectors for $\mathrm{iso}(V)$ corresponds to a commuting set of observables in both $\mathcal{W}^n$ and $\mathcal{T}^n$ using the maps $\mathbf{D}$ and $\mathbf{M}$, respectively. Each hyperbolic pair $(\mathbf{u}_i,\mathbf{v}_i)$ in $\mathrm{symp}(V)$ corresponds via $\mathbf{D}$ to a pair of observables in $\mathcal{W}^n$ that anticommute and corresponds via $\mathbf{M}$ to a pair in $\mathcal{T}^n$ with commutator $[\mathbf{M}(\mathbf{u}_i),\mathbf{M}(\mathbf{v}_i)]=i$.

Theorem 2 is useful in relating a general continuous-variable entanglement-assisted quantum error-correcting code to a canonical one (described below) by a unitary operator. The unitary operator corresponds to an encoding circuit for the code.

Theorem 2. There exists a unitary operator U_{Υ} corresponding to a symplectic matrix Υ so that the following two conditions hold $(\forall\mathbf{u}\in R^{2n})$:

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

$$\mathbf{M}(\Upsilon\mathbf{u}) = U_{\Upsilon}\mathbf{M}(\mathbf{u})U_{\Upsilon}^{-1}. \tag{17}$$

Theorem 2 is a consequence of the Stone-von Neumann theorem [19]. The unitary U_{Υ}^{-1} for the encoding circuit relates a general continuous-variable entanglement-assisted quantum error-correcting code to the canonical one.

IV. CANONICAL ENTANGLEMENT-ASSISTED QUANTUM ERROR-CORRECTING CODE

We first consider a code protecting against a canonical error set $S_0\subset\mathbb{R}^{2n}$ with errors $\mathbf{D}(\mathbf{u})$ where $\mathbf{u}\in\mathbb{R}^{2n}$. We later extend to a more general error set by applying Theorem 2.

Continuous-variable errors are equivalent to translations in position and kicks in momentum [12,15]. These errors correspond to vectors in $\mathbb{R}^{2n}$ via the inverse map $\mathbf{D}^{-1}$.

Suppose Alice wishes to protect a k-mode quantum state $|\varphi\rangle$:

$$|\varphi\rangle = \int\cdots\int dx_1\cdots dx_k\varphi(x_1,\ldots,x_k)\ \ |x_1\rangle\cdots|x_k\rangle. \tag{18}$$

Alice and Bob possess c sets of infinitely squeezed, perfectly entangled states $|\Phi\rangle^{\otimes c}$ where

$$|\Phi\rangle \equiv \left(\int dx\ \ |x\rangle|x\rangle\right)/\sqrt{\pi}.$$

The state $|\Phi\rangle$ is a zero-valued eigenstate of the relative position observable $\hat{x}_A-\hat{x}_B$ and total momentum observable $\hat{p}_A+\hat{p}_B$. Alice possesses $l=n-k-c$ ancilla registers initialized to infinitely squeezed zero-position eigenstates of the position observables $\hat{x}_{k+1},\ldots,\hat{x}_{k+l}$: $|\mathbf{0}\rangle=|0\rangle^{\otimes l}$. She encodes the state $|\varphi\rangle$ with the canonical isometric encoder U_0 as follows:

$$U_0:|\varphi\rangle|\Phi\rangle^{\otimes c}\rightarrow|\varphi\rangle|\mathbf{0}\rangle|\Phi\rangle^{\otimes c}. \tag{19}$$

The canonical code corrects the error set

$$S_0 = \left\{ \begin{array}{c} (\ \alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2),\mathbf{b},\mathbf{a}_2|\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2),\mathbf{a},\mathbf{a}_1) \\ :\mathbf{b},\mathbf{a} \in \mathbb{R}^l, \mathbf{a}_1,\mathbf{a}_2 \in \mathbb{R}^c \end{array} \right\}, \quad (20)$$

for some known functions $\alpha,\beta:\mathbb{R}^l \times \mathbb{R}^c \times \mathbb{R}^c \to \mathbb{R}^k$. Suppose an error $\mathbf{D}(\mathbf{u})$ occurs where

$$\mathbf{u} = (\ \alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2),\mathbf{b},\mathbf{a}_2|\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2),\mathbf{a},\mathbf{a}_1). \quad (21)$$

The state $|\varphi\rangle|\mathbf{0}\rangle|\Phi\rangle^{\otimes c}$ becomes (up to a global phase)

$$\mathbf{Z}(\alpha)\mathbf{X}(\beta)|\varphi\rangle \otimes |\mathbf{a}\rangle \otimes |\mathbf{a}_1,\mathbf{a}_2\rangle, \quad (22)$$

where $|\mathbf{a}\rangle = \mathbf{X}(\mathbf{a})|\mathbf{0}\rangle$ and $|\mathbf{a}_1,\mathbf{a}_2\rangle = \mathbf{X}(\mathbf{a}_1)\mathbf{Z}(\mathbf{a}_2)|\Phi\rangle^{\otimes c}$. Bob measures the position observables of the ancillas $|\mathbf{a}\rangle$ and the relative position and total momentum observables of the state $|\mathbf{a}_1,\mathbf{a}_2\rangle$. He obtains the reduced error syndrome $\mathbf{r} = (\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)$. The reduced error syndrome specifies the error up to an irrelevant value of $\mathbf{b}$ in Eq. (21). Bob reverses the error $\mathbf{u}$ by applying the map $\mathbf{D}(-\mathbf{u}')$ where

$$\mathbf{u}' = (\ \alpha(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2),\mathbf{0},\mathbf{a}_2|\beta(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2),\mathbf{a},\mathbf{a}_1). \quad (23)$$

The canonical code is degenerate because the $\mathbf{Z}(\mathbf{b})$ errors do not affect the encoded state and Bob does not need to know $\mathbf{b}$ to correct the errors.

We can describe the operation of the canonical code using binary matrix algebra. This technique gives a correspondence between the canonical code and classical coding theory. The following parity check matrix F characterizes the errors that the canonical code can correct:

$$F \equiv \left[\begin{array}{ccc|ccc} \mathbf{0}_{l\times k} & \mathbf{I}_{l\times l} & \mathbf{0}_{l\times c} & \mathbf{0}_{l\times k} & \mathbf{0}_{l\times l} & \mathbf{0}_{l\times c} \\ \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{I}_{c\times c} & \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{0}_{c\times c} \\ \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{0}_{c\times c} & \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{I}_{c\times c} \end{array} \right]. \quad (24)$$

The rows in the above matrix F correspond to observables via the map $\mathbf{M}$ in Eq. (12). Bob can measure these observables to diagnose the error. However, a problem exists. Suppose Bob naively attempts to learn the error by measuring the observables $\mathbf{M}(\mathbf{f})$ for all rows $\mathbf{f}$ in F. Bob disturbs the state because these observables do not commute. We remedy this situation later by supposing that Alice and Bob share entanglement as in the above construction in Eq. (19).

Let us define the *canonical symplectic code* C_0 corresponding to F to be all the real vectors symplectically orthogonal to the rows of F:

$$C_0 \equiv \text{rowspace}(F)^{\perp}. \quad (25)$$

Let S_0 be the set of correctable errors. All pairs of errors in S_0 obey one of the following constraints: $\forall \mathbf{u},\mathbf{u}' \in S_0$ with $\mathbf{u} \neq \mathbf{u}'$ either $\mathbf{u}-\mathbf{u}' \notin C_0$ or $\mathbf{u}-\mathbf{u}' \in \text{iso}(C_0^{\perp})$. The condition $\mathbf{u}-\mathbf{u}' \notin C_0$ states that an error is correctable if it has a unique error syndrome. The latter condition applies if any two errors have the same effect on the encoded state.

The rowspace of F is a $(2c+l)$-dimensional subspace of $\mathbb{R}^{2n}$. Therefore it decomposes as a direct sum of an isotropic and symplectic subspace according to Theorem 1. The first l rows of F are a basis for the isotropic subspace and the last $2c$ rows are a basis for the symplectic subspace.

We can remedy the problems with the parity check matrix in Eq. (24) by constructing an augmented parity check matrix F_{aug} as

$$\left[\begin{array}{ccc|ccc} \mathbf{0}_{l\times k} & \mathbf{I}_{l\times l} & \mathbf{0}_{l\times c} & \mathbf{0}_{l\times k} & \mathbf{0}_{l\times l} & \mathbf{0}_{l\times c} \\ \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{I}_{c\times c} & \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{0}_{c\times c} \\ \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{0}_{c\times c} & \mathbf{0}_{c\times k} & \mathbf{0}_{c\times l} & \mathbf{I}_{c\times c} \end{array} \right].$$

The error-correcting properties of the code are the same as before. The extra entries correspond to Bob's half of entangled modes shared with Alice. These extra modes are noiseless because they are on the receiving end of the channel. The isotropic subspace of rowspace(F) remains the same in the above construction. The symplectic subspace of rowspace(F) becomes isotropic in the higher dimensional space rowspace(F_{aug}). Each row $\mathbf{f}$ of F_{aug} corresponds to an element of the set

$$\mathcal{M}_0 \equiv \{\mathbf{M}(\mathbf{f}) : \mathbf{f} \text{ is a row of } F_{aug}\}. \quad (26)$$

Observables in $\mathcal{M}_0$ commute because rowspace(F_{aug}) is purely isotropic. Bob can then measure these observables to learn the error without disturbing the state. The *canonical codespace* $\mathcal{C}_0$ is the simultaneous zero eigenspace of operators in $\mathcal{M}_0$—the encoding in Eq. (19) satisfies this constraint. Measurement of the observables corresponding to the first l rows of F_{aug} gives Bob the error vector $\mathbf{a}$. The next c measurements give Bob the error vector $\mathbf{a}_1$ and the last c measurements give Bob the error vector $\mathbf{a}_2$. This reduced syndrome $(\mathbf{a},\mathbf{a}_1,\mathbf{a}_2)$ specifies the error up to an irrelevant value of $\mathbf{b}$. Bob can reverse the error $\mathbf{u}$ by applying the map $\mathbf{D}(-\mathbf{u}')$ with $\mathbf{u}'$ defined in Eq. (23). The number of entangled modes used in the code is

$$c = \dim(\text{iso}(\text{rowspace}(F)))/2,$$

and the number of encoded modes is

$$k = n - \dim(\text{symp}(\text{rowspace}(F))) - c.$$

Thus Alice and Bob can use the above canonical code with entanglement assistance to correct for a canonical error set.

V. GENERAL ENTANGLEMENT-ASSISTED QUANTUM ERROR-CORRECTING CODES

We now show how to construct an entanglement-assisted quantum error-correcting code from an arbitrary subspace C of $\mathbb{R}^{2n}$. We give an example of this construction as we develop the theory. Suppose that subspace C is $(2n-m)$-dimensional where $m=2c+l$ for some $c,l \geq 0$ and $c+l<n$. Think of subspace C as an arbitrary symplectic code. We can find a symplectic basis $\{\mathbf{u}_i,\mathbf{v}_i\}_{i=1}^n$ for $\mathbb{R}^{2n}$ by Theorem 1 with the following two constraints. First, it has hyperbolic pairs $(\mathbf{u}_i,\mathbf{v}_i)$ $i=1,\ldots,n$. Second, $2n-m$ vectors in $\{\mathbf{u}_i,\mathbf{v}_i\}_{i=1}^n$ correspond to a basis for C and the other m vectors are a basis for the m-dimensional subspace $C^{\perp}$. Let us define the set

$$\mathcal{R} \equiv \{\mathbf{u}_1,\ldots,\mathbf{u}_{c+l},\mathbf{v}_1,\ldots,\mathbf{v}_c\} \quad (27)$$

as a basis for the m-dimensional subspace $C^{\perp}$. Define the set

$$\mathcal{R}_0 \equiv \{\mathbf{e}_1,\ldots,\mathbf{e}_{c+l},\mathbf{e}_{n+1},\ldots,\mathbf{e}_{n+c}\} \quad (28)$$

as a basis for the canonical subspace $C_0^{\perp}$.

How do we find the symplectic basis for $\mathbb{R}^{2n}$? We can employ a symplectic Gram-Schmidt orthogonalization procedure similar to that outlined in Ref. [4]. Suppose we have an initial arbitrary set of vectors that form a basis for C. We can multiply and add the vectors together without changing the error-correcting properties of the eventual code that we formulate. These operations are "row operations." Row operations are useful for determining an alternate set of vectors that determine a basis for $C^{\perp}$. This alternate set then decomposes into purely symplectic and purely isotropic parts.

We turn to an example to highlight the above theory. Consider the following four vectors:

$$\begin{aligned}
&(1\ 0\ 1\ 0 \mid 0\ 1\ 0\ 0),\\
&(1\ 1\ 0\ 1 \mid 0\ 0\ 0\ 0),\\
&(0\ 1\ 0\ 0 \mid 1\ 1\ 1\ 0),\\
&(0\ 0\ 0\ 0 \mid 1\ 1\ 0\ 1).
\end{aligned} \tag{29}$$

Suppose they span the dual $C^{\perp}$ of an arbitrary subspace C. $C^{\perp}$ is then a four-dimensional vector space. This subspace is similar to one for a discrete-variable entanglement-assisted quantum error-correcting code [3]. We use it to develop a continuous-variable entanglement-assisted code. We perform row operations on the above set of vectors and obtain the following four vectors:

$$\begin{aligned}
\mathbf{u}_1 &= (1\ 1\ 0\ 1 \mid 0\ 0\ 0\ 0),\\
\mathbf{u}_2 &= \left(-\sqrt{\tfrac{1}{2}}\ \sqrt{2}\ -\sqrt{2}\ \sqrt{\tfrac{1}{2}} \mid \sqrt{\tfrac{1}{2}}\ -\sqrt{\tfrac{1}{2}}\ \sqrt{\tfrac{1}{2}}\ 0\right),\\
\mathbf{v}_1 &= (1\ 0\ 1\ 0 \mid 0\ 1\ 0\ 0),\\
\mathbf{v}_2 &= \left(-\sqrt{2}\ \sqrt{\tfrac{1}{2}}\ -\sqrt{\tfrac{9}{2}}\ \sqrt{\tfrac{1}{2}} \mid \sqrt{\tfrac{1}{2}}\ -\sqrt{2}\ 0\ \sqrt{\tfrac{1}{2}}\right).
\end{aligned} \tag{30}$$

The above vectors define a symplectic basis for $C^{\perp}$ and are in the set $\mathcal{R}$. The above vectors have the same symplectic relations as the following four standard basis vectors:

$$\begin{aligned}
\mathbf{e}_1 &= (1\ 0\ 0\ 0 \mid 0\ 0\ 0\ 0),\\
\mathbf{e}_2 &= (0\ 1\ 0\ 0 \mid 0\ 0\ 0\ 0),\\
\mathbf{e}_5 &= (0\ 0\ 0\ 0 \mid 1\ 0\ 0\ 0),\\
\mathbf{e}_6 &= (0\ 0\ 0\ 0 \mid 0\ 1\ 0\ 0).
\end{aligned} \tag{31}$$

The above standard basis vectors are in the set $\mathcal{R}_0$.

We return to the general theory. A symplectic matrix Υ then exists that maps the hyperbolic pairs $(\mathbf{u}_i, \mathbf{v}_i)$ to the standard hyperbolic pairs $(\mathbf{e}_i, \mathbf{e}_{n+i})$ for all i [18]. Let H and F be the matrices whose rows consist of elements of $\mathcal{R}$ and $\mathcal{R}_0$, respectively. Let H_{aug} and F_{aug} be the augmented versions of H and F, respectively. Then $H\,\Upsilon^T = F$ and $H_{\text{aug}} P \Upsilon^T P^T = F_{\text{aug}}$ where P is a permutation matrix that makes columns $n+1$ through $n+c$ be the last c columns and shifts columns $n+c+1$ through $2n+c$ left by c positions.

The four vectors in Eq. (31) determine a canonical entanglement-assisted code. We place them as row vectors in a parity check matrix F:

$$F = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right]. \tag{32}$$

The four vectors in Eq. (30) determine an entanglement-assisted code. We place them as row vectors in a parity check matrix H:

$$H = \left[\begin{array}{cccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ -\sqrt{\frac{1}{2}} & \sqrt{2} & -\sqrt{2} & \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ -\sqrt{2} & \sqrt{\frac{1}{2}} & -\sqrt{\frac{9}{2}} & \sqrt{\frac{1}{2}} & \sqrt{\frac{1}{2}} & -\sqrt{2} & 0 & \sqrt{\frac{1}{2}} \end{array}\right]. \tag{33}$$

A symplectic matrix Υ relates F to H. This symplectic matrix Υ determines the encoding circuit. We augment the above matrices F and H to matrices F_{aug} and H_{aug}, respectively. The augmented matrices F_{aug} and H_{aug} have the matrix $[-I_{2\times 2}\ 0_{2\times 2}]^T$ to the left of the vertical bar in F and H and the matrix $[0_{2\times 2}\ I_{2\times 2}]^T$ as the last columns of F and H, respectively. All the rows in the augmented parity check matrices F_{aug} and H_{aug} are then orthogonal with respect to the symplectic product and therefore correspond to a commuting set of observables via the map $\mathbf{M}$. We later confirm that this code corrects for an arbitrary single-mode error.

Our main general result is as follows. There exists a continuous-variable entanglement-assisted code with the following properties. Alice encodes her state with the operation $U_{\Upsilon}^{-1} U_0$. The set S of correctable errors obeys the following constraint:

$$\forall \mathbf{u}, \mathbf{u}' \in S\ :\ \mathbf{u} \neq \mathbf{u}',$$

$$\mathbf{u} - \mathbf{u}' \notin C \vee \mathbf{u} - \mathbf{u}' \in \text{iso}(C^{\perp}).$$

The codespace $\mathcal{C}$ is the simultaneous zero eigenspace of the ordered set:

$$\mathcal{M} \equiv \{\mathbf{M}(\mathbf{h})\ :\ \mathbf{h}\ \text{is a row of}\ H_{aug}\}. \tag{34}$$

Performing U_{Υ}, measuring the operators in $\mathcal{M}_0$ is equivalent to measuring operators in $\mathcal{M}$ followed by performing U_{Υ}. Suppose an error $\mathbf{D}(\mathbf{u})$ occurs where $\mathbf{u} \in S$. The general error set relates to the canonical set by the mapping in Theorem 2: $[U_{\Upsilon} \mathbf{D}(\mathbf{u}) U_{\Upsilon}^{-1}] = [\mathbf{D}(\Upsilon u)]$. Bob measures the reduced syndrome $\mathbf{r}$ by measuring the observables in the set $\mathcal{M}$. Bob finds the error $\mathbf{u}$ corresponding to the reduced syndrome $\mathbf{r}$ and performs $\mathbf{D}(-\mathbf{u})$ to undo the error. Figure 1 illustrates the above operations for an entanglement-assisted code.

The code corresponding to the parity check matrix in Eq. (33) corrects for an arbitrary single-mode error. Suppose that an error $D(u)$ occurs on the first mode. We set $u = (p|x)$ and

$p,x \in \mathbb{R}$ so that p is a momentum-quadrature error and x is a position-quadrature error. Then Bob measures the error syndrome to be as follows:

$$[x \;\; \sqrt{1/2}(p-x) \;\; x \;\; \sqrt{1/2}p - \sqrt{2}x].$$

Suppose the error $D(u)$ occurs on modes 2, 3, or 4. The error syndromes in respective order are then as follows:

$$[x \;\; \sqrt{2}x - \sqrt{1/2} \;\; p \;\; \sqrt{1/2}x - \sqrt{2}p],$$

$$[0 \;\; -\sqrt{2}x + \sqrt{1/2}p \;\; x \;\; -\sqrt{9/2}x],$$

$$[x \;\; \sqrt{1/2}x \;\; 0 \;\; \sqrt{1/2}(p+x)].$$

The above error syndromes are unique for any nonzero p and x. Bob can uniquely identify on which mode the error $D(u)$ occurs and correct for it.

A. Realistic performance with finitely squeezed states and inefficient homodyne detectors

The above analysis assumes that we possess infinitely squeezed states and ideal detectors. We comment briefly on the realistic performance of our codes under nonideal circumstances. Our commentary is similar to that found in Refs. [12–14].

The squeezing in both the ancilla modes and the entangled modes must make the noise from the vacuum small and the efficiency of the homodyne detectors should be close to unity. Suppose that a parameter ϵ_1 bounds the second-moment noise contributions from squeezing and homodyne detection. Suppose furthermore that the expected error scales and the length scales of the encoded wave packets are on the order of a parameter ϵ_2. Our system performs well if $\epsilon_1 \ll \epsilon_2$. The system under these circumstances behaves as a discrete system within an infinite-dimensional Hilbert space as Lloyd and Slotine originally observed [13]. Our scheme should perform well under these circumstances just as the other schemes do [12–14].

VI. LINEAR-OPTICAL ENCODING ALGORITHM

We give an algorithm for decomposing an arbitrary encoding circuit into one- and two-mode operations using linear optics. The algorithm is an alternative to the one given in [20]. The unitary U_Y^{-1} for the encoding circuit is an element of the group $\mathcal{G}_n^{Sp}$ that preserves the phase-free Heisenberg-Weyl group up to conjugation [15,21]. The symplectic group $\mathrm{Sp}(2n,\mathbb{R})$ is isomorphic to $\mathcal{G}_n^{Sp}$. Previous results show that any $\mathcal{G}_n^{Sp}$ transformation admits a decomposition in terms of linear optical elements and squeezers [20,22]. Our algorithm is a different technique for determining the encoding unitary. It uses a symplectic Gaussian elimination technique similar to a discrete-variable algorithm [17].

The Fourier transform gate, two-mode quantum nondemolition interactions, a squeezer, and a continuous-variable phase gate generate all transformations in $\mathcal{G}_n^{Sp}$. A position-quadrature squeezer $S_i(a)$ on mode i rescales the position quadrature by a with reciprocal scaling by $1/a$ in the momentum quadrature:

$$\hat{x}_i \to a\hat{x}_i, \quad \hat{p}_i \to \hat{p}_i/a.$$

A Fourier transform F_i on mode i acts as

$$\hat{x}_i \to -\hat{p}_i, \quad \hat{p}_i \to \hat{x}_i.$$

A two-mode position-quadrature nondemolition interaction $Q_{12}^X(g)$ with interaction strength g transforms the quadrature observables as

$$\hat{x}_1 \to \hat{x}_1, \quad \hat{p}_1 \to \hat{p}_1 - g\hat{p}_2,$$

$$\hat{x}_2 \to \hat{x}_2 + g\hat{x}_1, \quad \hat{p}_2 \to \hat{p}_2.$$

A two-mode momentum-quadrature nondemolition interaction $Q_{12}^P(g)$ with interaction strength g transforms the quadrature observables as

$$\hat{x}_1 \to \hat{x}_1 - g\hat{x}_2, \quad \hat{p}_1 \to \hat{p}_1,$$

$$\hat{x}_2 \to \hat{x}_2, \quad \hat{p}_2 \to \hat{p}_2 + g\hat{p}_1.$$

A position-quadrature phase gate $P^X(g)$ with interaction strength g transforms the quadrature observables as

$$\hat{x} \to \hat{x}, \quad \hat{p} \to \hat{p} + g\hat{x},$$

and a momentum-quadrature phase gate $P^P(g)$ transforms the quadrature observables as

$$\hat{x} \to \hat{x} + g\hat{p}, \quad \hat{p} \to \hat{p}.$$

Filip *et al.* implemented $S(a)$, $Q_{12}^X(g)$, and $Q_{12}^P(g)$ using linear optics [16].

We provide an implementation of the continuous-variable phase gate. Begin with two modes—we wish to perform the phase gate on mode 1. Suppose mode 2 is a position-squeezed ancilla mode. Perform a position-quadrature nondemolition interaction $Q_{12}^X(g_1)$ on modes 1 and 2:

$$\hat{x}_1 \to \hat{x}_1, \quad \hat{p}_1 \to \hat{p}_1 - g_1\hat{p}_2,$$

$$\hat{x}_2 \to \hat{x}_2 + g_1\hat{x}_1, \quad \hat{p}_2 \to \hat{p}_2.$$

Fourier transform mode 2:

$$\hat{x}_1 \to \hat{x}_1,$$

$$\hat{p}_1 - g_1\hat{p}_2 \to \hat{p}_1 - g_1\hat{p}_2,$$

$$\hat{x}_2 + g_1\hat{x}_1 \to -\hat{p}_2,$$

$$\hat{p}_2 \to \hat{x}_2 + g_1\hat{x}_1.$$

Perform a momentum-quadrature nondemolition interaction $Q_{12}^P(g_2)$ on modes 1 and 2:

$$\hat{x}_1 \to \hat{x}_1,$$

$$\hat{p}_1 - g_1\hat{p}_2 \to \hat{p}_1 - g_1\hat{p}_2 + g_2(\hat{x}_2 + g_1\hat{x}_1),$$

$$-\hat{p}_2 \to -\hat{p}_2 - g_2\hat{x}_1,$$

$$\hat{x}_2 + g_1\hat{x}_1 \to \hat{x}_2 + g_1\hat{x}_1.$$

Measure the position quadrature of mode 2 to get result x. Mode 1 collapses as

$$\hat{x}_1 \to \hat{x}_1,$$

$$\hat{p}_1 - g_1\hat{p}_2 + g_2(\hat{x}_2 + g_1\hat{x}_1) \to \hat{p}_1 + g_1 x + g_2\hat{x}_2 + 2g_2g_1\hat{x}_1.$$

Correct the momentum of mode 2 by displacing by $g_1 x$ so that

$$\hat{x}_1 \to \hat{x}_1,$$

$$\hat{p}_1 + g_1 x + g_2\hat{x}_2 + 2g_2g_1\hat{x}_1 \to \hat{p}_1 + g_2\hat{x}_2 + 2g_2g_1\hat{x}_1.$$

The Heisenberg-picture quadrature observables for mode 1 are approximately $\hat{x}_1$, $\hat{p}_1 + 2g_2g_1\hat{x}_1$ because the original quadrature $\hat{x}_2$ has position-squeezing. So we implement a continuous-variable position-quadrature phase gate $P^X(g = 2g_2g_1)$.

We use the above gates to detail a symplectic Gaussian elimination procedure. This procedure decomposes an arbitrary encoding circuit whose symplectic matrix is Υ.

(i) If $\Upsilon_{1,1}$ equals zero, permute the first mode with the second. Continue permuting modes until $\Upsilon_{1,1}$ is nonzero. Normalize $\Upsilon_{1,1}$ by simulating $S_1(\Upsilon_{1,1}^{-1})$.

(ii) Simulate $Q_{1i}^X(-\Upsilon_{i,1})$ for all $i \in \{2,\ldots,n\}$. The first column then has the form

$$[1 \;\; 0 \;\; \cdots \;\; 0 \;\; \Upsilon_{n+1,1} \;\; \Upsilon_{n+2,1} \;\; \cdots \;\; \Upsilon_{2n,1}]^T.$$

(iii) Simulate $P_1^X(-\Upsilon_{n+1,1})$ followed by F_1.

(iv) Simulate $Q_{1i}^P(-\Upsilon_{j,1})$ for all $i \in \{2,\ldots,n\}$ and $j = i+n$. Perform F_1^{-1}. The first column has the form $[1 \;\; 0 \;\; \cdots \;\; 0]^T$.

(v) Name the new matrix Υ'. Proceed to decouple column $n+1$ of Υ'. Matrix element $\Upsilon_{1,1} = 1$ because Υ' is symplectic. Simulate $Q_{1i}^P(-\Upsilon_{i+j,n+1})$ for all $i \in \{2,\ldots,n\}$ and $j = i+n$.

(vi) Simulate $P_1^P(-\Upsilon_{1,n+1})$. Perform F_1^{-1}.

(vii) Simulate $Q_{1i}^X(-\Upsilon_{i,1})$ for all $i \in \{2,\ldots,n\}$. Perform F_1.

The first round of the algorithm is complete and the new matrix Υ'' has its first row and column equal to $\mathbf{e}_1$, its $(n+1)^{st}$ row and column equal to $\mathbf{e}_{n+1}$, and all other entries equal to the corresponding entries in Υ. The remaining rounds of the algorithm consist of applying the same procedure to the submatrix formed from rows and columns $2,\ldots n, n+2,\ldots,2n$ of Υ. All of the operations in the algorithm consist of one- and two-mode operations implementable with linear optics. The encoding circuit is the inverse of all the operations put in reverse order.

VII. CONCLUSION

We have constructed a general theory of entanglement-assisted error correction for continuous-variable quantum information. The theory of continuous-variable quantum error correction broadens when Alice and Bob share a set of entangled modes. They begin with a set of noncommuting observables that have good error-correcting properties. They then employ shared entanglement to resolve the anticommutativity in the original observables.

Our codes suffer from the same vulnerabilities as Braunstein's earlier codes for continuous variables [12]. The theory should be useful as experimentalists improve the quality of squeezing and homodyne detection technology. Our example of a continuous-variable entanglement-assisted code requires two entangled modes and corrects for an arbitrary single-mode error.

We also provided a way to construct encoding circuits using passive optical elements, homodyne measurements, feedforward control, conditional displacements, and off-line squeezers. The algorithm decomposes the encoding circuit in terms of a polynomial number of gates. The algorithm requires a large number of squeezers to implement an encoding circuit. But this scheme for encoding should become feasible as technology improves.

ACKNOWLEDGMENTS

The authors thank Igor Devetak for useful discussions and Min-Hsiu Hsieh for the MATLAB code. M.M.W. acknowledges support from NSF Grants No. CCF-0545845 and No. CCF-0448658, and T.A.B. and H.K. acknowledge support from NSF Grant No. CCF-0448658.

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] T. A. Brun, I. Devetak, and M.-H. Hsieh, Science **314**, 436 (2006).
[4] T. A. Brun, I. Devetak, and M.-H. Hsieh, e-print arXiv:quant-ph/0608027 (2006).
[5] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[6] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[7] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[8] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[9] A. Calderbank, E. Rains, P. Shor, and N. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[10] G. Bowen, Phys. Rev. A **66**, 052313 (2002).
[11] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[12] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
[13] S. Lloyd and Jean-Jacques E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).
[14] S. L. Braunstein, Nature (London) **394**, 47 (1998).
[15] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).
[16] R. Filip, P. Marek, and U. L. Andersen, Phys. Rev. A **71**, 042308 (2005).

[17] E. Hostens, J. Dehaene, and B. DeMoor, Phys. Rev. A **71**, 042315 (2005).
[18] A. C. da Silva, *Lectures on Symplectic Geometry* (Springer, Berlin, 2001).
[19] J. Eisert and M. B. Plenio, Int. J. Quantum Inf. **1**, 479 (2003).
[20] S. L. Braunstein, Phys. Rev. A **71**, 055801 (2005).
[21] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88**, 097904 (2002).
[22] S. D. Bartlett and B. C. Sanders, Phys. Rev. A **65**, 042304 (2002).