Encoding a qubit in an oscillator

Daniel Gottesman,[1,2,*] Alexei Kitaev,[1,†] and John Preskill[3,‡]
[1]*Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052*
[2]*Computer Science Division, EECS, University of California, Berkeley, California 94720*
[3]*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125*
(Received 9 August 2000; published 11 June 2001)

Quantum error-correcting codes are constructed that embed a finite-dimensional code space in the infinite-dimensional Hilbert space of a system described by continuous quantum variables. These codes exploit the noncommutative geometry of phase space to protect against errors that shift the values of the canonical variables q and p. In the setting of quantum optics, fault-tolerant universal quantum computation can be executed on the protected code subspace using linear optical operations, squeezing, homodyne detection, and photon counting; however, nonlinear mode coupling is required for the preparation of the encoded states. Finite-dimensional versions of these codes can be constructed that protect encoded quantum information against shifts in the amplitude or phase of a d-state system. Continuous-variable codes can be invoked to establish lower bounds on the quantum capacity of Gaussian quantum channels.

DOI: 10.1103/PhysRevA.64.012310 PACS number(s): 03.67.Lx

I. INTRODUCTION

Classical information can be carried by either a discrete (digital) signal or a continuous (analog) signal. Although in principle an analog signal can be processed, digital computing is far more robust—a digital signal can be readily restandardized and protected from damage caused by the gradual accumulation of small errors.

Quantum information can also be carried by either a discrete (finite-dimensional) system, such as a two-level atom or an electron spin, or by a continuous (infinite-dimensional) system, such as to a harmonic oscillator or a rotor. Even in the finite-dimensional case, quantum information is in a certain sense continuous — a state is a vector in a Hilbert space that can point in any direction. Nevertheless, we have known for nearly five years that cleverly encoded quantum states can be restandardized and protected from the gradual accumulation of small errors, or from the destructive effects of decoherence due to uncontrolled interactions with the environment [1,2].

One is tempted to wonder whether we can go still further and protect the quantum state of a system described by *continuous quantum variables*. Probably this is too much to hope for, since even the problem of protecting analog classical information seems to pose insuperable difficulties.

In this paper we achieve a more modest goal: we describe quantum error-correcting codes that protect a state of a *finite-dimensional* quantum system (or ''qudit'') that is encoded in an infinite-dimensional system. These codes may be useful for implementing quantum computation and quantum communication protocols that use harmonic oscillators or rotors that are experimentally accessible.

We also explain how encoded quantum states can be processed fault tolerantly. Once encoded states have been prepared, a universal set of fault-tolerant quantum gates can be implemented using, in the language of quantum optics, linear optical operations, squeezing, homodyne detection, and photon counting. However, for preparation of the encoded states, nonlinear couplings must be invoked.

Our continuous-variable quantum error-correcting codes are effective in protecting against sufficiently weak diffusive phenomena that cause the position and momentum of an oscillator to drift, or against losses that cause the amplitude of an oscillator to decay. By concatenating with conventional finite-dimensional quantum codes, we can also provide protection against errors that heavily damage a (sufficiently small) subset of all the oscillators in a code block. A different scheme for realizing robust and efficient quantum computation based on linear optics has been recently proposed by Knill, Laflamme, and Milburn [3,4].

We begin in Sec. II by describing codes that embed an n-state quantum system in a larger d-state system, and that protect the encoded quantum information against shifts in the amplitude or phase of the d-state system. A realization of this coding scheme based on a charged particle in a magnetic field is discussed in Sec. III. Our continuous-variable codes are obtained in Sec. IV by considering a $d\rightarrow\infty$ limit. Formally, the code states of the continuous-variable codes are nonnormalizable states, infinitely squeezed in both position and momentum; in Sec. V we describe the consequences of using more realistic approximate code states that are finitely squeezed. In Sec. VI we outline the theory of more general continuous-variable codes based on lattice sphere packings in higher dimensional phase space.

We discuss in Sec. VII how continuous-variable codes protect against quantum diffusion, amplitude damping, and unitary errors. In Sec. VIII we establish a lower bound on the quantum capacity of the Gaussian quantum channel.

We then proceed to develop schemes for fault-tolerant manipulation of encoded quantum information, starting in Sec. IX with a discussion of the symplectic operations that can [3]be implemented with linear optics and squeezing. In Sec. X we discuss the measurement of the error syndrome

*Email address: gottesma@eecs.berkeley.edu
†Email address: kitaev@microsoft.com
‡Email address: preskill@theory.caltech.edu

and error recovery, which can be achieved with symplectic operations and homodyne detection. Completion of the fault-tolerant universal gate set by means of photon counting is described in Sec. XI, and the preparation of encoded states is explained in Sec. XII. Finally, Sec. XIII contains some further remarks about the physical realization of our coding schemes, and Sec. XIV contains concluding comments.

II. SHIFT-RESISTANT QUANTUM CODES

An unusual feature of our codes is that they are designed to protect against a different type of error than has been considered in previous discussions of quantum coding. This distinction is more easily explained if we first consider not the case of a continuous quantum variable, but instead the (also interesting) case of a ''qudit,'' a d-dimensional quantum system. Quantum codes can be constructed that encode k protected qudits in a block of N qudits, so that the encoded qudits can be perfectly recovered if up to t qudits are damaged, irrespective of the nature of the damage [5–8]. Error recovery will be effective if errors that act on many qudits at once are rare. More precisely, a general error superoperator acting on N qudits can be expanded in terms of a basis of operators, each of definite ''weight'' (the number of qudits on which the operator acts nontrivially). Encoded information is well protected if the error superoperator has nearly all its support on operators of weight t or less.

But consider instead a different situation, in which the amplitude for an error to occur on each qudit is not small, but the errors are of a restricted type. The possible errors acting on a single qudit can be expanded in terms of a unitary operator basis with d^2 elements, the ''Pauli operators:''

$$X^a Z^b, \quad a,b=0,1,2,\ldots,d-1. \tag{1}$$

Here X and Z are generalizations of the Pauli matrices σ_x and σ_z, which act in a particular basis $\{|j\rangle, j=0,1,2,\ldots,d-1\}$ according to

$$X:|j\rangle \rightarrow |j+1 \pmod d\rangle,$$
$$Z:|j\rangle \rightarrow \omega^j |j\rangle, \tag{2}$$

where $\omega = \exp(2\pi i/d)$. Note that it follows that

$$ZX = \omega XZ. \tag{3}$$

For N qudits, there is a unitary operator basis with d^{2N} elements consisting of all tensor products of single-qudit Pauli operators.

We will now imagine that errors with $|a|,|b|$ small compared to d are common, but errors with large $|a|$ and $|b|$ are rare. This type of error model could be expected to apply in the case of a continuous quantum variable, which is formally the $d\rightarrow\infty$ limit of a qudit. For example, decoherence causes the position q and momentum p of a particle to diffuse with some nonzero diffusion constant. In any finite time interval q and p will drift by some amount that may be small, but is certainly not zero. How can we protect encoded quantum information under these conditions?

Fortunately, the general ''stabilizer'' framework [9,10] for constructing quantum codes can be adapted to this setting. In this framework, one divides the elements of a unitary operator basis into two disjoint and exhaustive classes: the set $\mathcal{E}$ of ''likely errors'' that we want to protect against, and the rest; the ''unlikely errors.'' A code subspace is constructed as the simultaneous eigenspace of a set of commuting ''stabilizer generators,'' that generate an Abelian group, the ''code stabilizer.'' The code can reverse errors in the set $\mathcal{E}$ if, for each pair of errors E_a and E_b, either $E_a^\dagger E_b$ lies in the stabilizer group, or $E_a^\dagger E_b$ fails to commute with some element of the stabilizer. (In the latter case, the two errors alter the eigenvalues of the generators in distinguishable ways; in the former case they do not, but we can successfully recover from an error of type a by applying either $E_a^\dagger$ or $E_b^\dagger$.) In typical discussions of quantum coding, $\mathcal{E}$ is assumed to be the set of all tensor products of Pauli operators with weight up to t (those that act trivially on all but at most t qudits). But the same principles can be invoked to design codes that protect against errors in a set $\mathcal{E}$ with other properties.

Quantum codes for continuous variables have been described previously by Braunstein [11] and by Lloyd and Slotine [12]. For example, one code they constructed can be regarded as the continuous limit of a qudit code of the type originally introduced by Shor in the binary ($d=2$) case, an $[[N=9,k=1,2t+1=3]]$ code that protects a single qudit encoded in a block of 9 from arbitrary damage inflicted on any one of the 9. The 8 stabilizer generators of the code can be expressed as

$$Z_1Z_2^{-1}, Z_2Z_3^{-1}, Z_4Z_5^{-1}, Z_5Z_6^{-1}, Z_7Z_8^{-1}, Z_8Z_9^{-1},$$
$$(X_1X_2X_3)\cdot(X_4X_5X_6)^{-1}, (X_4X_5X_6)\cdot(X_7X_8X_9)^{-1}, \tag{4}$$

and encoded operations that commute with the stabilizer and hence act on the encoded qudit can be chosen to be

$$\overline{Z} = Z_1Z_4Z_7,$$
$$\overline{X} = X_1X_2X_3. \tag{5}$$

In the $d\rightarrow\infty$ limit, we obtain a code that is the simultaneous eigenspace of eight commuting operators acting on nine particles, which are

$$q_1-q_2, q_2-q_3, q_4-q_5, q_5-q_6, q_7-q_8, q_8-q_9,$$
$$(p_1+p_2+p_3)-(p_4+p_5+p_6),$$
$$(p_4+p_5+p_6)-(p_7+p_8+p_9). \tag{6}$$

Logical operators that act in the code space are

$$\overline{q} = q_1+q_4+q_7,$$
$$\overline{p} = p_1+p_2+p_3. \tag{7}$$

This code is designed to protect against errors in which one of the particles makes a large jump in q or p (or both), while

the others hold still. But it provides little protection against small diffusive motions of all the particles, which allow $\overline{q}$ and $\overline{p}$ to drift.

Entanglement purification protocols for continuous variable systems have also been proposed — good entangled states can be distilled from noisy entangled states via a protocol that requires two-way classical communication [13,14]. These purification protocols work well against certain sorts of errors, but their reliance on two-way classical communication makes them inadequate for accurately preserving unknown states in an imperfect quantum memory, or for robust quantum computation.

Returning to qudits, let us consider an example of a quantum code that can protect against small shifts in both amplitude and phase, but not against large shifts. It is already interesting to discuss the case of a system consisting of a single qudit, but where the dimension n of the encoded system is (of course) less than d. For example, a qudit ($n=2$) can be encoded in a system with dimension $d=18$, and protected against shifts by one unit in the amplitude or phase of the qudit; that is, against errors of the form X^aZ^b where $|a|,|b|\leqslant 1$. The stabilizer of this code is generated by the two operators

$$X^6, \quad Z^6, \tag{8}$$

and the commutation relations of the Pauli operators with these generators are

$$(X^aZ^b)\cdot X^6=\omega^{6b}X^6\cdot(X^aZ^b),$$

$$(X^aZ^b)\cdot Z^6=\overline{\omega^{6a}}Z^6\cdot(X^aZ^b). \tag{9}$$

Therefore, a Pauli operator commutes with the stabilizer only if a and b are both multiples of $3=18/6$; this property ensures that the code can correct single shifts in both amplitude and phase. Logical operators acting on the encoded qudit are

$$\overline{X}=X^3, \quad \overline{Z}=Z^3, \tag{10}$$

which evidently commute with the stabilizer and are not contained in it.

Since the code words are eigenstates of Z^6 with eigenvalue one, the only allowed values of j are multiples of three. And since there are also eigenstates of X^6 with eigenvalue one, the code words are invariant under a shift in j by six units. A basis for the two-dimensional code space is

$$|\overline{0}\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|6\rangle+|12\rangle),$$

$$|\overline{1}\rangle=\frac{1}{\sqrt{3}}(|3\rangle+|9\rangle+|15\rangle). \tag{11}$$

If an amplitude error occurs that shifts j by ± 1, the error can be diagnosed by measuring the stabilizer generator Z^6, which reveals the value of j modulo 3; the error is corrected by adjusting j to the nearest multiple of 3. Phase errors are shifts in the Fourier transformed conjugate basis, and can be corrected similarly.

This code is actually *perfect*, meaning that each possible pair of eigenvalues of the generators X^6 and Z^6 is a valid syndrome for correcting a shift. There are nine possible errors $\{X^aZ^b,|a|,|b|\leqslant 1\}$, and the Hilbert space of the qudit contains nine copies of the two-dimensional code space, one corresponding to each possible error. These ''error spaces'' just barely fit in the qudit space for $d=18=9\cdot 2$.

Similar perfect codes can be constructed that protect against larger shifts. For $d=r_1r_2n$, consider the stabilizer generators

$$X^{r_1n}, \quad Z^{r_2n}. \tag{12}$$

There is an encoded *qunit*, acted on by logical operators

$$\overline{X}=X^{r_1},$$

$$\overline{Z}=Z^{r_2}, \tag{13}$$

which evidently commute with the stabilizer and satisfy

$$\overline{ZX}=\omega^{r_1r_2}\overline{XZ}=e^{2\pi i/n}\overline{XZ}. \tag{14}$$

The commutation relations of the Pauli operators with the generators are

$$(X^aZ^b)\cdot X^{r_1n}=\omega^{r_1nb}X^{r_1n}\cdot(X^aZ^b)=e^{2\pi ib/r_2}X^{r_1n}\cdot(X^aZ^b),$$

$$(X^aZ^b)\cdot Z^{r_2n}=\overline{\omega}^{r_2na}Z^{r_2n}\cdot(X^aZ^b)=e^{-2\pi ia/r_1}Z^{r_2n}\cdot(X^aZ^b). \tag{15}$$

The phases are trivial only if a is an integer multiple of r_1 and b an integer multiple of r_2. Therefore, this code can correct all shifts with

$$|a|<\frac{r_1}{2},$$

$$|b|<\frac{r_2}{2}. \tag{16}$$

The number of possible error syndromes is $r_1r_2=d/n$, so the code is perfect.

Expressed in terms of Z eigenstates, the code words contain only values of j that are multiples of r_1 (since $Z^{r_2n}=1$), and are invariant under a shift of j by r_1n (since $X^{r_1n}=1$). Hence a basis for the n-dimensional code subspace is

$$|\overline{0}\rangle = \frac{1}{\sqrt{r_2}}(|0\rangle + |nr_1\rangle + \ldots + |(r_2-1)nr_1\rangle),$$

$$|\overline{1}\rangle = \frac{1}{\sqrt{r_2}}(|r_1\rangle + \ldots + |((r_2-1)n+1)r_1\rangle),$$

$$\vdots$$

$$|\overline{n-1}\rangle = \frac{1}{\sqrt{r_2}}(|(n-1)r_1\rangle + \ldots + |(r_2n-1)r_1\rangle). \quad (17)$$

If the states undergo an amplitude shift, the value of j modulo r_1 is determined by measuring the stabilizer generator Z^{r_2n}, and the shift can be corrected by adjusting j to the nearest multiple of r_1. The code words have a similar form in the Fourier transformed conjugate basis (the basis of X eigenstates), but with r_1 and r_2 interchanged. Therefore, amplitude shifts by less than $r_1/2$ and phase shifts by less than $r_2/2$ can be corrected.

III. A QUDIT IN A LANDAU LEVEL

A single electron in a uniform magnetic field in two dimensions provides an enlightening realization of our codes. General translations in a magnetic field are noncommuting, since an electron transported around a closed path acquires an Aharonov-Bohm phase $e^{ie\Phi}$, where Φ is the magnetic flux enclosed by the path. Two translations T and S commute only if the operator $TST^{-1}S^{-1}$ translates an electron around a path that encloses a flux $\Phi = k\Phi_0$, where $\Phi_0 = 2\pi/e$ is the flux quantum and k is an integer.

Translations commute with the Hamiltonian H, and two translations T_1 and T_2 form a maximally commuting set if they generate a lattice that has a unit cell enclosing one quantum of flux. Simultaneously diagonalizing H, T_1, and T_2, we obtain a Landau level of degenerate energy eigenstates, one state corresponding to each quantum of magnetic flux. Then T_1 and T_2^n are the stabilizer generators of a code, where $\overline{Z} = T_1^{1/n}$ and $\overline{X} = T_2$ are the logical operators on a code space of dimension n.

Suppose the system is in a periodically identified box (a torus), so that $T_1^{r_1} = (T_2^n)^{r_2} = 1$ are translations around the cycles of the torus. The number of flux quanta through the torus, and hence the degeneracy of the Landau level, is nr_1r_2. The code, then, embeds an n-dimensional system in a system of dimension $d = r_1r_2n$.

In this situation, the logical operations $\overline{X}$ and $\overline{Z}$ can be visualized as translations of the torus in two different directions; the stabilizer generator $\overline{X}^n$ is a translation by a fraction $1/r_2$ of the length of the torus in one direction, and the stabilizer generator $\overline{Z}^n$ is a translation by $1/r_1$ of the length in the other direction. Therefore, for any state in the code space, the wave function of the electron in a cell containing n flux quanta is periodically repeated altogether r_1r_2 times to fill the entire torus. Our code can be regarded as a kind of ''quantum repetition code''—identical ''copies'' of the wave function are stored in each of the r_1r_2 cells. But of course there is only one electron, so if we detect the electron in one cell its state is destroyed in all the cells.

This picture of the state encoded in a Landau level cautions us about the restrictions on the type of error model that the code can fend off successfully. If the environment strongly probes one of the cells and detects nothing, the wave function is suppressed in that cell. This causes a $\overline{X}$ error in the encoded state with a probability of about $1/2r_2$, and a $\overline{Z}$ error with a probability of about $1/2r_1$. The code is more effective if the typical errors gently deform the state in each cell, rather than strongly deforming it in one cell.

IV. CONTINUOUS VARIABLE CODES FOR A SINGLE OSCILLATOR

Formally, we can construct quantum codes for systems described by continuous quantum variables by considering the large-d limit of the shift-resistant codes described in Sec. II. We might have hoped to increase d to infinity while holding r_1/d and r_2/d fixed, maintaining the ability to correct shifts in both amplitude and phase that are a fixed fraction of the ranges of the qudit. However, since the perfect codes satisfy

$$\frac{r_1}{d} = \frac{1}{nr_2}, \quad \frac{r_2}{d} = \frac{1}{nr_1}, \quad (18)$$

this is not possible. Nonetheless, interesting codes can be obtained as the amplitude and phase of the qudit approach the position q and momentum p of a particle—we can hold fixed the size of the shifts Δq and Δp that can be corrected, as the ranges of q and p become unbounded.

Another option is to take $d \to \infty$ with $r_1/d \equiv 1/m$ fixed and $r_2 = m/n$ fixed, obtaining a *rotor* $Z = e^{i\theta}$ (or a particle in a periodically identified finite box) that can be protected against finite shifts in both the orientation θ of the rotor and its (quantized) angular momentum L. The stabilizer of this code is generated by

$$Z^{r_2n} \to e^{i\theta m},$$

$$X^{r_1n} = X^{d/r_2} \to e^{-2\pi iL(n/m)} \quad (19)$$

and the logical operations are

$$\overline{Z} = e^{i\theta m/n},$$

$$\overline{X} = e^{-2\pi iL/m}. \quad (20)$$

Since $\overline{X}$ shifts the value of θ by $2\pi/m$, and $\overline{Z}$ shifts the value of L by $m/n = r_2$, this code can correct shifts in θ with $\Delta\theta < \pi/m$ and shifts in L with $|\Delta L| < m/2n$.

Alternatively, we can consider a limit in which r_1 and r_2 both become large. We may write $r_1 = \alpha/\varepsilon$ and $r_2 = 1/n\alpha\varepsilon$, where $d = nr_1r_2 = 1/\varepsilon^2$, obtaining a code with stabilizer generators

$$Z^{r_2n} \to (e^{2\pi iq\varepsilon})^{(1/\alpha\varepsilon)} = e^{2\pi iq/\alpha},$$

$$X^{r_1 n} \to (e^{-ip\varepsilon})^{(n\alpha/\varepsilon)} = e^{-inp\alpha}, \tag{21}$$

and logical operations

$$\overline{Z} = e^{2\pi i q/n\alpha}, \quad \overline{X} = e^{-ip\alpha}, \tag{22}$$

where α is an arbitrary real number. Using the identity $e^A e^B = e^{[A,B]} e^B e^A$ (which holds if A and B commute with their commutator) and the canonical commutation relation $[q,p] = i$, we verify that

$$\overline{ZX} = \omega \overline{XZ}, \quad \omega = e^{2\pi i/n}. \tag{23}$$

Since $\overline{X}$ translates q by α and $\overline{Z}$ translates p by $2\pi/n\alpha$, the code protects against shifts with

$$|\Delta q| < \frac{\alpha}{2},$$

$$|\Delta p| < \frac{\pi}{n\alpha}. \tag{24}$$

Note that the shifts in momentum and position that the code can correct obey the condition

$$\Delta p \Delta q < \frac{\pi}{2n}\hbar. \tag{25}$$

In typical situations, errors in q and p are of comparable magnitude, and it is best to choose $\alpha = \sqrt{2\pi/n}$ so that

$$\overline{Z} = \exp\left(iq\sqrt{\frac{2\pi}{n}} \right), \quad \overline{X} = \exp\left(-ip\sqrt{\frac{2\pi}{n}} \right). \tag{26}$$

Formally, the code words are coherent superpositions of infinitely squeezed states, e.g., (up to normalization)

$$|\overline{Z} = \omega^j\rangle = \sum_{s=-\infty}^{\infty} |q = \alpha(j+ns)\rangle,$$

$$|\overline{X} = \overline{\omega}^j\rangle = \sum_{s=-\infty}^{\infty} \left| p = \frac{2\pi}{n\alpha}(j+ns) \right\rangle. \tag{27}$$

(See Fig. 1.) Of course, realistic code words will be normalizable finitely squeezed states, rather than nonnormalizable infinitely squeezed states. But squeezing in at least one of p and q is required to comfortably fulfill condition (25).

The Wigner function associated with the code word wave function $\psi^{(j)}(q) \equiv \langle q|\overline{Z} = \omega^j\rangle$ is a sum of delta functions positioned at the sites of a lattice in phase space, where three quarters of the delta functions are positive and one quarter are negative. Explicitly, we have

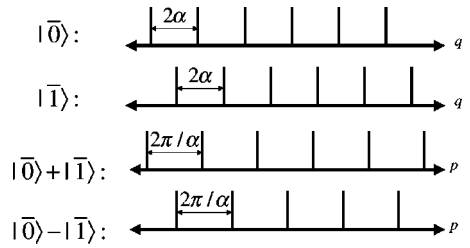

FIG. 1. Code words of the $n=2$ code. The states $|\overline{0}\rangle$, $|\overline{1}\rangle$ are superpositions of q eigenstates, periodically spaced with period 2α; the two basis states differ by a displacement in q by α. The states $(|0\rangle \pm |1\rangle)/\sqrt{2}$ are superpositions of p eigenstates, periodically spaced with period $2\pi/\alpha$; the two basis states differ by a displacement in p by π/α.

$$W^{(j)}(q,p) \equiv \frac{1}{2\pi}\int_{-\infty}^{\infty} dx e^{ipx} \psi^{(j)}(q+x/2)^* \psi^{(j)}(q-x/2)$$

$$\propto \sum_{s,t=-\infty}^{\infty} (-1)^{st} \delta\left(p - \frac{\pi}{n\alpha}s \right) \delta\left(q - \alpha j - \frac{n\alpha}{2}t \right); \tag{28}$$

the δ functions are negative on the sublattice with s,t odd. If we integrate over p, the oscillating sign causes the terms with odd t to cancel in the sum over s, and the surviving positive δ functions have support at $q = (n \times \text{integer} + j)\alpha$. If we integrate over q, the terms with odd s cancel in the sum over t, and the surviving positive δ functions have support at $p = (2\pi/n\alpha) \times$ integer. Wigner functions for the $\overline{X}$ eigenstates are similar, but with the roles of q and p interchanged.

It is also of interest to express the encoded states in terms of the basis of coherent states. Consider for example the encoded state with $\overline{X} = 1$, which is the unique simultaneous eigenstate with eigenvalue one of the operators $e^{2\pi i q/\alpha}$ and $e^{-ip\alpha}$. In fact starting with any state $|\psi\rangle$, we can construct the encoded state (up to normalization) as

$$\left(\sum_{s=-\infty}^{\infty} e^{-isp\alpha} \right) \left(\sum_{t=-\infty}^{\infty} e^{2\pi i t q/\alpha} \right) |\psi\rangle$$

$$= \sum_{s,t} \exp[i(-sp\alpha + 2\pi t q/\alpha + \pi st)] |\psi\rangle. \tag{29}$$

In particular, if we choose $|\psi\rangle$ to be the ground state $|0\rangle$ of the oscillator, then the operator $\Sigma_{s,t} \exp[i(-sp\alpha + 2\pi t q/\alpha + \pi st)]$ displaces it to a coherent state centered at the point $(q,p) = (s\alpha, 2\pi t/\alpha)$ in the quadrature plane. Thus the encoded state is an equally weighted superposition of coherent states, with centers chosen from the sites of a lattice in the quadrature plane whose unit cell has area 2π. Since the coherent states are overcomplete , the expansion is not unique; indeed, if we choose $|\psi\rangle$ to be a coherent state rather than the vacuum, then the lattice is rigidly translated, but the encoded state remains invariant.

We can envision the stabilizer of the code as a lattice of translations in phase space that preserve the code words; the lattice generated by the translations $e^{2\pi i q/\alpha}$ and $e^{-inp\alpha}$. In

fact, this lattice need not be rectangular—we can encode an n-dimensional system in the Hilbert space of a single oscillator by choosing *any* two variables Q and P that satisfy the canonical commutation relation $[Q,P]=i$, and constructing the code space as the simultaneous eigenstate of $e^{2\pi iQ}$ and e^{-inP}. The unit cell of the lattice has area $2\pi\hbar n$, in keeping with the principle that each quantum state ''occupies'' an area $2\pi\hbar$ in the phase space of a system with one continuous degree of freedom.

V. FINITE SQUEEZING

Strictly speaking, our code words are nonnormalizable states, infinitely squeezed in both q and p. In practice, we will have to work with approximate code words that will be finitely squeezed normalizable states. We need to consider how using such approximate code words will affect the probability of error.

We will replace a position eigenstate $\delta(0)$ by a normalized Gaussian of width Δ centered at the origin,

$$|\psi_0\rangle=\int_{-\infty}^{\infty}\frac{dq}{(\pi\Delta^2)^{1/4}}e^{-1/2\,q^2/\Delta^2}|q\rangle$$

$$=\int_{-\infty}^{\infty}\frac{dp}{(\pi/\Delta^2)^{1/4}}e^{-1/2\,\Delta^2p^2}|p\rangle. \tag{30}$$

A code word, formally a coherent superposition of an infinite number of δ functions, becomes a sum of Gaussians weighted by a Gaussian envelope function of width κ^{-1}; in the special case of a two-dimensional code space, the approximate code words become

$$|\tilde{0}\rangle=N_0\sum_{s=-\infty}^{\infty}e^{-1/2\,\kappa^2(2s\alpha)^2}T(2s\alpha)|\psi_0\rangle,$$

$$|\tilde{1}\rangle=N_1\sum_{s=-\infty}^{\infty}e^{-1/2\,\kappa^2[(2s+1)\alpha)]^2}T[(2s+1)\alpha]|\psi_0\rangle, \tag{31}$$

where $T(a)$ translates q by a, $N_{0,1}$ are normalization factors, and we use, e.g., $|\tilde{0}\rangle$ rather than $|\overline{0}\rangle$ to denote the approximate code word. We will assume that $\kappa\alpha$ and Δ/α are small compared to one, so that $N_0\approx N_1\approx(4\kappa^2\alpha^2/\pi)^{1/4}$; then in momentum space, the approximate code word becomes, e.g.,

$$(|\tilde{0}\rangle+|\tilde{1}\rangle)/\sqrt{2}\approx\left(\frac{\kappa^2\alpha^2}{\pi}\right)^{1/4}\int_{-\infty}^{\infty}\frac{dp}{(\pi/\Delta^2)^{1/4}}e^{-\frac{1}{2}\Delta^2p^2}$$

$$\times\sum_{s=-\infty}^{\infty}e^{-1/2\,\kappa^2(s\alpha)^2}e^{ip(\alpha s)}|p\rangle. \tag{32}$$

By applying the Poisson summation formula,

$$\sum_{m=-\infty}^{\infty}e^{-\pi a(m-b)^2}=(a)^{-1/2}\sum_{s=-\infty}^{\infty}e^{-\pi s^2/a}e^{2\pi isb}, \tag{33}$$

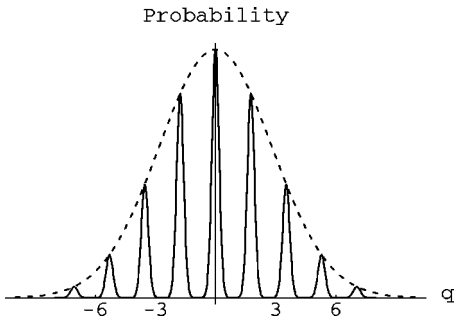

FIG. 2. Probability distribution in position space $P(q)=\frac{1}{2}|\langle q|(|\tilde{0}\rangle+|\tilde{1}\rangle)|^2$ for an approximate code word with $\Delta=\kappa=0.25$. The dashed line is the distribution's Gaussian envelope.

this approximate code word can be rewritten as

$$(|\tilde{0}\rangle+|\tilde{1}\rangle)/\sqrt{2}\approx\left(\frac{\kappa^2\alpha^2}{\pi}\right)^{1/4}\int_{-\infty}^{\infty}\frac{dp}{(\pi/\Delta^2)^{1/4}}e^{-1/2\,\Delta^2p^2}\frac{\sqrt{2\pi}}{\kappa\alpha}$$

$$\times\sum_{m=-\infty}^{\infty}\exp\left[-\frac{1}{2}\left(p-\frac{2\pi}{\alpha}m\right)^2\Big/\kappa^2\right]|p\rangle$$

$$=\int_{-\infty}^{\infty}\frac{dp}{(\pi\kappa^2)^{1/4}}\left(\frac{4\pi\Delta^2}{\alpha^2}\right)^{1/4}\sum_{m=-\infty}^{\infty}e^{-1/2\Delta^2p^2}$$

$$\times\exp\left[-\frac{1}{2}\left(p-\frac{2\pi}{\alpha}m\right)^2\Big/\kappa^2\right]|p\rangle, \tag{34}$$

again a superposition of Gaussians weighted by a Gaussian envelope. (See Fig. 2.)

The approximate code words $|\tilde{0}\rangle,|\tilde{1}\rangle$ have a small overlap if Δ is small compared to α, and κ is small compared to π/α. For estimating the error probability caused by the overlap, let's consider the special case where q and p are treated symmetrically, $\alpha=\sqrt{\pi}$ and $\kappa=\Delta$, then

$$|\langle q|\tilde{0}\rangle|^2\approx\frac{2}{\sqrt{\pi}}\sum_{s=-\infty}^{\infty}e^{-4\pi\Delta^2s^2}\exp[-(q-2s\sqrt{\pi})^2/\Delta^2] \tag{35}$$

and

$$\frac{1}{2}|\langle p|\tilde{0}\rangle+\langle p|\tilde{1}\rangle|^2\approx\frac{2}{\sqrt{\pi}}\sum_{m=-\infty}^{\infty}e^{-\Delta^2p^2}$$

$$\times\exp[-(p-2m\sqrt{\pi})^2/\Delta^2]. \tag{36}$$

To perform error recovery, we measure the value of q and p modulo $\sqrt{\pi}$ and then correct for the observed shift. In the state $|\tilde{0}\rangle$, the probability of failure is the probability that q is closer to an odd multiple of $\sqrt{\pi}$ than an even multiple, and in the state $(|\tilde{0}\rangle+|\tilde{1}\rangle)/\sqrt{2}$, the error probability is the probability that p is closer to an odd multiple of $\sqrt{\pi}$ than an even multiple. For both the amplitude and phase errors, the intrinsic error probability arising from the imperfections of the

approximate code words becomes exponentially small for small Δ. Using the asymptotic expansion of the error function,

$$\int_x^\infty dt e^{-t^2} = \left(\frac{1}{2x}\right) e^{-x^2}[1 - O(1/x^2)], \tag{37}$$

we may estimate the error probability by summing the contributions from the tails of all the Gaussians, obtaining

$$\begin{aligned} \text{Error Prob} &< \frac{2}{\sqrt{\pi}} \left(\sum_{n=-\infty}^{\infty} e^{-4\pi\Delta^2 n^2} \right) 2 \int_{\sqrt{\pi}/2}^{\infty} dq e^{-q^2/\Delta^2} \\ &\sim \frac{2}{\sqrt{\pi}} \frac{1}{2\Delta} 2\Delta \frac{\Delta}{\sqrt{\pi}} e^{-\pi/4\Delta^2} \\ &= \frac{2\Delta}{\pi} e^{-\pi/4\Delta^2}. \end{aligned} \tag{38}$$

This error probability is about 1% for $\Delta \sim .5$, and is already less than 10^{-6} for a still modest value $\Delta \sim .25$. Using finitely squeezed approximate code words does not badly compromise the error-correcting power of the code, since a gentle spreading in p and q is just the kind of error the code is intended to cope with.

The mean photon number of a finitely squeezed approximate code word is

$$\langle a^\dagger a \rangle + 1/2 = \frac{1}{2}\langle p^2 + q^2 \rangle \approx \Delta^{-2} \tag{39}$$

for small Δ. Therefore, an error probability of order 10^{-6} can be achieved with Gaussian approximate code words that have mean photon number of about $(.25)^{-2} \sim 16$.

More generally, a finitely squeezed code word $|\psi\rangle$ can be regarded as a perfect code word $|\xi\rangle$ that has undergone an error; we may write

$$|\psi\rangle = \int du dv \, \eta(u,v) e^{i(-up+vq)} |\xi\rangle, \tag{40}$$

where $\eta(u,v)$ is an error ''wave function.'' In the special case of a Gaussian finitely squeezed code word, we have

$$\eta(u,v) = \frac{1}{\sqrt{\pi\kappa\Delta}} \exp\left(-\frac{1}{2}(u^2/\Delta^2 + v^2/\kappa^2) \right), \tag{41}$$

where Δ and κ are the squeezing parameters defined above.

If $\eta(u,v)$ vanishes for $|u| > \alpha/2$ or $|v| > \pi/(n\alpha)$, then the error is correctable. In this case, the interpretation of $\eta(u,v)$ as a wave function has a precise meaning, since there is an unambiguous decomposition of a state into code word and error. Indeed, if $|\xi_1\rangle$, $|\xi_2\rangle$ are perfect code words and $|\psi_1\rangle$, $|\psi_2\rangle$ are the corresponding finitely squeezed code words with error wave functions η_1, η_2, then

$$\langle \psi_1 | \psi_2 \rangle = \langle \xi_1 | \xi_2 \rangle \langle \eta_1 | \eta_2 \rangle, \tag{42}$$

where

$$\langle \eta_1 | \eta_2 \rangle = \int du dv \, \eta_1(u,v)^* \eta_2(u,v). \tag{43}$$

VI. CONTINUOUS VARIABLE CODES FOR MANY OSCILLATORS

The continuous variable codes described in Sec. IV are based on simple lattices in the two-dimensional phase space of a single particle. We can construct more sophisticated codes from lattices in the $2N$-dimensional phase space of N particles. Then codes of higher quality can be constructed that take advantage of efficient packings of spheres in higher dimensions.

For a system of N oscillators, a tensor product of Pauli operators can be expressed in terms of the canonical variables q_i and p_i as

$$U_{\alpha\beta} = \exp\left[i\sqrt{2\pi} \left(\sum_{i=1}^{N} \alpha_i p_i + \beta_i q_i \right) \right], \tag{44}$$

where the α_i's and β_i's are real numbers. (In this setting, the Pauli operators are sometimes called ''Weyl operators.'') Two such operators commute up to a phase:

$$U_{\alpha\beta} U_{\alpha'\beta'} = e^{2\pi i[\omega(\alpha\beta,\alpha'\beta')]} U_{\alpha'\beta'} U_{\alpha\beta}, \tag{45}$$

where

$$\omega(\alpha\beta,\alpha'\beta') \equiv \alpha\cdot\beta' - \alpha'\cdot\beta \tag{46}$$

is the symplectic form. Thus two Pauli operators commute if and only if their symplectic form is an integer.

Now a general continuous variable stabilizer code is the simultaneous eigenspace of commuting Pauli operators, the code's stabilizer generators. If the continuous variable phase space is $2N$-dimensional and the code space is a finite-dimensional Hilbert space, then there must be $2N$ independent generators. The elements of the stabilizer group are in one-to-one correspondence with the points of a lattice $\mathcal{L}$ in phase space, via the relation

$$U(k_1, k_2, \ldots k_{2N}) = \exp\left[i\sqrt{2\pi} \left(\sum_{a=1}^{2N} k_a v_a \right) \right]. \tag{47}$$

Here $\{v_a, a = 1,2,\ldots,2N\}$ are the basis vectors of the lattice (each a linear combination of q's and p's), the k_a's are arbitrary integers, and $U(k_1, k_2, \ldots k_{2N})$ is the corresponding element of the stabilizer. For the stabilizer group to be Abelian, the symplectic inner product of any pair of basis vectors must be an integer; that is, the antisymmetric $2N \times 2N$ matrix

$$A_{ab} = \omega(v_a, v_b) \tag{48}$$

has integral entries. The lattice $\mathcal{L}$ has a $2N \times 2N$ generator matrix M whose rows are the basis vectors,

$$M=\begin{pmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ v_{2N} \end{pmatrix}. \tag{49}$$

In terms of M, the matrix A can be expressed as

$$A=M\omega M^T, \tag{50}$$

where ω denotes the $2N\times 2N$ matrix

$$\omega=\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}, \tag{51}$$

and I is the $N\times N$ identity matrix.

The generator matrix of a lattice is not unique. The replacement

$$M\rightarrow M'=RM \tag{52}$$

leaves the lattice unmodified, where R is an invertible integral matrix with determinant ± 1 (whose inverse is also integral). Under this replacement, the matrix A changes according to

$$A\rightarrow A'=RAR^T. \tag{53}$$

By Gaussian elimination, an R can be constructed such that the antisymmetric matrix A is transformed to

$$A'=\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}, \tag{54}$$

where D is a positive diagonal $N\times N$ matrix.

There are also Pauli operators that provide a basis for the operations acting on the code subspace—these are the Pauli operators that commute with the stabilizer but are not contained in the stabilizer. The operators that commute with the stabilizer themselves form a lattice $\mathcal{L}^\perp$ that is dual (in the symplectic form) to the stabilizer lattice. The basis vectors of this lattice can be chosen to be $\{u_b, b=1,2,3,\ldots,2N\}$ such that

$$\omega(u_a,v_b)=\delta_{ab}; \tag{55}$$

then the generator matrix

$$M^\perp=\begin{pmatrix} u_1 \\ u_2 \\ \cdot \\ \cdot \\ u_{2N} \end{pmatrix} \tag{56}$$

of $\mathcal{L}^\perp$ has the property

$$M^\perp\omega M^T=I. \tag{57}$$

It follows from Eq. (48) and Eq. (55) that the $\mathcal{L}$ basis vectors can be expanded in terms of the $\mathcal{L}^\perp$ basis vectors as

$$v_a=\sum_b A_{ab}u_b, \tag{58}$$

or

$$M=AM^\perp, \tag{59}$$

and hence that

$$\omega(u_a,u_b)=(A)^{-1}_{ba}, \tag{60}$$

or

$$M^\perp\omega(M^\perp)^T=(A^{-1})^T. \tag{61}$$

If the lattice basis vectors are chosen so that A has the standard form Eq. (54), then

$$(A^{-1})^T=\begin{pmatrix} 0 & D^{-1} \\ -D^{-1} & 0 \end{pmatrix}. \tag{62}$$

In the special case of a self-dual lattice, corresponding to a code with a one-dimensional code space, both A and A^{-1} must be integral; hence $D=D^{-1}$ and the standard form of A is

$$A=\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}=\omega. \tag{63}$$

Since the code subspace is invariant under the translations in $\mathcal{L}$, we can think of the encoded information as residing on a torus, the unit cell of $\mathcal{L}$. The encoded Pauli operators $\{\overline{X}^a\overline{Z}^b\}$ are a lattice of translations on this torus, corresponding to the coset space $\mathcal{L}^\perp/\mathcal{L}$. The number of encoded Pauli operators is the ratio of the volume of the unit cell of $\mathcal{L}$ to the volume of the unit cell of $\mathcal{L}^\perp$, namely the determinant of A, which is therefore the square of the dimension of the Hilbert space of the code. Thus the dimension of the code space is

$$n=|\mathrm{Pf}A|=\det D, \tag{64}$$

where PfA denotes the *Pfaffian*, the square root of the determinant of the antisymmetric matrix A.

The stabilizer lattice unit cell has volume $|\mathrm{Pf}A|$ in units with $h=2\pi\hbar=1$, and the unit cell of the lattice of encoded operations has volume $|\mathrm{Pf}A|^{-1}$ in these units. So the code fits an n-dimensional code space into n units of phase space volume, as expected.

Codes of the CSS type (those analogous to the binary quantum codes first constructed by Calderbank and Shor [15] and by Steane [16]) are constructed by choosing one lattice $\mathcal{L}_q$ describing stabilizer generators that are linear combinations of the q's, and another lattice $\mathcal{L}_p\subset\mathcal{L}_q^\perp$ describing stabilizer generators that are linear combinations of the p's.

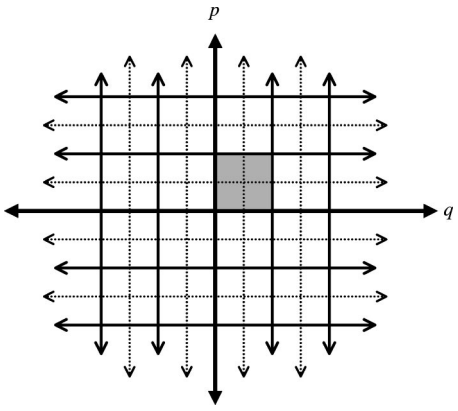

FIG. 3. The stabilizer lattice and its dual for an $n=2$ code of a single oscillator. Solid lines indicate the stabilizer lattice; solid and dotted lines together comprise the dual lattice. In units of $(2\pi\hbar)^2$, the unit cell of the stabilizer lattice (shaded) has area 2, and the unit cell of its dual has area 1/2.

(Here $\mathcal{L}_q^{\perp}$ denotes the *Euclidean* dual of the lattice $\mathcal{L}_q$.) The generator matrix of a CSS code has the form

$$M=\begin{pmatrix} M_q & 0 \\ 0 & M_p \end{pmatrix}, \tag{65}$$

where M_q and M_p are $N\times N$ matrices, and the integral matrix A has the form

$$A=\begin{pmatrix} 0 & M_q M_p^T \\ -M_p M_q^T & 0 \end{pmatrix}. \tag{66}$$

For single-oscillator codes described in Sec. IV, A is the 2×2 matrix

$$A=\begin{pmatrix} 0 & n \\ -n & 0 \end{pmatrix}, \tag{67}$$

where n is the code's dimension. For a single-oscillator CSS code, the lattice is rectangular, as shown in Fig. 3.

The closest packing of circles in two dimensions is achieved by the hexagonal lattice. The generator matrix for a hexagonally encoded qunit can be chosen to be

$$M=\begin{pmatrix} \frac{2}{\sqrt{3}}\,n \end{pmatrix}^{1/2}\begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}, \tag{68}$$

and the dual lattice is generated by

$$M^{\perp}=\frac{1}{n}\,M. \tag{69}$$

The shortest vector of the dual lattice has length $(2/n\sqrt{3})^{1/2}$, compared to length $1/\sqrt{n}$ for the square lattice. Therefore the size of the smallest uncorrectable shift is larger for the hexagonal code than for the square lattice code, by the factor $(2/\sqrt{3})^{1/2}\approx 1.07457$.

An important special class of quantum codes for many oscillators are the *concatenated codes*. In particular, we can encode a qudit in each of N oscillators using the code of Sec. IV. Then we can use a binary stabilizer code that encodes k qudits in a block of N oscillators, and protects against arbitrary errors on any t oscillators, where $2t+1$ is the binary code's distance. The concatenated codes have the important advantage that they can protect against a broader class of errors than small diffusive shifts applied to each oscillator — if most of the oscillators undergo only small shifts in p and q, but a few oscillators sustain more extensive damage, then concatenated codes still work effectively.

For example, there is a binary [[7,1,3]] quantum code, well suited to fault-tolerant processing, that encodes one logical qudit in a block of seven qudits and can protect against heavy damage on any one of the seven [2]. Given seven oscillators, we can encode a qudit in each one that is resistant to quantum diffusion, and then use the [[7,1,3]] block code to protect one logical qudit against severe damage to any one of the oscillators.

For $n\geqslant 5$, there is a [[5,1,3]] polynomial code [17], also well suited to fault-tolerant processing, encoding one qunit in a block of 5. (Actually, [[5,1,3]] quantum codes exist for $n<5$ as well [6,7], but these codes are less conducive to fault-tolerant computing.) The larger value of n increases the vulnerability of each qunit to shift errors. Hence, whether the [[7,1,3]] binary code or the [[5,1,3]] should be preferred depends on the relationship of the size of the typical shift errors to the rate of large errors.

VII. ERROR MODELS

What sort of errors can be corrected by these codes? The codes are designed to protect against errors that shift the values of the canonical variables p and q. In fact the Pauli operators are a complete basis, so the action of a general superoperator $\mathcal{E}$ acting on the input density matrix ρ of a single oscillator can be expanded in terms of such shifts, as in

$$\mathcal{E}(\rho)=\int d\alpha d\beta d\alpha' d\beta' C(\alpha,\beta;\alpha'\beta') \times e^{i(\alpha p+\beta q)}\rho e^{-i(\alpha' p+\beta' q)}. \tag{70}$$

If the support of $C(\alpha,\beta;\alpha',\beta')$ is concentrated on sufficiently small values of its arguments, then the input ρ can be recovered with high fidelity.

A useful model of decoherence is the special case of a ''Pauli channel'' in which $C(\alpha,\beta;\alpha',\beta')$ is diagonal and the superoperator can be expressed as

$$\mathcal{E}(\rho)=\int d\alpha d\beta P(\alpha,\beta) e^{i(\alpha p+\beta q)}\rho e^{-i(\alpha p+\beta q)}. \tag{71}$$

Since $\mathcal{E}$ is positive and trace preserving, we infer that $P(\alpha,\beta)\geqslant 0$ and

$$\int d\alpha d\beta P(\alpha,\beta)=1. \tag{72}$$

Thus, we may interpret $P(\alpha,\beta)$ as a probability distribution: the phase space translation

$$(q,p)\rightarrow(q-\alpha,p+\beta) \tag{73}$$

is applied with probability $P(\alpha,\beta)$.

Weak interactions between an oscillator and its environment drive a diffusive process that can be well modeled by a Pauli channel. If the environment quickly ''forgets'' what it learns about the oscillator, the evolution of the oscillator can be described by a master equation. Over a short time interval dt, the shifts applied to the oscillator may be assumed to be small, so that the Pauli operator can be expanded in powers of α and β. Suppose that the shifts are symmetrically distributed in phase space such that

$$\langle\alpha\rangle=\langle\beta\rangle=0,$$

$$\langle\alpha^2\rangle=\langle\beta^2\rangle,$$

$$\langle\alpha\beta\rangle=0, \tag{74}$$

where $\langle\cdot\rangle$ denotes the mean value determined by the probability distribution $P(\alpha,\beta)$. Suppose further that the shifts are diffusive, so that the mean square displacement increases linearly with dt; we may write

$$\langle\alpha^2\rangle=\langle\beta^2\rangle=Ddt, \tag{75}$$

where D is a diffusion constant. We then obtain

$$\begin{aligned}\rho(t+dt)&=\int d\alpha d\beta P(\alpha,\beta)e^{i(\alpha p+\beta q)}\rho e^{-i(\alpha p+\beta q)}\\&=\rho(t)+Ddt\left(p\rho p-\frac{1}{2}p^2\rho-\frac{1}{2}\rho p^2\right)\\&\quad+Ddt\left(q\rho q-\frac{1}{2}q^2\rho-\frac{1}{2}\rho q^2\right)+O(dt^{3/2}),\end{aligned} \tag{76}$$

or

$$\dot{\rho}=-\frac{D}{2}[p,[p,\rho]]-\frac{D}{2}[q,[q,\rho]]. \tag{77}$$

The interpretation of D as a diffusion constant can be confirmed by computing

$$\frac{d}{dt}\mathrm{tr}(p^2\rho)=D=\frac{d}{dt}\mathrm{tr}(q^2\rho); \tag{78}$$

the mean square values of p and q increase with time as Dt.

More generally, the master equation contains a diffusive term determined by the covariance of the distribution $P(\alpha,\beta)$, and perhaps also a nondissipative drift term determined by the mean of $P(\alpha,\beta)$. Our quantum error-correcting codes can successfully suppress decoherence caused by quantum diffusion, if the recovery operation is applied often enough; roughly, the time interval Δt between error correction steps should be small compared to the characteristic diffusion time D^{-1}.

Interactions with the environment might also damp the amplitude of the oscillator, as described by the master equation

$$\dot{\rho}=\Gamma\left(a\rho a^\dagger-\frac{1}{2}a^\dagger a\rho-\frac{1}{2}\rho a^\dagger a\right); \tag{79}$$

here $a=(q+ip)/\sqrt{2}$ is the annihilation operator and Γ is a decay rate. This master equation cannot be obtained from a Pauli channel, but as for quantum diffusion, the effects of amplitude damping over short-time intervals can be expressed in terms of small phase-space displacements.

The master equation for amplitude damping can be obtained as the $dt\rightarrow 0$ limit of the superoperator

$$\begin{aligned}\rho(t+dt)=\mathcal{E}(\rho(t))&=(\sqrt{\Gamma dt}a)\rho(t)(\sqrt{\Gamma dt}a^\dagger)\\&\quad+\left(I-\frac{\Gamma dt}{2}a^\dagger a\right)\rho(t)\left(I-\frac{\Gamma dt}{2}a^\dagger a\right).\end{aligned} \tag{80}$$

For dt small, the annihilation operator can be expanded in terms of Pauli operators as

$$\begin{aligned}\sqrt{\Gamma dt}a\approx&-\frac{i}{2}(e^{i\sqrt{\Gamma dt/2}q}-e^{-i\sqrt{\Gamma dt/2}q})\\&+\frac{1}{2}(e^{i\sqrt{\Gamma dt/2}p}-e^{-i\sqrt{\Gamma dt/2}p}).\end{aligned} \tag{81}$$

Thus, if the time interval Δt between error correction steps is small compared to the damping time Γ^{-1}, the displacements applied to code words are small, and error correction will be effective.

Aside from decoherence, we also need to worry about ''unitary errors.'' For example, an inadvertent rotation of the phase of the oscillator induces the unitary transformation

$$\mathrm{U}(\theta)\equiv\exp(i\theta a^\dagger a). \tag{82}$$

Like any unitary transformation, this phase rotation can be expanded in terms of Pauli operators. It is convenient to introduce the notation for the phase-space displacement operator

$$D(\gamma)\equiv\exp(\gamma a-\gamma^* a^\dagger)=\exp i\sqrt{2}[(\mathrm{Im}\gamma)q-(\mathrm{Re}\gamma)p], \tag{83}$$

where γ is a complex number. The displacements satisfy the identity

$$\mathrm{tr}(D(\gamma)D(\eta)^\dagger)=\pi\delta^2(\gamma-\eta), \tag{84}$$

so the operator $U(\theta)$ can be expanded in terms of displacements as

$$U(\theta)=\frac{1}{\pi}\int d^2\gamma u_\theta(\gamma)D(\gamma), \tag{85}$$

where

$$u_\theta(\gamma)=\mathrm{tr}(U(\theta)D(\gamma)^\dagger). \tag{86}$$

Evaluating the trace in the coherent state basis, we find that

$$u_\theta(\gamma)=\frac{ie^{i\theta/2}}{2\sin(\theta/2)}\exp\left(-\frac{i}{2}|\gamma|^2\cot(\theta/2)\right). \tag{87}$$

For small θ, the coefficient

$$u_\theta(\gamma)\approx\frac{i}{\theta}\exp\left(-\frac{i}{\theta}|\gamma|^2\right) \tag{88}$$

has a rapidly oscillating phase, and can be regarded as a distribution with support concentrated on values of γ such that $|\gamma|^2\sim\theta$; indeed, formally

$$\lim_{\theta\to 0}u_\theta(\gamma)=\pi\delta^2(\gamma). \tag{89}$$

Thus a rotation by a small angle θ can be accurately expanded in terms of small displacements—error correction is effective if an oscillator is slightly overrotated or underrotated.

VIII. THE GAUSSIAN QUANTUM CHANNEL

At what rate can error-free digital information be conveyed by a noisy continuous signal? In classical information theory, an answer is provided by Shannon's noisy channel coding theorem for the Gaussian channel [18]. This theorem establishes the capacity that can be attained by a signal with specified average power, for a channel with specified bandwidth and specified Gaussian noise power. The somewhat surprising conclusion is that a nonzero rate can be attained for any nonvanishing value of the average signal power.

A natural generalization of the Gaussian classical channel is the *Gaussian quantum channel*. The Gaussian quantum channel is a Pauli channel: N oscillators are transmitted, and the q and p displacements acting on the oscillators are independent Gaussian random variables with mean 0 and variance σ^2. A code is an M-dimensional subspace of the Hilbert space of the N oscillators, and the rate R of the code (in qudits) is defined as

$$R=\frac{1}{N}\log_2 M. \tag{90}$$

The quantum-information capacity C_Q of the channel is the maximal rate at which quantum information can be transmitted with fidelity arbitrarily close to one.

The need for a constraint on the signal power to define the capacity of the Gaussian classical channel can be understood on dimensional grounds. The classical capacity (in bits) is a dimensionless function of the variance σ^2, but σ^2 has dimensions. Another quantity with the same dimensions as σ^2 is needed to construct a dimensionless variable, and the power fulfills this role. But no power constraint is needed to define the quantum capacity of the quantum channel. The capacity (in qudits) is a function of the dimensionless variable $\hbar/\sigma^2$, where $\hbar$ is Planck's constant.

An upper bound on the quantum capacity of the Gaussian quantum channel was derived by Holevo and Werner [19]; they obtained (reverting now to units with $\hbar=1$)

$$C_Q\leqslant\log_2(1/\sigma^2), \tag{91}$$

for $0<\sigma^2<1$, and $C_Q=0$ for $\sigma^2\geqslant 1$. They also computed the coherent information I_Q of the Gaussian quantum channel, and maximized it over Gaussian signal states, finding [19]

$$(I_Q)_{\max}=\log_2(1/e\sigma^2), \tag{92}$$

for $0<\sigma^2<1/e$ (where $e=2.718\,28\ldots$). The coherent information is *conjectured* to be an attainable rate [1–3]; if this conjecture is true, then Eq. (92) provides a lower bound on C_Q.

Using our continuous variable codes, rigorous lower bounds on C_Q can be established. For σ^2 sufficiently small, a nonzero attainable rate can be established asymptotically for large N by either of two methods. In one method, the $n=2$ code described in Sec. IV is invoked for each oscillator, and concatenated with a binary quantum code. In the other method, which more closely follows Shannon's construction, a code for N oscillators is constructed as in Sec. VI, based on a close packing of spheres in $2N$-dimensional phase space. However (in contrast to the classical case), neither method works if σ^2 is too large. For large σ^2, encodings can be chosen that protect against q shifts or against p shifts, but not against both.

To establish an attainable rate using concatenated coding (the method that is easier to explain), we first recall a result concerning the quantum capacities of binary channels [15,20]. If X and Z errors are independent and each occur with probability p_e, then binary CSS codes exist that achieve a rate

$$R>1-2H_2(p_e)\equiv 1+2p_e\log_2 p_e+2(1-p_e)\log_2(1-p_e); \tag{93}$$

this rate is nonzero for $p_e<.1100$.

Now, for the Gaussian quantum channel, if we use the $n=2$ continuous variable code, errors afflicting the encoded qudit are described by a binary channel with independent X and Z errors. Since the code can correct shifts in q or p that satisfy $\Delta q,\Delta p<\sqrt{\pi}/2$, the error probability is

$$p_e<2\frac{1}{\sqrt{2\pi\sigma^2}}\int_{\sqrt{\pi}/2}^{\infty}dx e^{-x^2/2\sigma^2}. \tag{94}$$

Since the expression bounding p_e in Eq. (94) has the value .110 for $\sigma\approx.555$, we conclude that the Gaussian quantum channel has nonvanishing quantum capacity C_Q provided that

$$\sigma<.555. \tag{95}$$

One might expect to do better by concatenating the *hexagonal* $n=2$ single-oscillator code with a binary stabilizer

code, since the hexagonal code can correct larger shifts than the code derived from a square lattice. For the Gaussian quantum channel, the symmetry of the hexagonal lattice ensures that X, Y, and Z errors afflicting the encoded qudit are equally likely. A shift is correctable if it lies within the ''Voronoi cell'' of the dual lattice, the cell containing all the points that are closer to the origin than to any other lattice site. By integrating the Gaussian distribution over the hexagonal Voronoi cell, we find that the probability $p_{e,\mathrm{total}}$ of an uncorrectable error satisfies

$$p_{e,\mathrm{total}} < 1 - \frac{12}{2\pi\sigma^2}\int_0^r dx \int_0^{x/\sqrt{3}} dy e^{-(x^2+y^2)/2\sigma^2}, \quad (96)$$

where $r=(\pi/2\sqrt{3})^{1/2}$ is the size of the smallest uncorrectable shift. For a binary quantum channel with equally likely X, Y, and Z errors, it is known [21] that there are stabilizer codes achieving a nonvanishing rate for $p_{e,\mathrm{total}} < .1905$; our bound on $p_{e,\mathrm{total}}$ reaches this value for $\sigma \approx .547$.

Somewhat surprisingly, for very noisy Gaussian quantum channels, square lattice codes concatenated with CSS codes seem to do better than hexagonal codes concatenated with stabilizer codes. The reason this happens is that a CSS code can correct independent X and Z errors that occur with total probability $p_{e,\mathrm{total}} = p_X + p_Z - p_X \cdot p_Z$, which approaches $0.2079 > 0.1905$ as $p_X = p_Z \to 0.1100$. For a given value of σ, the qudit encoded in each oscillator will have a lower error probability if the hexagonal code is used. But if the square lattice is used, a higher qudit error rate is permissible, and this effect dominates when the channel is very noisy.

We remark that this analysis is readily extended to more general Gaussian quantum channels. We may consider Pauli channels acting on a single oscillator in which the probability distribution $P(\alpha,\beta)$ is a more general Gaussian function, not necessarily symmetric in p and q. In that case, a symplectic transformation (one preserving the commutator of p and q) can be chosen that transforms the covariance matrix of the Gaussian to a multiple of the identity; therefore, this case reduces to that already discussed above. We may also consider channels acting on N oscillators that apply shifts in the $2N$-dimensional phase space, chosen from a Gaussian ensemble. Again there is a symplectic transformation that diagonalizes the covariance matrix; therefore, this case reduces to N independent single oscillator channels, each with its own value of σ^2.

IX. SYMPLECTIC OPERATIONS

To use these codes for fault-tolerant quantum computation, we will need to be able to prepare encoded states, perform error recovery, and execute quantum gates that act on the encoded quantum information. The most difficult task is encoding; we will postpone the discussion of encoding until after we have discussed encoded operations and error recovery.

Suppose, for example, that we have N oscillators, each encoding a qunit. We wish to apply $\mathrm{U}(n^N)$ transformations that preserve the code subspace of the N qunits. As is typical of quantum codes, we will find that there is a discrete subgroup of $\mathrm{U}(n^N)$ that we can implement ''easily;'' but to complete a set of universal gates we must add further transformations that are ''difficult.'' In the case of our continuous variable codes, the easy gates will be accomplished using linear optical elements (phase shifters and beam splitters), along with elements that can ''squeeze'' an oscillator. For the ''difficult'' gates we will require the ability to count photons.

The easy gates are the gates in the Clifford group. In general, the Clifford group of a system of N qunits is the group of unitary transformations that, acting by conjugation, take tensor products of Pauli operators to tensor products of Pauli operators (one says that they preserve the ''Pauli group''). Since for N oscillators the tensor products of Pauli operators have the form (44), the Clifford group transformations, acting by conjugation, are linear transformations of the p's and q's that preserve the canonical commutation relations. Such transformations are called symplectic transformations. The symplectic group has a subgroup that preserves the photon number

$$(\text{total photon number}) = \sum_{i=1}^{N} a_i^\dagger a_i . \quad (97)$$

The transformations in this subgroup can be implemented with linear optics [22]. The full symplectic group also contains ''squeeze operators'' that take an a to a linear combination of a's and $a^\dagger$'s; equivalently, the squeeze operators rescale canonical operators by a real number λ along one axis in the quadrature plane, and by λ^{-1} along the conjugate axis, as in (for example)

$$q_1 \to \lambda q_1, \quad p_1 \to \lambda^{-1} p_1 . \quad (98)$$

With squeezing and linear optics, we can in principle implement any symplectic transformation.

Aside from the symplectic transformations, we will also assume that it is easy to do displacements that shift q and p by constants. A displacement of q_1 by c is actually the limiting case of a symplectic transformation on two oscillators q_1 and q_2:

$$q_1 \to q_1 + \varepsilon q_2, \quad p_1 \to p_1 + \varepsilon p_2$$
$$q_2 \to q_2 - \varepsilon q_1, \quad p_2 \to p_2 - \varepsilon p_1, \quad (99)$$

where $\varepsilon \to 0$ with $\varepsilon q_2 = c$ held fixed.

Since for the code with stabilizer generators (21) the Pauli operators acting on our encoded qunits are $\overline{X} = e^{ip\alpha}$ and $\overline{Z} = e^{2\pi i q/n\alpha}$, the Clifford group transformations acting on N qunits constitute a subgroup of the symplectic transformations (including shifts) acting on N oscillators, the subgroup that preserves a specified lattice in phase space. Thus we can do any encoded Clifford group gate we please by executing an appropriate symplectic transformation (possibly including a shift).

A similar comment applies to the case of a qunit encoded in a qudit. Since the logical Pauli operators are $\overline{X} = X^{r_1}$ and $\overline{Z} = Z^{r_2}$, each Clifford group transformation in the

n-dimensional code space is also a Clifford group transformation on the underlying qudit.

But we must also be sure that our implementation of the Clifford group is *fault tolerant*. In previous discussions of quantum fault tolerance for $[[N,k,2t+1]]$ codes, the central theme has been that propagation of error from one qudit to another in the same code block must be very carefully controlled [23,24]. For shift-resistant codes the main issue is rather different. Since each qudit typically has a (small) error anyway, propagation of error from one qudit to another is not necessarily so serious. But what must be controlled is *amplification* of errors—gates that turn small errors into large errors should be avoided.

The Clifford group can be generated by gates that are fault-tolerant in this sense. The Clifford group for qunits can be generated by three elements. The SUM gate is a two-qunit gate that acts by conjugation on the Pauli operators according to

$$\text{SUM:} \quad X_1^a X_2^b \to X_1^a X_2^{b-a}, \quad Z_1^a Z_2^b \to Z_1^{a+b} Z_2^b. \tag{100}$$

Here qunit 1 is said to be the control of the SUM gate, and qunit 2 is said to be its target; in the binary $(n=2)$ case, SUM is known as controlled-NOT, or CNOT. The Fourier gate F acts by conjugation as

$$F: \quad X \to Z, \quad Z \to X^{-1}; \tag{101}$$

for $n=2$ the Fourier Transform is called the Hadamard gate. The phase gate P acts as

$$P: \quad X \to (\eta) XZ, \quad Z \to Z, \tag{102}$$

where the *n*-dependent phase η is $\omega^{1/2}$ if n is even and 1 if n is odd. Any element of the Clifford group can be expressed as a product of these three generators. (In Ref. [8] another gate S was included among the generators of the Clifford group, but in fact the S gate can be expressed as a product of SUM gates.)

For an *n*-dimensional system encoded in a continuous variable system, these Clifford group generators can all be realized as symplectic transformations. In the case where the stabilizer generators are symmetric in q and p,

$$\overline{X} = \exp\left(-ip\sqrt{\frac{2\pi}{n}}\right), \quad \overline{Z} = \exp\left(iq\sqrt{\frac{2\pi}{n}}\right), \tag{103}$$

the required symplectic transformations are

$$\begin{aligned} &\text{SUM:} q_1 \to q_1, \quad p_1 \to p_1 - p_2, \\ &q_2 \to q_1 + q_2, \quad p_2 \to p_2, \\ &F: \quad q \to p, \quad p \to -q, \\ &P: \quad q \to q, \quad p \to p - q + c, \end{aligned} \tag{104}$$

where the *n*-dependent shift c is 0 for n even and $\sqrt{\pi/2n}$ for n odd. Under these symplectic transformations, small deviations of q and p from the stabilizer lattice remain small; in this sense the transformations are fault tolerant.

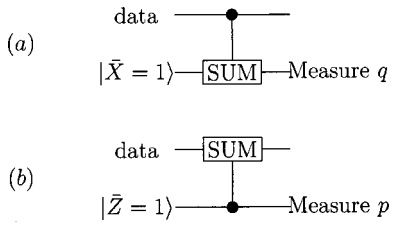

FIG. 4. Measurement of the error syndrome. (a) To diagnose the q shift, an ancilla is prepared in the encoded $\overline{X}=1$ state, a SUM gate is executed with the data as control and the ancilla as target, and the position of the ancilla is measured. (b) To diagnose the p shift, the ancilla is prepared in the $\overline{Z}=1$ state, a SUM gate is executed with the ancilla as control and the data as target, and the momentum of the ancilla is measured.

X. ERROR RECOVERY

If we are willing to destroy the encoded state, then measuring the encoded $\overline{X}$ or $\overline{Z}$ is easy—we simply conduct a homodyne measurement of the q or p quadrature of the oscillator. For example, suppose that we measure q for a state in the code subspace. If there are no errors and the measurement has perfect resolution, the only allowed values of q will be integer multiples of α. If there are errors or the measurement is imperfect, classical error correction can be applied to the outcome, by adjusting it to the nearest $\alpha \cdot k$, where k is an integer. Then the outcome of the measurement of $\overline{Z}$ is ω^k.

To diagnose errors in a coded data state, we must measure the stabilizer generators. This measurement can be implemented by ''feeding'' the errors from the code block to a coded ancilla, and then measuring the ancilla destructively, following the general procedure proposed by Steane [25] (see Fig. 4). For example, to measure the generator $e^{2\pi i q/\alpha}$ (i.e., the value of q modulo α), we prepare the ancilla in the state $(|\overline{0}\rangle + |\overline{1}\rangle)/\sqrt{2}$, the equally weighted superposition of all $|q = s \cdot \alpha\rangle$, s being an integer. Then a SUM gate is executed with the data as control and the ancilla as target—acting according to

$$q_2 \to q_1 + q_2, \tag{105}$$

where q_1, q_2 are the values of q for the data and ancilla respectively, prior to the execution of the SUM gate. By measuring q of the ancilla, the value of $q_1 + q_2$ is obtained, and this value modulo α determines the shift that should be applied to the data to recover from the error.

Similarly, to measure the stabilizer generator $e^{inp\alpha}$, we prepare the ancilla in the state $|\overline{0}\rangle$, the equally weighted superposition of all $|p = s \cdot 2\pi/n\alpha\rangle$, s being an integer. Then a SUM gate is executed with the ancilla as control and the data as target. Finally, the p quadrature of the ancilla is measured. The outcome reveals the value of $p_2 - p_1$ prior to the SUM gate, where p_1 is the momentum of the data, and p_2 is the momentum of the ancilla. The measured value modulo $2\pi/n\alpha$ then determines the shift that should be applied to the data to recover from the error.

Of course, the ancilla used in the syndrome measurement can also be faulty, resulting in errors in the syndrome and

imperfect recovery. Similarly, the measurement itself will not have perfect resolution, and the shift applied to recover will not be precisely correct. Furthermore, as is discussed in Sec. V, the ideal code words are unphysical nonnormalizable states, so that the encoded information will always be carried by approximate code words. For all these reasons, deviations from the code subspace are unavoidable. But if a fresh supply of ancilla oscillators is continuously available, we can prevent these small errors from accumulating and eventually damaging the encoded quantum information.

XI. UNIVERSAL QUANTUM COMPUTATION

Symplectic transformations together with homodyne measurements are adequate for Clifford group computation and for error recovery (assuming we have a supply of encoded states). But to achieve universal computation in the code space, we need to introduce additional operations. Fortunately, the quantum optics laboratory offers us another tool that can be used to go beyond the symplectic computational model—the ability to count photons.

There are a variety of ways in which photon counting can be exploited to complete a universal set of fault-tolerant gates. We will describe two possible ways, just to illustrate how universal fault-tolerant quantum computation might be realized with plausible experimental tools. For this discussion, we will consider the binary case $n=2$.

A. Preparing a Hadamard eigenstate

We can complete the universal gate set if we have the ability to prepare eigenstates of the Hadamard operator H [26,27]. For this purpose it suffices to be able to *destructively* measure H of an encoded qudit. Assuming we are able to prepare a supply of the encoded $\overline{Z}$ eigenstate $|\overline{0}\rangle$, we can make an encoded Einstein-Podolsky-Rosen (EPR) pair using symplectic gates. Then by destructively measuring H for one encoded qudit in the pair, we prepare the other qudit in an encoded eigenstate of H with the known eigenvalue.

But how can we destructively measure H? The Hadamard gate acts by conjugation on the encoded Pauli operators according to

$$H: \quad \overline{X}\to\overline{Z}, \quad \overline{Z}\to\overline{X}. \tag{106}$$

If we use the code that treats q and p symmetrically so that $\overline{X}=\exp(-ip\sqrt{\pi})$ and $\overline{Z}=\exp(iq\sqrt{\pi})$, then the Hadamard gate can be implemented by the symplectic transformation.

$$q\to p, \quad p\to -q \tag{107}$$

(recalling that $\overline{X}^2=\overline{Z}^2=I$ on the code subspace). This transformation is just the Fourier transform

$$F: \quad \exp\left(i\frac{\pi}{2}a^\dagger a\right) \tag{108}$$

(where $a^\dagger a$ is the photon number), which describes the natural evolution of the oscillator for one quarter cycle. Thus the phase of the Hadamard operator is simply the photon number modulo four; we can measure the eigenvalue of the encoded Hadamard transformation by counting photons.

In fact the photon number in the code space is even—all code words are invariant under a 180° rotation in the quadrature plane. Because of this feature, the preparation of the Hadamard eigenstate has some fault tolerance built in; if the photon count is off by one, the number will be odd and an error will be detected. In that case we reject the state we have prepared and make a new attempt. If the photon number is large, then obtaining a reliable determination of the photon number modulo four will require highly efficient photodetection. But on the other hand, the photon number need not be very large — the mean value of $a^\dagger a$ is about Δ^{-2}, where Δ is the squeeze factor, and we have seen that the intrinsic error rate due to imperfect squeezing is quite small for $\Delta\sim 1/4$, or $\langle a^\dagger a\rangle\sim 16$.

An alternative to preparing an encoded EPR pair and destructively measuring one member of the pair is to prepare $|\overline{0}\rangle$ and then perform a quantum nondemolition measurement of the photon number modulo 4. This might be done by coupling the oscillator to a two-level atom as proposed in Ref. [28]. Indeed, since only one bit of information needs to be collected (the photon number is either 0 or 2 modulo 4), the measurement could be made in principle by reading out a single atom. Suppose that the coupling of oscillator to atom is described by the perturbation

$$H'=\lambda a^\dagger a\sigma_z, \tag{109}$$

where $\sigma_z=-1$ in the atomic ground state $|g\rangle$ and $\sigma_z=1$ in the atomic excited state $|e\rangle$. By turning on this coupling for a time $t=\pi/4\lambda$, we execute the unitary transformation

$$\mathrm{U}=\exp[-i(\pi/4)a^\dagger a\sigma_z]. \tag{110}$$

Then the atomic state $(|g\rangle+|e\rangle)/\sqrt{2}$ evolves as

$$\mathrm{U}: \frac{1}{\sqrt{2}}(|g\rangle+|e\rangle)\to\frac{1}{\sqrt{2}}e^{ia^\dagger a\pi/4}(|g\rangle+e^{-ia^\dagger a\pi/2}|e\rangle). \tag{111}$$

By measuring the atomic state in the basis $(|g\rangle\pm|e\rangle)/\sqrt{2}$, we read out the value of the photon number modulo 4 (assumed to be either 2 or 4). Since this is a nondemolition measurement, it can be repeated to improve reliability. By measuring the photon number mod 4 many times (perhaps with rounds of error correction in between the measurements), we obtain a Hadamard eigenstate with excellent fidelity.

How does the ability to construct the Hadamard eigenstate enable us to achieve universal quantum computation? We can make contact with constructions that have been described previously in the literature by observing that the Hadamard eigenstate can be transformed by applying symplectic gates to the ''$\pi/8$-phase state.'' First note that the two Hadamard eigenstates can be converted to one another by applying the encoded gate $\overline{XZ}$, which can be implemented

$$e^{-i\pi/4}P = \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

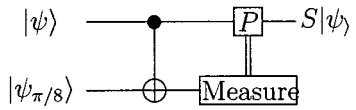

FIG. 5. Implementation of the S gate. An ancilla is prepared in the state $|\psi_{\pi/8}\rangle$, and a CNOT gate is executed with the data as control and the ancilla as target; then the ancilla is measured in the basis $\{|0\rangle, |1\rangle\}$. A P gate is applied to the data conditioned on the measurement outcome.

by shifting both p and q. Therefore it is sufficient to consider the eigenstate corresponding to the eigenvalue 1,

$$|\psi_{H=1}\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle. \tag{112}$$

By applying the symplectic single-qudit gate

$$H \cdot P^{-1} \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}, \tag{113}$$

we obtain the $\pi/8$ state

$$|\psi_{\pi/8}\rangle = \frac{1}{\sqrt{2}}(e^{-i\pi/8}|0\rangle + e^{i\pi/8}|1\rangle). \tag{114}$$

Now this $\pi/8$ state can be used to perform the nonsymplectic phase gate

$$S = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}, \tag{115}$$

which completes the universal gate set [29,30]. The gate is constructed by executing the circuit shown in Fig. 5. We perform a CNOT gate with the arbitrary single-qudit state $|\psi\rangle = a|0\rangle + b|1\rangle$ as the control, and the $\pi/8$ phase state as the target; then the target qudit is measured in the basis $\{|0\rangle, |1\rangle\}$. If the measurement outcome is $|0\rangle$ (which occurs with probability 1/2), then the control qudit has become $ae^{i\pi/8}|0\rangle + be^{-i\pi/8}|1\rangle = S|\psi\rangle$ and we are done. If the measurement outcome is $|1\rangle$, then the control qudit has become $ae^{-i\pi/8}|0\rangle + be^{i\pi/8}|1\rangle$, and we obtain $S|\psi\rangle$ by applying the symplectic single-qudit gate

$$e^{-i\pi/4}P = \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{116}$$

Completing the universal gate set by measuring the Hadamard transformation has some drawbacks. For one thing, while photon number modulo four corresponds to the Hadamard eigenvalue in the ideal code space, this correspondence will not apply to approximate code words unless they are of a special type.

Recall that the imperfections of the code words arising from finite squeezing can be described by an ''embedded error'' $|\eta\rangle$ as in Eq. (40); a Gaussian approximate code word has a Gaussian embedded error

$$\eta(u,v) = \frac{1}{\sqrt{\pi\Delta\kappa}} \exp\left(-\frac{1}{2}(u^2/\Delta^2 + v^2/\kappa^2) \right), \tag{117}$$

where Δ is the width in q and κ is the width in p. Symplectic gates act separately on the encoded qudit and the ''embedded error'' $|\eta\rangle$; for example, the Fourier transform gate and the SUM gate act on the error according to

$$F: |u,v\rangle \rightarrow |v,-u\rangle,$$

$$\text{SUM}: |u_1,v_1;u_2,v_2\rangle \rightarrow |u_1,v_1+v_2;u_2-u_1,v_2\rangle. \tag{118}$$

By measuring the photon number modulo 4, we actually measure the *product* of the eigenvalue of the Hadamard gate acting on the code word and the eigenvalue of F acting on the embedded error. The latter always equals 1 *if* we use symmetrically squeezed code words, with $\Delta = \kappa$.

Symmetric squeezing is not in itself sufficient to ensure that the measurement of the photon number modulo 4 will prepare the desired encoded Hadamard eigenstate. We also need to consider how the embedded error is affected by the preparation of the EPR pair that precedes the measurement. To prepare the EPR pair, we use the SUM gate. Suppose that we start with two symmetrically squeezed states. Then the SUM gate yields the error wave function

$$\eta'(u_1,v_1;u_2,v_2) = \exp\{-[u_1^2 + (v_1 - v_2)^2 + (u_1 + u_2)^2 + v_2^2]/\Delta^2\}. \tag{119}$$

Not only is it not symmetric, but the error is entangled between the two oscillators. The Fourier transform measurement will not give the desired result when applied to either oscillator.

To ameliorate this problem, we could perform error correction after the preparation of the EPR pair and before the measurement, where the error correction protocol has been designed to produce symmetrically squeezed states. Or we could avoid preparing the EPR state by using the nondemolition measurement of photon number modulo 4, as described above.

B. Preparing a cubic phase state

Now we will describe another way to use photon counting to implement nonsymplectic gates, which is less sensitive to the code word quality. Again, we will complete the universal gate set by constructing the $\pi/8$ phase gate S.

For our binary ($n=2$) code, the code subspace has the basis

$$|\overline{0}\rangle = \sum_{s=-\infty}^{+\infty} |q = 2s\alpha\rangle,$$

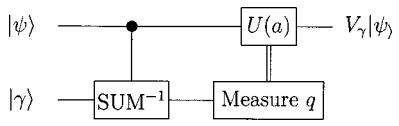

FIG. 6. Implementation of the cubic phase gate. An ancilla is prepared in the state $|\gamma\rangle$, and a SUM^{-1} gate is executed with the data as control and the ancilla as target; then the position of the ancilla is measured. A symplectic gate U(a) is then applied to the data, conditioned on the outcome a of the measurement.

$$|\overline{1}\rangle = \sum_{s=-\infty}^{+\infty} |q=(2s+1)\alpha\rangle. \tag{120}$$

(For now we ignore the embedded error due to imperfect squeezing; it will be taken into account later.) An S gate acting on the encoded qudit is implemented (up to an irrelevant overall phase) by the unitary operator

$$W = \exp\left(\frac{i\pi}{4}[2(q/\alpha)^3+(q/\alpha)^2-2(q/\alpha)]\right). \tag{121}$$

Indeed, we can check that

$$2x^3+x^2-2x(\mathrm{mod}8) = \begin{cases} 0, & \text{if } x=2s\ , \\ 1, & \text{if} x=2s+1\ . \end{cases} \tag{122}$$

The operator W is the product of a symplectic gate and the cubic phase gate

$$V_\gamma = \exp(i\gamma q^3), \tag{123}$$

where $\gamma=\pi/(2\alpha^3)$. But how do we implement the cubic gate? In fact, if we are able to prepare a ''cubic phase state''

$$|\gamma\rangle = \int dx e^{i\gamma x^3}|x\rangle, \tag{124}$$

then we can perform the gate V_γ by executing the circuit shown in Fig. 6.

To understand how the circuit works, consider the more general problem of implementing a phase gate that acts on the position eigenstates according to

$$V_\phi : |q\rangle \to e^{i\phi(q)}|q\rangle \tag{125}$$

(where $\phi(q)$ is a real-valued function), using the prepared phase state

$$|\phi\rangle = \int dx e^{i\phi(x)}|x\rangle. \tag{126}$$

If we perform the gate SUM^{-1} with position eigenstate $|q\rangle$ as control and $|\phi\rangle$ as target, and then measure the position of the target obtaining the outcome $|a\rangle$, the state of the control oscillator has become $e^{i\phi(q+a)}|q\rangle$. We can therefore complete the construction of V_ϕ by applying the transformation

$$\mathrm{U}(a) = e^{i[\phi(q)-\phi(q+a)]}. \tag{127}$$

If the function $\phi(q)$ is cubic, then the argument of the exponential is quadratic and hence U(a) is a symplectic transformation.

Now the problem of implementing universal quantum computation in the code subspace has been reduced to the problem of preparing the cubic phase state $|\gamma\rangle$. We can accomplish this task by preparing an EPR pair, and then performing a suitable photon counting measurement (a nonideal homodyne measurement) on one member of the pair.

Of course, the EPR pair will not be perfect. To be definite, let us suppose (although this assumption is not really necessary) that it is a Gaussian state

$$|\psi_{\sigma_p,\sigma_q}\rangle = \left(\frac{\sigma_p}{\pi\sigma_q}\right)^{1/2}\int dq_1 dq_2 \exp\left[-\frac{1}{2}\sigma_p^2\left(\frac{q_1+q_2}{2}\right)^2\right] \times \exp\left[-\frac{1}{2}(q_1-q_2)^2/\sigma_q^2\right]|q_1,q_2\rangle \tag{128}$$

with $\sigma_p,\sigma_q \ll 1$.

Now suppose that the second oscillator is mixed with a coherent light beam, resulting in a large shift in momentum,

$$|\psi\rangle \to e^{iwq}|\psi\rangle, \quad w \gg \sigma_q^{-1}, \sigma_p^{-1}; \tag{129}$$

then the photon number is measured and n photons are detected. Thus the state of the first oscillator becomes (up to normalization)

$$|\psi_1^{(n)}\rangle \approx \left(\frac{\sigma_p}{\pi\sigma_q}\right)^{1/2}\int dq_1 |q_1\rangle e^{-1/2\,\sigma_p^2 q_1^2} \times \int dq_2 \varphi_n^*(q_2) e^{iwq_2} e^{-1/2(q_1-q_2)^2/\sigma_q^2}, \tag{130}$$

where $|\varphi_n\rangle$ denotes the photon number eigenstate, the eigenstate with eigenvalue $n+\frac{1}{2}$ of the Hamiltonian $H=\frac{1}{2}(p^2+q^2)$.

We can evaluate the q_2 integral in Eq. (130) by appealing to the semiclassical approximation. For q_2 in the classically allowed region and far from the classical turning points, we may write

$$\varphi_n^*(q_2) \sim \frac{1}{\sqrt{2\pi p(q_2)}}\exp\left(-i\int^{q_2} dx p(x)\right) + \frac{1}{\sqrt{2\pi p(q_2)}}\exp\left(+i\int^{q_2} dx p(x)\right), \tag{131}$$

where

$$p(x) = \sqrt{2n+1-x^2}. \tag{132}$$

For $w \gg \sigma_q^{-1}$, the rapid phase oscillations strongly suppress the contribution to the integral arising from the left-moving part of $\varphi^{(n)}(q_2)$. A contribution from the right-moving part survives provided that

$$|p(q_1)-w| < \sigma_q^{-1}. \tag{133}$$

When this condition is satisfied, it is a reasonable approximation to replace the Gaussian factor $e^{-1/2(q_1-q_2)^2/\sigma_q^2}$ in the q_2 integral by $\sqrt{2\pi\sigma_q^2}\delta(q_1-q_2)$, so that we obtain

$$|\psi_1^{(n)}\rangle \approx (2\sigma_p\sigma_q)^{1/2}\int dq_1 |q_1\rangle e^{-1/2\sigma_p^2 q_1^2}\frac{1}{\sqrt{2\pi p(q_1)}} \times \exp\left(-i\int^{q_1} dx[p(x)-w]\right). \tag{134}$$

The probability that n photons are detected is given by the norm of this $|\psi_1^{(n)}\rangle$. The values of n that occur with appreciable probability satisfy Eq. (133) for some q_1 with $|q_1| < \sigma_p^{-1}$; thus typical measurement outcomes are in the range

$$n+\frac{1}{2}\sim\frac{1}{2}(w\pm\sigma_q^{-1})^2+\frac{1}{2}\sigma_p^{-2}, \tag{135}$$

with a flat probability distribution

$$\mathrm{Prob}(n)=\langle\psi_1^{(n)}|\psi_1^{(n)}\rangle\sim\frac{\sigma_q}{w}. \tag{136}$$

Heuristically, after the momentum shift is applied, the oscillator that is measured has momentum of order $w\pm\sigma_q^{-1}$, and position of order σ_p^{-1}, so that the value of the energy is $n+\frac{1}{2}=\frac{1}{2}(p^2+q^2)\sim\frac{1}{2}(w\pm\sigma_q^{-1})^2+\frac{1}{2}\sigma_p^{-2}$.

For a particular typical outcome of the photon-counting measurement, since $|\psi_1^{(n)}\rangle$ has its support on $|q_1|<\sigma_p^{-1} \ll w$, we can Taylor expand $p(x)$ about $x=q_1$ to express $|\psi_1^{(n)}\rangle$ as

$$\psi_1^{(n)}(q_1)\propto\exp\left(-i\int^{q_1}(\sqrt{(2n+1)-x^2}-w)dx\right) \propto\exp\left(\frac{i}{6\sqrt{2n+1}}q_1^3-i(\sqrt{2n+1}-w)q_1 + O(q_1^5/w^3)\right). \tag{137}$$

This is a cubic phase state to good precision if w is large enough.

The coefficient γ' of q_1^3 in the phase of ψ_1 is of order $n^{-1/2}$, while the phase γ of the operator V_γ that we wish to execute is of order one. However, we can construct V_γ from $V_{\gamma'}$ as

$$V_\gamma=(S_{\gamma/\gamma'})^{-1}V_{\gamma'}(S_{\gamma/\gamma'}), \tag{138}$$

where S_r is a squeeze operation that acts according to

$$S_r: q\to(r)^{1/3}q, \qquad p\to(r)^{-1/3}p. \tag{139}$$

Alternatively, we could squeeze the phase state $|\gamma'\rangle$ before we use it to implement the cubic phase gate.

Is this procedure fault tolerant? Before considering the errors introduced during the implementation of the cubic phase gate, we should check that the gate does not catastrophically amplify any preexisting errors. In general, a phase gate can transform a small position shift error into a potentially dangerous momentum shift error. Commuting $V(\phi)=e^{i\phi(q)}$ through the shift operator e^{-iup}, we find

$$e^{i\phi(q)}e^{-iup}=e^{-iup}e^{if_u(q)}e^{i\phi(q)}, \tag{140}$$

where $f_u(q)=\phi(q+u)-\phi(q)$; the operator $e^{if_u(q)}$ can be expanded in terms of momentum shift operators of the form e^{ivq} by evaluating the Fourier transform

$$\tilde{f}_u(v)=\int\frac{dq}{2\pi}e^{i(f_u(q)-vq)}. \tag{141}$$

Assuming we use a code where the parameter α is of order one, uncorrectable errors will be likely if $\tilde{f}_u(v)$ has significant support on values of v that are order one.

Suppose that $V(\phi)$ acts on an approximate code word whose wave function is concentrated on values of q in the domain $|q|<L$. Phase cancellations will strongly suppress $\tilde{f}_u(v)$, unless the stationary phase condition $f_u'(q)=v$ is satisfied for some value of q in the domain of the approximate code word. Therefore, $V(\phi)$ can propagate a preexisting position shift u to a momentum shift error of magnitude

$$|v|\sim\max_{|q|\le L}|f_u'(q)|. \tag{142}$$

The cubic phase gate needed to implement the encoded S gate is $W=e^{i\phi(q)}$, where $\phi(q)=\pi q^3/2\alpha^3$, so that $f_u(q)=3\pi uq^2/2\alpha^3+\cdots$ (ignoring small terms linear and constant in q), and $f_u'(q)=3\pi uq/\alpha^3$; the gate transforms the position shift u to a momentum shift

$$v\sim 3\pi Lu/\alpha^3. \tag{143}$$

For α of order one, then, to ensure that v is small we should use approximate code words with the property that the typical embedded position shift u satisfies

$$|u|\ll L^{-1}. \tag{144}$$

In particular, if the approximate code word's embedded errors are Gaussian, where κ is the typical size of a momentum shift and Δ is the typical size of a position shift, we require

$$\Delta\ll\kappa. \tag{145}$$

We assume that shift errors due to other causes are no larger than the embedded error.

In the circuit Fig. 6 that implements the cubic phase gate, position shift errors in either the encoded state $|\psi\rangle$ or the ancilla state $|\gamma\rangle$ might cause trouble. A shift by u in $|\psi\rangle$ is transformed to a phase error $e^{if_u(q)}$, and a shift by u in $|\gamma\rangle$ infects $|\psi\rangle$ with a phase error $e^{if_u(q+a)}$. Therefore, we should require that position shift errors in both $|\psi\rangle$ and $|\gamma\rangle$ satisfy the criterion (144), where L is the larger of the two wave packet widths.

When a cubic phase state is prepared by measuring half of an EPR pair, the packet width is of order σ_p^{-1} and typical position shift errors have $u \sim \sigma_q$. However, we must also take into account that either the encoded state or the ancilla must be squeezed as in Eq. (139). Suppose that the ancilla is squeezed, by a factor of order $n^{1/6} \sim w^{1/3}$; the wave packet is rescaled so that, after squeezing, the width L' and the typical shifts u' are given by

$$L' \sim \sigma_p^{-1} w^{-1/3}, \quad u' \sim \sigma_q w^{-1/3}. \tag{146}$$

Then the condition $|u'| \ll L'^{-1}$ is satisfied provided that $\sigma_q \ll \sigma_p w^{2/3}$. We also require that the rescaled packet has a large width compared to 1, or $\sigma_p \ll w^{-1/3}$.

For the derivation of Eq. (137), we used the approximations $w\sigma_q \gg 1$ and $w\sigma_p \gg 1$. We also need to check that the remainder terms in the Taylor expansion give rise to a phase error that is acceptably small. This error has the form $e^{if(q_1)}$, where $f(q_1) = O(q_1^5/w^3)$, corresponding to a momentum shift

$$v \sim f'(q_1) \sim \sigma_p^{-4} w^{-3}. \tag{147}$$

Squeezing amplifies this momentum shift error to $v' \sim v w^{1/3} \sim \sigma_p^{-4} w^{-8/3}$, which will be small compared to 1 provided that $\sigma_p \gg w^{-2/3}$. To summarize, our implementation of the cubic phase gate works well if the approximate code words have embedded errors satisfying $\Delta \ll \kappa$, and if widths σ_q and σ_p of the approximate EPR state satisfy $w \gg \sigma_q^{-1}$ and

$$w^{-1/3} \gg \sigma_p \gg w^{-2/3}. \tag{148}$$

Finally, how accurately must we count the photons? An error Δn in the photon number results in a phase error $e^{iv q_1}$ with $|v| \sim n^{-1/2} \Delta n$ in $\psi_1^{(n)}(q_1)$, which will be amplified by squeezing to $|v'| \sim |v| w^{1/3} \sim n^{-1/3} \Delta n$. Therefore, the precision of the photon number measurement should satisfy

$$\Delta n \ll n^{1/3} \tag{149}$$

to ensure that this error is acceptably small.

C. Purification

Either of the above two methods could be used to implement a nonsymplectic phase transformation that completes the universal gate set. Of course, experimental limitations might make it challenging to execute the gate with very high fidelity. One wonders whether it is possible to refine the method to implement fault-tolerant universal gates of improved fidelity.

In fact, such refinements are possible. We have seen that we can reach beyond the symplectic transformations and achieve universal quantum computation if we have a supply of appropriate ''nonsymplectic states'' that cannot be created with the symplectic gates. If the nonsymplectic states have the right properties, then we can carry out a purification protocol to distill from our initial supply of noisy nonsymplectic states a smaller number of nonsymplectic states with much better fidelity [31,32].

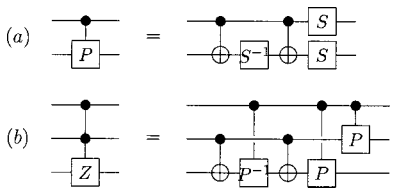

FIG. 7. Construction of the three-qudit gate $\Lambda^2(Z)$. (a) A $\Lambda(P)$ gate can be constructed (up to an overall phase) from two S gates, an S^{-1} gate, and two CNOT'S. The circuit is executed from left to right. (b) A $\Lambda^2(Z)$ gates can be constructed from two $\Lambda(P)$ gates, a $\Lambda(P^{-1})$ gate, and two CNOT'S.

An example of a nonsymplectic state that admits such a purification protocol is a variant of the state originally introduced by Shor [23], the three-qudit state

$$2^{-3/2} \sum_{a,b,c \in \{0,1\}} (-1)^{abc} |a\rangle_1 |b\rangle_2 |c\rangle_3; \tag{150}$$

it can be characterized as the simultaneous eigenstate of three commuting symplectic operators: $\Lambda(Z)_{1,2} X_3$ and its two cyclic permutations, where $\Lambda(Z)$ is the two-qudit conditional phase gate

$$\Lambda(Z): |a,b\rangle \to (-1)^{ab} |a,b\rangle. \tag{151}$$

As Shor explained, this nonsymplectic state can be employed to implement the Toffoli gate

$$T: |a,b,c\rangle \to |a,b,c \oplus ab\rangle, \tag{152}$$

and so provides an alternative way to complete the universal gate set.

To purify our supply of nonsymplectic states, symplectic gates are applied to a pair of nonsymplectic states and then one of the states is measured. Based on the outcome of the measurement, the other state is either kept or discarded. If the initial ensemble of states approximates the nonsymplectic states with adequate fidelity, then as purification proceeds, the fidelity of the remaining ensemble converges rapidly toward one.

The details of the purification protocol will be described elsewhere; here we will only remark that these Shor states can be readily created using symplectic gates and $\pi/8$-phase gates. The Shor state is obtained if we apply the transformation

$$\Lambda^2(Z): |a,b,c\rangle \to (-1)^{abc} |a,b,c\rangle \tag{153}$$

to the state

$$H_1 H_2 H_3 |0,0,0\rangle = 2^{-3/2} \sum_{a,b,c \in \{0,1\}} |a,b,c\rangle. \tag{154}$$

As shown in Fig. 7, $\Lambda^2(Z)$ can be applied by executing a circuit containing 5 S gates, 4 S^{-1} gates, and 8 CNOT gates.

Therefore, if we can apply symplectic gates accurately, and are also able to create a supply of $\pi/8$ states of reasonable fidelity (or can otherwise implement S gates of reason-

able fidelity), then we can use the purification protocol to implement Toffoli gates with very good fidelity.

XII. ENCODING

Now we have discussed how to execute universal quantum computation fault tolerantly, and how to perform error recovery. But the discussion has all been premised on the assumption that we can prepare encoded states. It is finally time to consider how this can be done. In fact, preparing simultaneous eigenstates of the stabilizer generators $\exp(2\pi iq/\alpha)$ and $\exp(-inp\alpha)$ is a challenging task.

For the $[[N,k]]$ stabilizer codes that have been discussed previously, encoding is not intrinsically difficult in that it can be accomplished with Clifford group gates. Acting by conjugation, Clifford group transformations take tensor products of Pauli matrices to tensor products of Pauli operators. In particular, there is a Clifford group transformation that takes the state $|0\rangle^{\otimes N}$ (the simultaneous eigenstate with eigenvalue one of all N single-qudit Z's) to the encoded $|\overline{0}\rangle^{\otimes k}$ (the simultaneous eigenstate with eigenvalue one of $(N-k)$ stabilizer generators and k encoded $\overline{Z}$'s).

Where our codes are different, in both their finite-dimensional and infinite-dimensional incarnations, is that a *single* qudit or oscillator is required to obey *two* independent stabilizer conditions—i.e., to be the simultaneous eigenstate of two independent Pauli operators. Hence there is no Clifford group encoder. In the continuous variable case, the problem can be stated in more familiar language: the symplectic transformations take Gaussian (coherent or squeezed) states to Gaussian states. Hence no symplectic transformation can take (say) the oscillator's ground state to a state in the code subspace.

So encoding requires nonsymplectic operations, and as far as we know it cannot be accomplished by counting photons either—we must resort to a nonlinear coupling between oscillators, such as a $\chi^{(3)}$ coupling. We will describe one possible encoding scheme: First, we prepare a squeezed state, an eigenstate of the momentum with $p=0$. This state is already an eigenstate with eigenvalue one of the stabilizer generator $e^{inp\alpha}$, but not an eigenstate of $e^{2\pi iq/\alpha}$; rather its value of q is completely indefinite. To obtain an encoded state, we must project out the component with a definite value of q modulo α.

This can be achieved by coupling the oscillator to another oscillator that serves as a meter, via the perturbation of the Hamiltonian

$$H' = \lambda q(b^\dagger b), \tag{155}$$

where b is the annihilation operator of the meter.[1] This perturbation modifies the frequency of the meter,

$$\Delta\omega_{\text{meter}} = \lambda q; \tag{156}$$

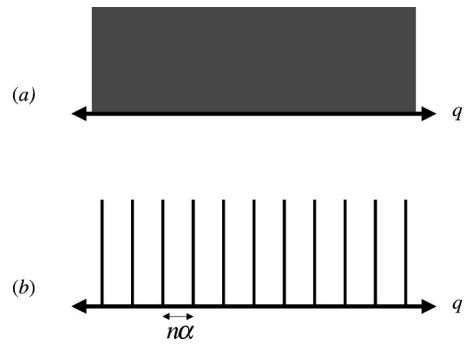

FIG. 8. Preparation of an encoded state. (a) An eigenstate of p is prepared, which has an indefinite value of q. (b) The value of q modulo $n\alpha$ is measured, projecting out a state that differs from the encoded $\overline{Z}$ eigenstate by a shift in q.

then if this coupling is turned on for a time $t=2\pi/\lambda n\alpha$, the phase of the meter advances by

$$\Delta\theta_{\text{meter}} = 2\pi q/n\alpha. \tag{157}$$

By reading out the phase, we can determine the value of q modulo $n\alpha$, and apply a shift if necessary to obtain the state with $q\equiv 0 \pmod{n\alpha}$, the known state $|\overline{0}\rangle$ in the code subspace. (See Fig. 8.)

Of course, in practice the state squeezed in p prepared in the first step will be only finitely squeezed, and the measurement of q modulo $n\alpha$ will have imperfect resolution. If the squeezed state is Gaussian and the measurement has a Gaussian acceptance, then this procedure will produce an approximate code word of the sort described in Sec. V.

If we are able to prepare ''good enough'' encoded states, we can distill better ones. The distillation protocol is similar to the error recovery procedure, but where the ancilla used for syndrome measurement may be fairly noisy. We might improve the convergence of the distillation procedure by discarding the data oscillator if the measurement of the ancilla oscillator yields a value of q or p that is too distant from the values allowed by the code stabilizer.

So far, we have described how to prepare encoded states for the ''single-oscillator'' codes described in Sec. IV. To prepare an encoded state for one of the N-oscillator codes described in Sec. VI, we proceed in two steps. First we prepare each of N oscillators in a single-oscillator encoded state. Then we apply a symplectic transformation to obtain the encoded state of the N-oscillator code.

A particular known encoded state of a lattice stabilizer code can itself be regarded as a code with an $(n=1)$-dimensional code space. Hence it can be characterized by a *self-dual* symplectic lattice. For example, the $\overline{X}=1$ state of a qunit encoded in a single oscillator is the simultaneous eigenstate with eigenvalue of one of the operators $e^{-ip\alpha}$ and $e^{2\pi iq/\alpha}$—the state associated with the self-dual lattice whose basis vectors are $p\alpha/\sqrt{2\pi}$ and $q\sqrt{2\pi}/\alpha$.

One encoded state can be transformed to another by symplectic gates if there is a symplectic linear transformation that takes the self-dual lattice associated with the first state to

[1]There is an extensive literature on the experimental realization and applications of this kind of coupling; see [33].

the self-dual lattice associated with the second. In fact, such a symplectic transformation exists for any pair of self-dual lattices.

A linear transformation acting on the p's and q's modifies the generator matrix M of a lattice according to

$$M \to MS; \tag{158}$$

this transformation is symplectic if

$$S\omega S^T = \omega, \tag{159}$$

where

$$\omega = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}. \tag{160}$$

We saw in Sec. VI that we can always choose the generator matrix M of a self-dual lattice so that the matrix A has the form

$$A \equiv M\omega M^T = \omega; \tag{161}$$

that is, so that M is a symplectic matrix. Therefore, the generator matrices M_1 and M_2 of two self-dual lattices can each be chosen to be symplectic; then the linear transformation

$$S = M_1^{-1} M_2 \tag{162}$$

that takes one lattice to the other is also symplectic. Thus, while the task of preparing the encoded states of the single-oscillator codes can be accomplished only by introducing a nonlinear coupling between oscillators, proceeding from single-oscillator encoded states to many-oscillator encoded states can be achieved with linear optical operations and squeezing.

XIII. PHYSICAL FAULT TOLERANCE?

In a physical setting, making use of the continuous variable quantum error-correcting codes proposed here (or ''digital'' quantum codes that have been proposed previously) is a daunting challenge. We must continually measure the stabilizer operators (the ''error syndrome'') to diagnose the errors; to recover we must apply frequent shifts of the canonical variables that are conditioned on the measurement outcomes. Cold ancilla oscillators must be provided that are steadily consumed by the syndrome measurements. The ancillas must be discarded (or refreshed) to rid the system of excess entropy that has been introduced by the accumulated errors.

An alternative to this complex scheme was suggested in Ref. [34]. Perhaps we can engineer a quantum system whose (degenerate) ground state is the code subspace. Then the natural coupling of the system to its environment will allow the system to relax to the code space, removing errors introduced by quantum and thermal noise, or through the imperfect execution of quantum gates. Such a system, if it could be built, would be a highly stable quantum memory.

Continuous variable coding suggests possible approaches to implementing this type of physical fault tolerance. For example, the Hamiltonian

$$H = 2 - [\cos p + \cos(2\pi n q)] \tag{163}$$

has an n-fold degenerate (but nonnormalizable) ground state that is just the code space of a continuous variable code. (The operators $\cos p$ and $\cos 2\pi nq$ commute and can be simultaneously diagonalized.) The low-lying states of a real system whose Hamiltonian is a reasonable approximation to H would resemble the approximate code words described in Sec. V.

One possible way to realize physical fault tolerance is suggested by the codes for an electron in a Landau level, described in Sec. III. The wave functions in the code space are doubly periodic with a unit cell that encloses n flux quanta, where n is the code's dimension. If we turn on a tunable periodic potential whose unit cell matches that of the code, then the Landau level is split into n energy bands, and the code words are the states with vanishing Bloch momentum. Therefore, an encoded state could be prepared by turning on the potential, waiting for dissipative effects to cause the electrons to relax to the bottom of the lowest band, and then adiabatically turning off the potential. If dissipative effects cause electrons to relax to the bottom of a band on a timescale that is short compared to spontaneous decay from one band to another, then more general encoded states could be prepared by a similar method. Furthermore, turning on the potential from time to time would remove the accumulated Bloch momentum introduced by errors, allowing the electron to relax back to the code space.

XIV. CONCLUDING COMMENTS

We have described codes that protect quantum states encoded in a finite-dimensional subspace of the Hilbert space of a system described by continuous quantum variables. With these codes, continuous variable systems can be used for robust storage and fault-tolerant processing of quantum information.

For example, the coded information could reside in the Hilbert space of a single-particle system described by canonical quantum variables q and p. In practice, these variables might describe the states of a mode of the electromagnetic field in a high-finesse microcavity, or the state of the center of mass motion of an ion in a trap. Or the continuous Hilbert space could be the state space of a rotor described by an angular variable θ and its conjugate angular momentum L; in practice, these variables might be the phase and charge of a superconducting quantum dot. Our coding scheme can also be applied to a charged particle in a magnetic field.

Our codes are designed to protect against small errors that occur continually—diffusive drifts in the values of the canonical variables. The codes are less effective in protecting against large errors that occur rarely. In some settings, we may desire protection against both kinds of errors. One way to achieve that would be to *concatenate* our continuous-variable codes with conventional finite-dimensional quantum codes.

When we consider how to manipulate continuous-variable quantum information fault tolerantly, the issues that arise are rather different than in previous discussions of quantum fault tolerance. With continuous variable codes, propagation of error from one oscillator to another is not necessarily a serious problem. More damaging are processes that amplify a small shift of the canonical variables to a large shift. We have described how to implement a universal set of fault-tolerant quantum gates; with these, harmful error amplification can be avoided as the encoded state is processed.

Apart from encouraging the intriguing possibility that continuous quantum variables might prove useful for the construction of robust quantum memories and computers, these new quantum codes also have important theoretical applications. In this paper we have discussed an application to the theory of the quantum capacity of the Gaussian quantum channel. Furthermore, quantum codes can be invoked to investigate the efficacy of quantum cryptographic protocols, even in cases where the protocol makes no direct use of the encoded states [35]. With continuous-variable codes, we can demonstrate the security of key distribution protocols based on the transmission of continuous variable quantum information. This application is discussed in a separate paper [36].

ACKNOWLEDGMENTS

We gratefully acknowledge helpful discussions with Isaac Chuang, Sumit Daftuar, David DiVincenzo, Andrew Doherty, Steven van Enk, Jim Harrington, Jeff Kimble, Andrew Landahl, Hideo Mabuchi, Harsh Mathur, Gerard Milburn, Michael Nielsen, and Peter Shor. This work was supported in part by the Department of Energy under Grant No. DE-FG03-92-ER40701, and by the Caltech MURI Center for Quantum Networks under ARO Grant No. DAAD19-00-1-0374. Some of this work was done at the Aspen Center for Physics.

[1] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[2] A. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[3] E. Knill, R. Laflamme, and G. Milburn, Nature (London) (London) **409**, 46-52 (2001); e-print quant-ph/0006088.
[4] E. Knill, R. Laflamme, and G. Milburn, e-print quant-ph/0006120.
[5] E. Knill, e-print quant-ph/9608048; E. Knill, e-print quant-ph/9608049.
[6] H. F. Chau, Phys. Rev. A **55**, R839 (1997); H. F. Chau, *ibid.* **56**, R1 (1997).
[7] E. M. Rains, e-print quant-ph/9703048.
[8] D. Gottesman, Lect. Notes. Comp. Sci. **1509**, 302 (1999).
[9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[10] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[11] S. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
[12] S. Lloyd and J. E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).
[13] S. Parker, S. Bose, and M. B. Plenio, Phys. Rev. A **61**, 032305 (2000).
[14] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 4002 (2000); L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. A **62**, 032304 (2000).
[15] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[16] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[17] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1998), p. 176, e-print quant-ph/9611025; D. Aharonov and M. Ben-Or, e-print quant-ph/9906129.
[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[19] A. S. Holevo and R. F. Werner, e-print quant-ph/9912067.
[20] S. Lloyd, Phys. Rev. A **56**, 1613 (1997).
[21] B. W. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[22] H. Barnum, M. A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).
[23] P. W. Shor, in *Proceedings of the 37th Annual Symphony on Foundations of Computer Science* (IEEE, Los Alamitos, CA, 1996), p. 56.
[24] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[25] A. Steane, Phys. Rev. Lett. **78**, 2252 (1997).
[26] E. Knill, R. Laflamme, and W. H. Zurek, Proc. R. Soc. London, Ser. A **454**, 365 (1998).
[27] D. Gottesman and I. Chuang, Nature (London) **402**, 390 (1999),
[28] S. Schneider, H. M. Wiseman, W. J. Munro, and G. J. Milburn, Fortschr. Physik **46**, 391 (1998).
[29] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, Inf. Process. Lett. **75**, 101 (2000).
[30] X. Zhou, D. W. Leung, and I. L. Chuang, Phys. Rev. A **62**, 052316 (2000).
[31] A. Yu. Kitaev (unpublished).
[32] E. Dennis, e-print quant-ph/9905027.
[33] V. Giovannetti, S. Mancini, and P. Tombesi, e-print quant-ph/0005066, and references therein.
[34] A. Yu. Kitaev, e-print quant-ph/9707021.
[35] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[36] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).