# Achievable rates for the Gaussian quantum channel

Jim Harrington* and John Preskill†
*Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125*
(Received 17 May 2001; published 8 November 2001)

We study the properties of quantum stabilizer codes that embed a finite-dimensional protected code space in an infinite-dimensional Hilbert space. The stabilizer group of such a code is associated with a symplectically integral lattice in the phase space of $2N$ canonical variables. From the existence of symplectically integral lattices with suitable properties, we infer a lower bound on the quantum capacity of the Gaussian quantum channel that matches the one-shot coherent information optimized over Gaussian input states.

DOI: 10.1103/PhysRevA.64.062301 PACS number(s): 03.67.Lx

## I. INTRODUCTION

A central problem in quantum information theory is to determine the quantum capacity of a noisy quantum channel—the maximum rate at which coherent quantum information may be transmitted through the channel and recovered with arbitrarily good fidelity [1,2]. A general solution to the corresponding problem for classical noisy channels was found by Shannon in the pioneering paper that launched classical information theory [3,4]. With the development of the theory of quantum error correction [5,6], considerable progress has been made toward characterizing the quantum channel capacity [7], but it remains less well understood than the classical capacity.

The asymptotic coherent information has been shown to provide an upper bound on the capacity [8,9] and a matching lower bound has been conjectured, but not proven [10]. Unfortunately, the coherent information is not subadditive [11], so that its asymptotic value is not easily computed. Therefore, it has been possible to verify the coherent information conjecture in just a few simple cases [12].

One quantum channel of considerable intrinsic interest is the Gaussian quantum channel, which might also be simple enough to be analytically tractable, thus providing a fertile testing ground for the general theory of quantum capacities. A simple analytic formula for the capacity of the Gaussian classical channel was found by Shannon [3,4]. The Gaussian quantum channel was studied by Holevo and Werner [13], who computed the one-shot coherent information for Gaussian input states, and derived an upper bound on the quantum capacity.

Lower bounds on the quantum capacity of the Gaussian quantum channel were established by Gottesman, Kitaev, and Preskill [14]. They developed quantum error-correcting codes that protect a finite-dimensional subspace of an infinite-dimensional Hilbert space, and showed that these codes may be used to transmit high-fidelity quantum information at a nonzero asymptotic rate. In this paper, we continue the study of the Gaussian quantum channel begun in [14]. Our main result is that the coherent information computed by Holevo and Werner is in fact an achievable rate. This result lends nontrivial support to the coherent information conjecture.

We define the Gaussian quantum channel and review the results of Holevo and Werner [13] in Sec. II. In Sec. III, we describe the stabilizer codes for continuous quantum variables introduced in [14], which are based on the concept of a symplectically integral lattice embedded in phase space. In Secs. IV and V, we apply these codes to the Gaussian quantum channel, and calculate an achievable rate arising from lattices that realize efficient packings of spheres in high dimensions. This achievable rate matches the one-shot coherent information $I_Q$ of the channel in cases where $2^{I_Q}$ is an integer. Rates achieved with concatenated coding are calculated in Sec. VI; these fall short of the coherent information but come close. In Sec. VII, we consider the Gaussian classical channel, and again find that concatenated codes achieve rates close to the capacity. Section VIII contains some concluding comments about the quantum capacity of the Gaussian quantum channel.

## II. THE GAUSSIAN QUANTUM CHANNEL

The Gaussian quantum channel is a natural generalization of the Gaussian classical channel. In the classical case, we consider a channel such that the input $x$ and the output $y$ are real numbers. The channel applies a displacement to the input by distance $\xi$,

$$y = x + \xi, \tag{1}$$

where $\xi$ is a Gaussian random variable with mean zero and variance $\sigma^2$; the probability distribution governing $\xi$ is

$$P(\xi) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\xi^2/2\sigma^2}. \tag{2}$$

Similarly, acting on a quantum system described by canonical variables $q$ and $p$ that satisfy the commutation relation $[q,p] = i\hbar$, we may consider a quantum channel that applies a phase-space displacement described by the unitary operator

$$D(\alpha) = \exp(\alpha a^\dagger + \alpha^* a), \tag{3}$$

where $\alpha$ is a complex number, $[a,a^\dagger] = 1$, and $q$, $p$ may be expressed in terms of $a$ and $a^\dagger$ as

*Email address: jimh@theory.caltech.edu
†Email address: preskill@theory.caltech.edu

 

$$q=\sqrt{\frac{\hbar}{2}}(a+a^\dagger),\quad p=-i\sqrt{\frac{\hbar}{2}}(a-a^\dagger). \tag{4}$$

This quantum channel is Gaussian if $\alpha$ is a complex Gaussian random variable with mean zero and variance $\tilde{\sigma}^2$. In that case, the channel is the superoperator (trace-preserving completely positive map) $\mathcal{E}$ that acts on the density operator $\rho$ according to

$$\rho\to\mathcal{E}(\rho)=\frac{1}{\pi\tilde{\sigma}^2}\int d^2\alpha\, e^{-|\alpha|^2/\tilde{\sigma}^2}D(\alpha)\rho D(\alpha)^\dagger. \tag{5}$$

In other words, the position $q$ and momentum $p$ are displaced independently,

$$q\to q+\xi_q,\quad p\to p+\xi_p, \tag{6}$$

where $\xi_q$ and $\xi_p$ are real Gaussian random variables with mean zero and variance $\sigma^2=\hbar\tilde{\sigma}^2$.

To define the capacity, we consider a channel's $n$th extension. In the classical case, a message is transmitted consisting of the $n$ real variables

$$\vec{x}=(x_1,x_2,\ldots,x_n), \tag{7}$$

and the channel applies the displacement

$$\vec{x}\to\vec{x}+\vec{\xi},\quad \vec{\xi}=(\xi_1,\xi_2,\ldots,\xi_n), \tag{8}$$

where the $\xi_i$'s are independent Gaussian random variables, each with mean zero and variance $\sigma^2$. A code consists of a finite number $m$ of $n$-component input signals

$$\vec{x}^{(a)},\quad a=1,2,\ldots,m \tag{9}$$

and a decoding function that maps output vectors to the index set $\{1,2,\ldots,m\}$. We refer to $n$ as the *length* of the code.

If the input vectors were unrestricted, then for fixed $\sigma^2$ we could easily construct a code with an arbitrarily large number of signals $m$ and a decoding function that correctly identifies the index ($a$) of the input with an arbitrarily small probability of error; even for $n=1$, we merely choose the distance between signals to be large compared to $\sigma$. To obtain an interesting notion of capacity, we impose a constraint on the *average power* of the signal,

$$\frac{1}{n}\sum_i (x_i^{(a)})^2\leqslant P, \tag{10}$$

for each $a$. We say that a rate $R$ (in bits) is achievable with power constraint $P$ if there is a sequence of codes satisfying the constraint such that the $\beta$th code in the sequence contains $m_\beta$ signals with length $n_\beta$, where

$$R=\lim_{\beta\to\infty}\frac{1}{n_\beta}\log_2 m_\beta, \tag{11}$$

and the probability of a decoding error vanishes in the limit $\beta\to\infty$. The capacity of the channel with power constraint $P$ is the supremum of all achievable rates.

The need for a constraint on the signal power to define the capacity of the Gaussian classical channel may be understood on dimensional grounds. The classical capacity (in bits) is a dimensionless function of the variance $\sigma^2$, but $\sigma^2$ has dimensions. Another quantity with the dimensions of $\sigma^2$ is needed to construct a dimensionless variable, and the power $P$ fills this role.

In contrast, no power constraint is needed to define the quantum capacity of the quantum channel. Rather, Planck's constant $\hbar$ enables us to define a dimensionless variance $\tilde{\sigma}^2=\sigma^2/\hbar$, and the capacity is a function of this quantity. In the quantum case, a code consists of an encoding superoperator that maps an $m$-dimensional Hilbert space $\mathcal{H}_m$ into the infinite-dimensional Hilbert space $\mathcal{H}^{\otimes N}$ of $N$ canonical quantum systems, and a decoding superoperator that maps $\mathcal{H}^{\otimes N}$ back to $\mathcal{H}_m$. We say that the rate $R$ (in qubits) is achievable if there is a sequence of codes such that

$$R=\lim_{\beta\to\infty}\frac{1}{N_\beta}\log_2 m_\beta, \tag{12}$$

where arbitrary states in $\mathcal{H}_m$ may be recovered with a fidelity that approaches 1 as $\beta\to\infty$. The quantum capacity $C_Q$ of the channel is defined as the supremum of all achievable rates.

Holevo and Werner [13] studied a more general Gaussian channel that includes damping or amplification as well as displacement. However, we will confine our attention in this paper to channels that apply only displacements. Holevo and Werner derived a general upper bound on the quantum capacity by exploiting the properties of the "diamond norm" (norm of complete boundedness) of a superoperator. The diamond norm is defined as follows: First, we define the trace norm of an operator $X$ as

$$\|X\|_{\rm tr}\equiv{\rm tr}\sqrt{X^\dagger X}, \tag{13}$$

which for a self-adjoint operator is just the sum of the absolute values of the eigenvalues. Then a norm of a superoperator $\mathcal{E}$ may be defined as

$$\|\mathcal{E}\|_{\rm so}=\sup_{X\neq 0}\frac{\|\mathcal{E}(X)\|_{\rm tr}}{\|X\|_{\rm tr}}. \tag{14}$$

The superoperator norm is not stable with respect to appending an ancillary system on which $\mathcal{E}$ acts trivially. Thus, we define the diamond norm of $\mathcal{E}$ as

$$\|\mathcal{E}\|_\diamond=\sup_n\|\mathcal{E}\otimes I_n\|_{\rm so}, \tag{15}$$

where $I_n$ denotes the $n$-dimensional identity operator. (This supremum is always attained for some $n$ no larger than the dimension of the Hilbert space on which $\mathcal{E}$ acts.) Holevo and Werner showed that the quantum capacity obeys the upper bound

$$C_Q(\mathcal{E})\leqslant\log_2\|\mathcal{E}\circ T\|_\diamond, \tag{16}$$

where $T$ is the transpose operation defined with respect to some basis. In the case of the Gaussian quantum channel, they evaluated this expression, obtaining

$$C_Q(\sigma^2) \leqslant \log_2(\hbar/\sigma^2) \tag{17}$$

for $\hbar/\sigma^2 > 1$, and $C_Q(\sigma^2)=0$ for $\hbar/\sigma^2 \leqslant 1$.

Holevo and Werner [13] also computed the *coherent information* of the Gaussian quantum channel for a Gaussian input state. To define the coherent information of the channel $\mathcal{E}$ with input density operator $\rho$, one introduces a reference system $R$ and a *purification* of $\rho$, a pure state $|\Phi\rangle$ such that

$$\mathrm{tr}_R(|\Phi\rangle\langle\Phi|)=\rho. \tag{18}$$

Then the coherent information $I_Q$ is

$$I_Q(\mathcal{E},\rho)=S(\mathcal{E}(\rho))-S(\mathcal{E}\otimes I_R(|\Phi\rangle\langle\Phi|)), \tag{19}$$

where $S$ denotes the Von Neumann entropy,

$$S(\rho)=-\mathrm{tr}(\rho\log_2\rho). \tag{20}$$

It is *conjectured* [10,8,9] that the quantum capacity is related to the coherent information by

$$C_Q(\mathcal{E})=\lim_{n\to\infty}\frac{1}{n}C_n(\mathcal{E}), \tag{21}$$

where

$$C_n(\mathcal{E})=\sup_{\rho} I_Q(\mathcal{E}^{\otimes n},\rho). \tag{22}$$

Unlike the mutual information that defines the classical capacity, the coherent information is not subadditive in general, and therefore, the quantum capacity need not coincide with the ''one-shot'' capacity $C_1$. Holevo and Werner showed that for the Gaussian quantum channel, the supremum of $I_Q$ over Gaussian input states is

$$(I_Q)_{\max}=\log_2(\hbar/e\sigma^2), \tag{23}$$

(where $e=2.71828,\ldots,$) for $\hbar/e\sigma^2>1$, and $(I_Q)_{\max}=0$ for $\hbar/e\sigma^2\leqslant 1$. According to the coherent-information conjecture, Eq. (23) should be an achievable rate.

## III. QUANTUM ERROR-CORRECTING CODES FOR CONTINUOUS QUANTUM VARIABLES

The lattice codes developed in [14] are stabilizer codes [15,16] that embed a finite-dimensional code space in the infinite-dimensional Hilbert space of $N$ ''oscillators,'' a system described by $2N$ canonical variables $q_1,q_2,\ldots q_N,p_1,p_2,\ldots,p_N$. That is, the code space is the simultaneous eigenstate of $2N$ commuting unitary operators, the generators of the code's stabilizer group. Each stabilizer generator is a *Weyl operator*, a displacement in the $2N$-dimensional phase space.

Such displacements may be parametrized by $2N$ real numbers $\alpha_1,\alpha_2,\ldots,\alpha_N,\beta_1,\beta_2,\ldots,\beta_N$, and expressed as

$$U(\alpha,\beta)=\exp\left[i\sqrt{2\pi}\left(\sum_{i=1}^{N}\alpha_i p_i+\beta_i q_i\right)\right]. \tag{24}$$

Two such operators obey the commutation relation

$$U(\alpha,\beta)U(\alpha',\beta')=e^{2\pi i\omega(\alpha\beta,\alpha'\beta')}U(\alpha',\beta')U(\alpha,\beta), \tag{25}$$

where

$$\omega(\alpha\beta,\alpha'\beta')\equiv\alpha\cdot\beta'-\alpha'\cdot\beta \tag{26}$$

is the symplectic form. Thus, Weyl operators commute if and only if their symplectic form is an integer.

The $2N$ generators of a stabilizer code are commuting Weyl operators

$$U(\alpha^{(a)},\beta^{(a)}),\quad a=1,2,\ldots,2N. \tag{27}$$

Thus, the elements of the stabilizer group are in one-to-one correspondence with the points of a lattice $\mathcal{L}$ generated by the $2N$ vectors $v^{(a)}=(\alpha^{(a)},\beta^{(a)})$. These vectors may be assembled into the generator matrix $M$ of $\mathcal{L}$ given by

$$M=\begin{pmatrix} v^{(1)} \\ v^{(2)} \\ \cdot \\ \cdot \\ v^{(2N)} \end{pmatrix}. \tag{28}$$

Then the requirement that the stabilizer generators commute, through Eq. (25), becomes the condition that the antisymmetric matrix

$$A=M\omega M^T \tag{29}$$

has integral entries, where $M^T$ denotes the transpose of $M$, $\omega$ is the $2N\times 2N$ matrix

$$\omega=\begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix}, \tag{30}$$

and $I_N$ is the $N\times N$ identity matrix. If the generator matrix $M$ of a lattice $\mathcal{L}$ has the property that $A$ is an integral matrix, then we will say that the lattice $\mathcal{L}$ is *symplectically integral*.

Encoded operations that preserve the code subspace are associated with the code's *normalizer* group, the group of phase-space translations that commute with the code stabilizer. The generator matrix of the normalizer is a matrix $M^\perp$ that may be chosen to be

$$M^\perp=A^{-1}M, \tag{31}$$

so that

$$M^\perp\omega M^T=I; \tag{32}$$

and

$$(M^\perp)\omega(M^\perp)^T=(A^{-1})^T. \tag{33}$$

We will refer to the lattice generated by $M^{\perp}$ as the *symplectic dual* $\mathcal{L}^{\perp}$ of the lattice $\mathcal{L}$.

Another matrix that generates the same lattice as $M$ (and therefore defines a different set of generators for the same stabilizer group) is

$$M' = RM, \tag{34}$$

where $R$ is an integral matrix with $\det R = \pm 1$. This replacement changes the matrix $A$ according to

$$A \to RAR^T. \tag{35}$$

By Gaussian elimination, an $R$ may be constructed such that

$$A = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}, \tag{36}$$

and

$$(A^{-1})^T = \begin{pmatrix} 0 & D^{-1} \\ -D^{-1} & 0 \end{pmatrix}, \tag{37}$$

where $D$ is a positive diagonal integral $N \times N$ matrix. In the important special case of a *symplectically self-dual* lattice, both $A$ and $(A^{-1})^T$ are integral matrices; therefore $D = D^{-1}$ and the standard form of $A$ is

$$A = \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix} = \omega. \tag{38}$$

Hence, the generator matrix of a symplectically self-dual lattice may be chosen to be a real symplectic matrix: $M\omega M^T = \omega$.

If the lattice is rotated, then the generator matrix is transformed as

$$M \to MO, \tag{39}$$

where $O$ is an orthogonal matrix. Therefore, it is convenient to characterize a lattice with its Gram matrix

$$G = MM^T, \tag{40}$$

which is symmetric, positive, and rotationally invariant. In the case of a symplectically self-dual lattice, the Gram matrix $G$ may be chosen to be symplectic, and two symplectic Gram matrices $G$ and $G'$ describe the same lattice if

$$G' = RGR^T, \tag{41}$$

where $R$ is symplectic and integral. Therefore, the moduli space of symplectically self-dual lattices in $2N$ dimensions may be represented as

$$\mathcal{A}_N = H(2N)/Sp(2N,\mathbb{Z}), \tag{42}$$

where $H(2N)$ denotes the space of real symplectic positive $2N \times 2N$ matrices of determinant 1 and $SP(2N,\mathbb{Z})$ denotes the space of integral symplectic $2N \times 2N$ matrices. The space $\mathcal{A}_N$ may also be identified as the moduli space of principally polarized abelian varieties in complex dimension $N$ [17].

The encoded operations that preserve the code space but act trivially within the code space comprise the quotient group $\mathcal{L}^{\perp}/\mathcal{L}$. The order of this group, the ratio of the volume of the unit cell of $\mathcal{L}$ to that of $\mathcal{L}^{\perp}$, is $m^2$, where $m$ is the dimension of the code space. The volume of the unit cell of $\mathcal{L}$ is $|\det M| = |\det A|^{1/2}$ and the volume of the unit cell of $\mathcal{L}^{\perp}$ is $|\det M^{\perp}| = |\det A|^{-1/2}$; therefore, the dimension of the code space is

$$m = |\mathrm{Pf}\, A| = |\det M| = \det D, \tag{43}$$

where $\mathrm{Pf}\, A$ denotes the Pfaffian of $A$, the square root of its determinant. Thus, a symplectically self-dual lattice, for which $|\det M| = |\det M^{\perp}| = 1$, corresponds to a code with a one-dimensional code space. Given a $2N \times 2N$ generator matrix $M$ of a symplectically self-dual lattice, we can rescale it as

$$M \to \sqrt{\lambda} M, \tag{44}$$

where $\lambda$ is an integer, to obtain the generator matrix of a symplectically integral lattice corresponding to a code of dimension

$$m = \lambda^N. \tag{45}$$

The rate of this code, then, is

$$R = \log_2 \lambda. \tag{46}$$

When an encoded state is subjected to the Gaussian quantum channel, a phase-space displacement

$$(\vec{q},\vec{p}) \to (\vec{q},\vec{p}) + (\vec{\xi}_q,\vec{\xi}_p) \tag{47}$$

is applied. To diagnose and correct this error, the eigenvalues of all stabilizer generators are measured, which determines the value of $(\vec{\xi}_q,\vec{\xi}_p)$ modulo the normalizer lattice $\mathcal{L}^{\perp}$. To recover, a displacement of minimal length is applied that returns the stabilizer eigenvalues to their standard values, and so restores the quantum state to the code space. We may associate with the origin of the normalizer lattice its *Voronoi cell*, the set of points in $\mathbb{R}^{2N}$ that are closer to the origin than to any other lattice site. Recovery is successful if the applied displacement lies in this Voronoi cell. Thus, we may estimate the likelihood of a decoding error by calculating the probability that the displacement lies outside the Voronoi cell.

## IV. ACHIEVABLE RATES FROM EFFICIENT SPHERE PACKINGS

One way to establish an achievable rate for the Gaussian quantum channel is to choose a normalizer lattice $\mathcal{L}^{\perp}$ whose shortest nonzero vector is sufficiently large. In this section, we calculate an achievable rate by demanding that the Voronoi cell surrounding the origin contain all typical displacements of the origin in the limit of large $N$. In Sec. V, we will use a more clever argument to improve our estimate of the rate.

The volume of a sphere with unit radius in $n$ dimensions is

$$V_n = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}, \tag{48}$$

and from the Stirling approximation we find that

$$V_n \leqslant \left(\frac{2\pi e}{n}\right)^{n/2}. \tag{49}$$

It was shown by Minkowski [18,19], that lattice sphere packings exist in $n$ dimensions that fill a fraction at least $1/2^{(n-1)}$ of space. Correspondingly, if the lattice is chosen to be unimodular, so that its unit cell has unit volume, then kissing spheres centered at the lattice sites may be chosen to have a radius $r_n$ such that

$$V_n (r_n)^n \geqslant 2^{-(n-1)}, \tag{50}$$

or

$$r_n^2 \geqslant \frac{1}{4}(2/V_n)^{2/n} \geqslant \frac{n}{8\pi e}. \tag{51}$$

This lower bound on the efficiency of sphere packings has never been improved in the nearly 100 years since Minkowski's result. More recently, Buser and Sarnak [17] have shown that this same lower bound applies to lattices that are symplectically self dual.

Now consider the case of $n=2N$-dimensional phase space. For sufficiently large $n$, the channel will apply a phase-space translation by a distance that with high probability will be less than $\sqrt{n(\sigma^2+\varepsilon)}$, for any positive $\varepsilon$. Therefore, a code that may correct a shift this large will correct all likely errors. What rate can such a code attain? If the code is a lattice stabilizer code, and the dimension of the code space is $m$, then the unit cell of the code's normalizer lattice has volume

$$\Delta = \frac{1}{m} \times (2\pi\hbar)^N. \tag{52}$$

Nonoverlapping spheres centered at the sites of the normalizer lattice may be chosen to have radius $r=\sqrt{n(\sigma^2+\varepsilon)}$, where

$$\left(\frac{2\pi e}{n}\right)^{n/2} [n(\sigma^2+\varepsilon)]^{n/2} \geqslant \frac{1}{m} \times 2^{-n} \times (2\pi\hbar)^{n/2}, \tag{53}$$

or

$$m \geqslant \left(\frac{\hbar}{4e(\sigma^2+\varepsilon)}\right)^N. \tag{54}$$

The error probability becomes arbitrarily small for large $N$ if Eq. (54) is satisfied, for any positive $\varepsilon$. We conclude that the rate

$$R \equiv \frac{1}{N}\log_2 m = \log_2\left(\frac{\hbar}{4e\sigma^2}\right), \tag{55}$$

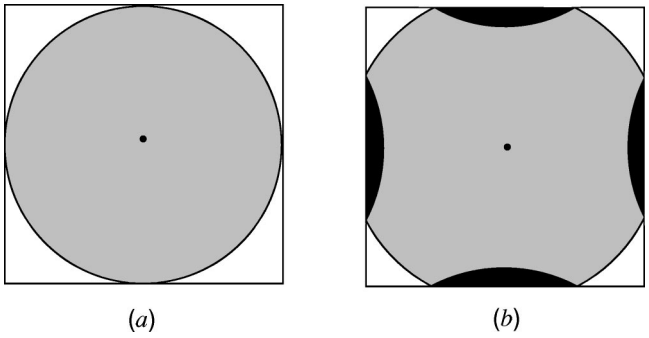

FIG. 1. Two ways to estimate the rate achieved by a lattice code. Each site of the normalizer lattice has a Voronoi cell (represented here by a square) containing all points that are closer to that site than any other site. Displacements that move a site to a position within its Voronoi cell may be corrected. The volume of the Voronoi cell determines the rate of the code. In (a), the ball containing typical displacements lies within the cell, so that the error probability is small. In (b), the ball of typical displacements is not completely contained within the cell, but the region where neighboring balls overlap (shown in black) has a small volume, so that the error probability is still small.

is achievable, provided $\hbar/4e\sigma^2 \geqslant 1$. However, as noted in Sec. III, the rates that may be attained by this construction (rescaling of a symplectically self-dual lattice) are always of the form $\log_2 \lambda$, where $\lambda$ is an integer.

## V. IMPROVING THE RATE

The achievable rate found in Eq. (55) falls two qubits short of the coherent information Eq. (23). We will now show that this gap may be closed by using tighter estimates of the error probability. We established Eq. (55) by filling phase space with nonoverlapping spheres, which is overly conservative. It is acceptable for the spheres to overlap, as long as the overlaps occupy an asymptotically negligible fraction of the total volume, as suggested in Fig. 1.

Our improved estimate applies another result obtained by Buser and Sarnak [17]. They note that the moduli space of symplectically self-dual lattices is compact and equipped with a natural invariant measure. Therefore, it makes sense to consider averaging over all lattices. Denote by $\langle \cdot \rangle$ the average over all symplectically self-dual lattices with specified dimension $n=2N$, and let $f(x)$ denote an integrable rotationally invariant function of the vector $x$ (that is a function of the length $|x|$ of $x$). Then, Buser and Sarnak [17] show that

$$\left\langle \sum_{x \in \mathcal{L}\setminus\{0\}} f(x) \right\rangle = \int f(x) d^n x. \tag{56}$$

(Note that the sum is over all *nonzero* vectors in the lattice $\mathcal{L}$.) It follows that there must exist a *particular* symplectically self-dual lattice $\mathcal{L}$ such that

$$\sum_{x \in \mathcal{L}\setminus\{0\}} f(x) \leqslant \int f(x) d^n x. \tag{57}$$

The statement that a *unimodular* lattice exists that satisfies Eq. (57) is the well-known Minkowski-Hlawka theorem [19]. Buser and Sarnak established the stronger result that the lattice may be chosen to be symplectically self dual.

We may use this result to bound the probability of a decoding error, and establish that a specified rate is achievable. Our argument will closely follow de Buda [20], who performed a similar analysis of lattice codes for the Gaussian classical channel. However, the quantum case is considerably easier to analyze, because we can avoid complications arising from the power constraint [21–23].

A decoding error occurs if the channel displaces the origin to a point outside the Voronoi cell centered at the origin. The Voronoi cell has a complicated geometry, so that the error probability is not easy to analyze. But, we may simplify the analysis with a trick [20]. Imagine drawing a sphere with radius

$$a=\sqrt{n(\sigma^2+\varepsilon)} \tag{58}$$

around each lattice site, where $\varepsilon>0$; this value of $a$ is chosen so that the typical displacement introduced by the channel has a length less than $a$; the probability of a shift larger than $a$ thus becomes negligible for large $n$. It may be that these spheres overlap. However, a vector that is contained in the sphere centered at the origin, and is not contained in the sphere centered at any other lattice site, must be closer to the origin than any other lattice site. Therefore, the vector is contained in the origin's Voronoi cell, and is a shift that may be corrected successfully. (See Fig. 1.)

Hence (ignoring the possibility of an atypical shift by $\xi>a$) we can upper bound the probability of error by estimating the probability that the shift moves any other lattice site into the sphere of radius $a$ around the origin. We then find

$$P_{\text{error}}\leqslant \sum_{x\in\mathcal{L}^{\perp}\setminus\{0\}} \int_{|r|\leqslant a} P(x-r)d^n r, \tag{59}$$

where $P(\xi)$ denotes the probability of a displacement by $\xi$.

The Buser-Sarnak theorem [17] tells us that there exists a lattice whose unit cell has volume $\Delta$, and which is related by rescaling to a symplectically self-dual lattice, such that

$$P_{\text{error}}\leqslant \frac{1}{\Delta}\int d^n x \int_{|r|\leqslant a} P(x-r)d^n r; \tag{60}$$

by interchanging the order of integration, we find that

$$P_{\text{error}}\leqslant \frac{1}{\Delta}V_n a^n, \tag{61}$$

the ratio of the volume of the $n$-dimensional sphere of radius $a$ to the volume of the unit cell.

Now the volume $\Delta$ of the unit cell of the normalizer lattice $\mathcal{L}^{\perp}$, and the dimension $m$ of the code space, are related by

$$\Delta=(2\pi\hbar)^N m^{-1}=(2\pi\hbar\times 2^{-R})^N, \tag{62}$$

where $R$ is the rate, and we may estimate the volume of the sphere as

$$V_n a^n\leqslant\left(\frac{2\pi e}{n}\right)^{n/2}[n(\sigma^2+\varepsilon)]^{n/2}, \tag{63}$$

where $n=2N$. Thus, we conclude that

$$P_{\text{error}}\leqslant\left(\frac{e(\sigma^2+\varepsilon)}{\hbar}\times 2^R\right)^N. \tag{64}$$

Therefore, the error probability becomes small for large $N$ for any rate $R$ such that

$$R<\log_2\left(\frac{\hbar}{e(\sigma^2+\varepsilon)}\right), \tag{65}$$

where $\varepsilon$ may be arbitrarily small. We conclude that the rate

$$R=\log_2\left(\frac{\hbar}{e\sigma^2}\right) \tag{66}$$

is achievable in the limit $N\to\infty$, provided that $\hbar/e\sigma^2>1$. This rate matches the optimal value Eq. (23) of the one-shot coherent information for Gaussian inputs. We note, again, that the rates that we obtain from rescaling a symplectically self-dual lattice are restricted to $R=\log_2\lambda$, where $\lambda$ is an integer. Thus, for specified $\sigma^2$, the achievable rate that we have established is really the maximal value of

$$R=\log_2\lambda,\quad \lambda\in\mathbb{Z}, \tag{67}$$

such that the positive integer $\lambda$ satisfies

$$\lambda<\frac{\hbar}{e\sigma^2}. \tag{68}$$

## VI. ACHIEVABLE RATES FROM CONCATENATED CODES

Another method for establishing achievable rates over the Gaussian quantum channel was described in [14], based on *concatenated coding*. In each of $N$ "oscillators" described by canonical variables $p_i$ and $q_i$, a $d$-dimensional system ("qudit") is encoded that is protected against sufficiently small shifts in $p_i$ and $q_i$. The encoded qudit is associated with a square lattice in two-dimensional phase space. Then, a stabilizer code is constructed that embeds a $k$-qudit code space in the Hilbert space of $N$ qudits; these $k$ encoded qudits are protected if a sufficiently small fraction of the $N$ qudits are damaged. Let us compare the rates achieved by concatenated codes to the rates achieved with codes derived from efficient sphere packings.

We analyze the effectiveness of concatenated codes in two stages. First, we consider how likely each of the $N$ qudits is to sustain damage if the underlying oscillator is subjected to the Gaussian quantum channel. The area of the unit cell of the two-dimensional square normalizer lattice that represents the encoded operations acting on the qudit is $2\pi\hbar/d$, and the minimum distance between lattice sites is $\delta=\sqrt{2\pi\hbar/d}$. A

displacement of $q$ by $a\delta$, where $a$ is an integer, is the operation $X^a$ acting on the code space, and a displacement of $p$ by $b\delta$ is the operation $Z^b$, where $X$ and $Z$ are the Pauli operators acting on the qudit; these act on a basis $\{|j\rangle, j=0,1,2,\ldots,d-1\}$ for the qudit according to

$$X:|j\rangle\rightarrow|j+1 \pmod d\rangle,$$

$$Z:|j\rangle\rightarrow\omega^j|j\rangle, \tag{69}$$

where $\omega=\exp(2\pi i/d)$.

Shifts in $p$ or $q$ may be corrected successfully provided that they satisfy

$$|\Delta q|<\delta/2=\sqrt{\frac{\pi\hbar}{2d}}, \quad |\Delta p|<\delta/2=\sqrt{\frac{\pi\hbar}{2d}}. \tag{70}$$

If the shifts in $q$ and $p$ are Gaussian random variables with variance $\sigma^2$, then the probability that a shift causes an uncorrectable error is no larger than the probability that the shift exceeds $\sqrt{\pi\hbar/2d}$, or

$$p_X,p_Z\leqslant 2\frac{1}{\sqrt{2\pi\sigma^2}}\int_{\sqrt{\pi\hbar/2d}}^{\infty}dx\, e^{-x^2/2\sigma^2}$$

$$=\mathrm{erfc}(\sqrt{\pi\hbar/4d\sigma^2}), \tag{71}$$

where erfc denotes the complementary error function. Here, $p_X$ is the probability of an "$X$ error" acting on the qudit, of the form $X^a$ for $a\not\equiv 0 \pmod d$, and $p_Z$ denotes the probability of a "$Z$ error" of the form $Z^b$ for $b\not\equiv 0 \pmod d$. The $X$ and $Z$ errors are uncorrelated, and errors with $a,b=\pm 1$ are much more likely than errors with $|a|,|b|>1$. By choosing $d\sim\hbar/\sigma^2$, we may achieve a small error probability for each oscillator.

The second stage of the argument is to determine the rate that may be achieved by a qudit code if $p_X,p_Z$ satisfy Eq. (71). We will consider codes of the Calderbank-Shor-Steane (CSS) type, for which the correction of $X$ errors and $Z$ errors may be considered separately [24,25]. A CSS code is a stabilizer code, in which each stabilizer generator is either a tensor product of $I$'s and powers of $Z$ (measuring these generators diagnoses the $X$ errors) or a tensor product of $I$'s and powers of $X$ (for diagnosing the $Z$ errors).

We can establish an achievable rate by averaging the error probability over CSS codes; we give only an informal sketch of the argument. Suppose that we fix the block size $N$ and the number of encoded qudits $k$. Now select the generators of the code's stabilizer group at random. About half of the $N-k$ generators are of the $Z$ type and about half are of the $X$ type. Thus, the number of possible values for the eigenvalues of the generators of each type is about

$$d^{(N-k)/2}. \tag{72}$$

Now, we can analyze the probability that an uncorrectable $X$ error afflicts the encoded quantum state (the probability of an uncorrectable $Z$ error is analyzed in exactly the same way). Suppose that $X$ errors act independently on the $N$ qudits in the block, with a probability of error per qudit of $p_X$. Thus, for large $N$, the typical number of damaged qudits is close to $p_XN$. A damaged qudit may be damaged in any of $d-1$ different ways [$X^a$, where $a=1,2,\ldots,(d-1)$]. We will suppose, pessimistically, that all $d-1$ shifts of the qudit are equally likely. The actual situation that arises in our concatenated coding scheme is more favorable—small values of $|a|$ are more likely—but our argument will not exploit this feature.

Thus, with high probability, the error that afflicts the block will belong to a typical set of errors that contains a number of elements close to

$$N_{\mathrm{typ}}\sim\binom{N}{Np_X}(d-1)^{Np_X}\sim d^{N[H_d(p_X)+p_X\log_d(d-1)]}, \tag{73}$$

where

$$H_d(p)=-p\log_d p-(1-p)\log_d(1-p). \tag{74}$$

If a particular typical error occurs, then recovery will succeed as long as there is no other typical error that generates the same error syndrome. It will be highly unlikely that another typical error has the same syndrome as the actual error, provided that the number of possible error syndromes $d^{(N-k)/2}$ is large compared to the number of typical errors. Therefore, the $X$ errors may be corrected with high probability for

$$\frac{1}{2}\left(1-\frac{k}{N}\right)>\frac{1}{N}\log_d N_{\mathrm{typ}}\sim H_d(p_X)+p_X\log_d(d-1), \tag{75}$$

or for a rate $R_d$ in qudits satisfying

$$R_d\equiv\frac{k}{N}<1-2H_d(p_X)-2p_X\log_d(d-1). \tag{76}$$

Similarly, the $Z$ errors may be corrected with high probability by a random CSS code if the rate satisfies

$$R_d<1-2H_d(p_Z)-2p_Z\log_d(d-1). \tag{77}$$

Converted to qubits, the rate becomes

$$R=(\log_2 d)R_d. \tag{78}$$

Under these conditions, the probability of error averaged over CSS codes becomes arbitrarily small for $N$ large. It follows that there is a particular sequence of CSS codes with rate approaching Eqs. (76)–(78), and error probability going to zero in the limit $N\rightarrow\infty$.

For given $\sigma^2$, the optimal rate that may be attained by concatenating a code that encodes a qudit in a single oscillator with a random CSS code, is found by estimating $p_X$ and $p_Z$ using Eq. (71) and then choosing $d$ to maximize the rate $R$ given by Eqs. (76)–(78). The results are shown in Fig. 2. This rate (in qubits) may be expressed as

$$R=\log_2(C^2\hbar/\sigma^2), \tag{79}$$

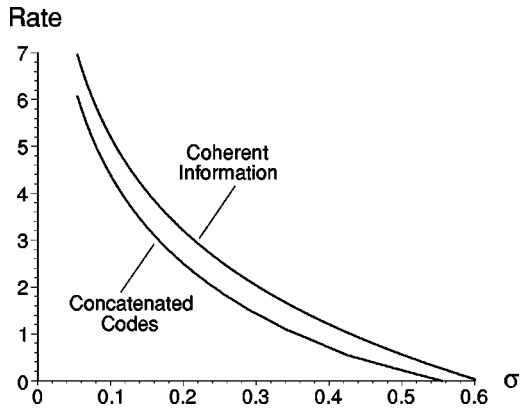


FIG. 2. Rates achieved by concatenated codes, compared to the one-shot coherent information optimized over Gaussian input states. Here, $\sigma$ is the standard deviation of the magnitude of the phase-space displacement introduced by the channel, in units with $\hbar=1$. The rate is in units of qubits per oscillator.

where $C^2$ is a slowly varying function of $\sigma^2/\hbar$ plotted in Fig. 3. It turns out that this rate is actually fairly close to $\log_2 d$; that is, the optimal dimension $d$ of the qudit encoded in each oscillator is approximately $C^2\hbar/\sigma^2$. With this choice for $d$, the error rate for each oscillator is reasonably small, and the random CSS code reduces the error probability for the encoded state to a value exponentially small in $N$ at a modest cost in rate. The rate achieved by concatenating coding lies strictly below the coherent information $I_Q$, but comes within one qubit of $I_Q$ for $\sigma^2 > 1.88\times 10^{-4}$.

Both the concatenated codes and the codes derived from efficient sphere packings are stabilizer codes, and therefore, both are associated with lattices in $2N$-dimensional phase space. But while the sphere-packing codes have been chosen so that the shortest nonzero vector on the lattice is large relative to the size of the unit cell, the concatenated codes correspond to sphere packings of poor quality. For the concatenated codes, the shortest vector of the normalizer lattice has length $\ell$, where

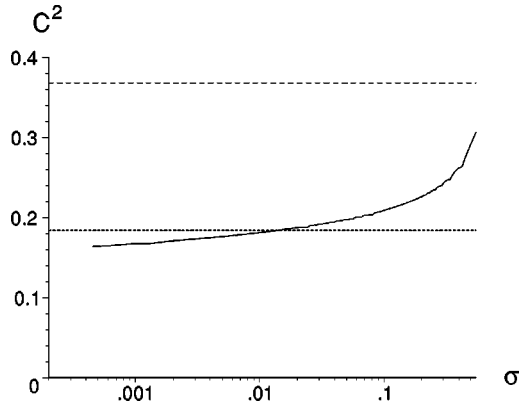


FIG. 3. The slowly varying function $C^2$, defined by $R=\log_2(C^2/\sigma^2)$, where $R$ is the rate achievable with concatenated codes. Units have been chosen such that $\hbar=1$. The horizontal lines are at $C^2=1/e$, corresponding to a rate equal to the coherent information, and at $C^2=1/2e$, corresponding to one qubit below the coherent information.

$$\ell^2 = 2\pi\hbar/d, \tag{80}$$

and the rate $R$ is close to $\log_2 d$. The efficient sphere packings have radius $r=\ell/2$ close to $\sqrt{n\sigma^2}$, or

$$\ell^2 = \frac{8N\hbar}{e}\times 2^{-R}. \tag{81}$$

Hence, if we compare sphere-packing codes and concatenated codes with comparable rates, the sphere-packing codes have minimum distance that is larger by a factor of about $\sqrt{4N/\pi e}$. The concatenated codes achieve a high rate not because the minimum distance of the lattice is large, but rather because the decoding procedure exploits the hierarchical structure of the code.

## VII. THE CLASSICAL GAUSSIAN CHANNEL

We have found that quantum stabilizer codes based on efficient sphere packings can achieve rates for the Gaussian quantum channel that match the one-shot coherent information, and that concatenated codes achieve rates that are below, but close to, the coherent information. Now, as an aside, we will discuss the corresponding statements for the classical Gaussian channel. We will see, in particular, that concatenated codes achieve rates that are close to the classical channel capacity.

Shannon's expression for the capacity of the classical Gaussian channel may be understood heuristically as follows [3,4]. If the input signals have average power $P$, which is inflated by the Gaussian noise to $P+\sigma^2$, then if $n$ real variables are transmitted, the total volume occupied by the space of output signals is the volume of a sphere of radius $\sqrt{n(P+\sigma^2)}$, or

$$V_{tot} = V_n[n(P+\sigma^2)]^{n/2}. \tag{82}$$

We will decode a received message as the signal state that is the minimal distance away. Consider averaging over all codes that satisfy the power constraint and have $m$ signals. When a message is received, the signal that was sent will typically occupy a decoding sphere of radius $\sqrt{n(\sigma^2+\varepsilon)}$ centered at the received message, which has volume

$$V_{\text{decoding sphere}} = V_n[n(\sigma^2+\varepsilon)]^{n/2}. \tag{83}$$

A decoding error may arise if another one of the $m$ signals, aside from the one that was sent, is also contained in the decoding sphere. The probability that a randomly selected signal inside the sphere of radius $\sqrt{n(P+\sigma^2)}$ is contained in a particular decoding sphere of radius $\sqrt{n(\sigma^2+\varepsilon)}$ is the ratio of the volume of the spheres, so the probability of a decoding error may be upper bounded by $m$ times that ratio, or

$$P_{\text{error}} < m\left(\frac{\sigma^2+\varepsilon}{\sigma^2+P}\right)^{n/2} = \left(2^{2R}\frac{\sigma^2+\varepsilon}{\sigma^2+P}\right)^{n/2}, \tag{84}$$

where $R$ is the rate of the code. If the probability of error averaged over codes and signals satisfies this bound, there is a particular code that satisfies the bound when we average

only over signals. If $P_{\text{error}}<\delta$ when we average over signals, then we can discard at most half of all the signals (reducing the rate by at most $1/n$ bits) to obtain a new code with $P_{\text{error}}<2\delta$ for *all* signals. Since $\varepsilon$ may be chosen arbitrarily small for sufficiently large $n$, we conclude that there exist codes with arbitrarily small probability of error and rate $R$ arbitrarily close to

$$C=\frac{1}{2}\log_2\left(1+\frac{P}{\sigma^2}\right), \tag{85}$$

which is the Shannon capacity. Conversely, for any rate exceeding $C$, the decoding spheres inevitably have nonnegligible overlaps, and the error rate cannot be arbitrarily small.

Suppose that, instead of Shannon's random coding, we use a lattice code based on an efficient packing of spheres. In this case, the power constraint may be imposed by including as signals all lattice sites that are contained in an $n$-dimensional ball of radius $\sqrt{nP}$, and the typical shifts by distance $\sqrt{n\sigma^2}$ must be correctable. Thus, decoding spheres of radius $\sqrt{n\sigma^2}$ are to be packed into a sphere of total radius $\sqrt{n(P+\sigma^2)}$. Suppose that the lattice is chosen so that nonoverlapping spheres centered at the lattice sites fill a fraction at least $2^{-(n-1)}$ of the total volume; the existence of such a lattice is established by Minkowski's estimate [18,19]. Then the number $m$ of signals satisfies

$$mV_n(n\sigma^2)^{n/2}\geqslant 2^{-(n-1)}V_n[n(P+\sigma^2)]^{n/2}, \tag{86}$$

or

$$m\geqslant 2^{-n}\left(1+\frac{P}{\sigma^2}\right)^{n/2}, \tag{87}$$

corresponding to the rate

$$R\equiv\frac{1}{n}\log_2 m=\frac{1}{2}\log_2\left(1+\frac{P}{\sigma^2}\right)-1, \tag{88}$$

which is one bit less than the Shannon capacity.

Much as in the discussion of quantum lattice codes in Sec. V, an improved estimate of the achievable rate is obtained if we allow the decoding spheres to overlap [20–23]. In fact, there are classical lattice codes with rate arbitrarily close to the capacity, such that the probability of error, *averaged* over signals, is arbitrarily small [23]. Unfortunately, though, because of the power constraint, the error probability depends on which signal is sent, and the trick of deleting the worst half of the signals would destroy the structure of the lattice. Alternatively, it may be shown that for any rate

$$R<\frac{1}{2}\log_2(P/\sigma^2), \tag{89}$$

there are lattice codes with maximal probability of error that is arbitrarily small [20]. This achievable rate approaches the capacity for large $P/\sigma^2$.

Now consider the rates that may be achieved for the Gaussian classical channel with concatenated coding. A $d$-state system (dit) is encoded in each of $n$ real variables. If each real variable takes one of $d$ possible values, with spacing $2\Delta x$ between the signals, then a shift by $\Delta x$ may be corrected. By replacing the sum over $d$ values by an integral, which may be justified for large $d$, we find an average power per signal

$$P\sim\frac{1}{2d\Delta x}\int_{-d\Delta x}^{d\Delta x}x^2dx=\frac{1}{3}(d\Delta x)^2; \tag{90}$$

thus, the largest correctable shift may be expressed in terms of the average power as

$$\Delta x=\sqrt{3P}/d. \tag{91}$$

For the Gaussian channel with mean zero and variance $\sigma^2$, the probability $p$ of an error in each real variable transmitted is no larger than the probability of a shift by a distance exceeding $\Delta x$, or

$$p\leqslant\operatorname{erfc}(\sqrt{3P/2d^2\sigma^2}), \tag{92}$$

where erfc denotes the complementary error function.

We reduce the error probability further by encoding $k<n$ dits in the block of $n$ dits. Arguing as in Sec. VI, we see that a random code for dits achieves an asymptotic rate in bits given by

$$R=(\log_2 d)[1-H_d(p)-p\log_d(d-1)]. \tag{93}$$

Given $\sigma^2$, using the expression Eq. (92) for $p$, and choosing $d$ to optimize the rate in Eq. (93), we obtain a rate close to the Shannon capacity, as shown in Fig. 4. As for the concatenated quantum code, the rate of the concatenated classical code is close to $\log_2 d$, where $d\sim C(\sigma^2)\sqrt{P/\sigma^2}$, and $C(\sigma^2)$ is a slowly varying function.

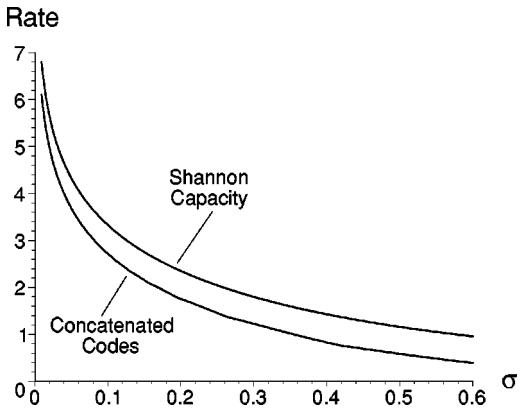


FIG. 4. Rates for the Gaussian classical channel achievable with concatenated codes, compared to the Shannon capacity. Here, $\sigma$ is the standard deviation of the displacement, in units with the power $P=1$. The rate is in units of bits per signal.

## VIII. CONCLUSIONS

We have described quantum stabilizer codes, based on symplectically integral lattices in phase space, that protect quantum information carried by systems described by continuous quantum variables. With these codes, we may estab-

lish lower bounds on the capacities of continuous-variable quantum channels.

For the Gaussian quantum channel, the best rate we know how to achieve with stabilizer coding matches the one-shot coherent information optimized over Gaussian inputs, at least when the value of the coherent information is $\log_2$ of an integer. That our achievable rate matches the coherent information only for isolated values of the noise variance $\sigma^2$ seems to be an artifact of our method of analysis, rather than indicative of any intrinsic property of the channel. Hence, it is tempting to speculate that this optimal one-shot coherent information actually is the quantum capacity of the channel.

Conceivably, better rates may be achieved with *nonadditive* quantum codes that cannot be described in terms of symplectically integral lattices. We do not know much about how to construct these codes, or about their properties.

In the case of the depolarizing channel acting on qubits, Shor and Smolin discovered that rates exceeding the one-shot coherent information could be achieved. Their construction used concatenated codes, where the ''outer code'' is a random stabilizer code, and the ''inner code'' is a degenerate code with a small block size [11]. The analogous procedure for the Gaussian channel would be to concatenate an outer code based on a symplectically integral lattice with an inner code that encodes one logical oscillator in a block of several oscillators. This inner code, then, embeds an infinite-dimensional code space in a larger infinite-dimensional space, as do codes constructed by Braunstein [26] and Lloyd and Slotine [27]. However, we have not been able to find concatenated codes of this type that achieve rates exceeding the one-shot coherent information of the Gaussian channel.

## ACKNOWLEDGMENTS

We thank Dave Beckman, Anne-Marie Bergé, Bob McEliece, Michael Postol, Eric Rains, Peter Shor, and Edward Witten for helpful discussions and correspondence. This work was supported in part by the Department of Energy under Grant No. DE-FG03-92-ER40701, by the National Science Foundation under Grant No. EIA-0086038, and by the Caltech MURI Center for Quantum Networks under ARO Grant No. DAAD19-00-1-0374.

[1] M.A. Nielsen and I.L Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] J. Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation*, http://www.theory.caltech;edu/people/preskill/ph229 (1998).
[3] C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[4] T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
[5] P.W. Shor, Phys. Rev. A **52**, 2493 (1995).
[6] A. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[7] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[8] B.W. Schumacher and M.A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[9] H. Barnum, M.A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).
[10] S. Lloyd, Phys. Rev. A **56**, 1613 (1997).
[11] P.W. Shor and J.A. Smolin, e-print quant-ph/9604006; D.P. DiVincenzo, P.W. Shor, and J.A. Smolin, Phys. Rev. A **57**, 830 (1998).
[12] C.H. Bennett, D.P. DiVincenzo, and J.A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997), quant-ph/9701015.
[13] A.S. Holevo and R.F. Werner, e-print quant-ph/9912067.
[14] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A (to be published), e-print quant-ph/0008040.
[15] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[16] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[17] P. Buser and P. Sarnak, Invent. Math. **117**, 27 (1994).
[18] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups* (Springer, New York, 1999).
[19] J.W.S. Cassels, *An introduction to the Geometry of Numbers* (Springer-Verlag, New York, 1971).
[20] R. de Buda, IEEE Trans. Inf. Theory **IT-21**, 441 (1975).
[21] R. de Buda, IEEE J. Sel. Areas Commun. **7**, 893 (1989).
[22] T. Linder, C. Schleger, and K. Zeger, IEEE Trans. Inf. Theory **39**, 1735 (1993).
[23] R. Urbanke and B. Rimoldi, IEEE Trans. Inf. Theory **44**, 273 (1998).
[24] A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996).
[25] A. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[26] S. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
[27] S. Lloyd and J.E. Slotine, Phys. Rev. Lett. **80**, 4088 (1998).