Good quantum error-correcting codes exist.

A. R. Calderbank and Peter W. Shor

AT&T Research, 600 Mountain Avenue, Murray Hill, NJ 07974

(Submitted September 12, 1995)

Abstract

A quantum error-correcting code is defined to be a unitary mapping (encoding) of k qubits (2-state quantum systems) into a subspace of the quantum state space of n qubits such that if any t of the qubits undergo arbitrary decoherence, not necessarily independently, the resulting n qubits can be used to faithfully reconstruct the original quantum state of the k encoded qubits. Quantum error-correcting codes are shown to exist with asymptotic rate $k/n = 1 - 2H_2(2t/n)$ where $H_2(p)$ is the binary entropy function $-p \log_2 p - (1-p) \log_2 (1-p)$. Upper bounds on this asymptotic rate are given.

03.65.Bz

I. INTRODUCTION

With the realization that computers that use the interference and superposition principles of quantum mechanics might be able to solve certain problems, including prime factorization, exponentially faster than classical computers [1], interest has been growing in the feasibility of these quantum computers, and several methods for building quantum gates and quantum computers have been proposed [2,3]. One of the most cogent arguments against the feasibility of quantum computation appears to be the difficulty of eliminating error caused by inaccuracy and decoherence [4]. Whereas the best experimental implementations of quantum gates accomplished so far have less than 90% accuracy [5], the accuracy required for factorization of numbers large enough to be difficult on conventional computers appears to be closer to one part in billions. We hope that the techniques investigated in this paper can eventually be extended so as to reduce this quantity by several orders of magnitude.

In the storage and transmission of digital data, errors can be corrected by using error-correcting codes [6]. In digital computation, errors can be corrected by using redundancy; in fact, it has been shown that fairly unreliable gates could be assembled to form a reliable computer [7]. It has widely been assumed that the quantum no-cloning theorem [8] makes error correction impossible in quantum communication and computation because redundancy cannot be obtained by duplicating quantum bits. This argument was shown to be in error for quantum communication in Ref. [9], where a code was given that mapped one qubit (two-state quantum system) into nine qubits so that the original qubit could be recovered perfectly even after arbitrary decoherence of any one of these nine qubits. This gives a quantum code on 9 qubits with rate $\frac{1}{9}$ that protects against one error. Here we show the existence of better quantum error-correcting codes, having higher information transmission rates and better error-correction capacity. Specifically, we show the existence of quantum error-correcting codes encoding k qubits into n qubits that correct t errors and have asymptotic rate $1-2H_2(2t/n)$ as $n \to \infty$. These codes work not by duplicating the quantum state of the encoded k qubits, but by spreading it out over all n qubits so that if t or fewer of these qubits are measured, no information about the quantum state of the encoded bits is revealed and, in fact, the quantum state can be perfectly recovered from the remaining $n-t$ qubits.

Suppose that we have a coherent quantum state of k qubits that we wish to store using a physical quantum system which is subject to some decoherence process. For example, during computation on the quantum computer proposed by Cirac and Zoller [3], we would need to store quantum information in entangled electronic states of ions held in an ion trap. The decoherence time of the quantum state of k entangled qubits is in general $1/k$ of the decoherence time of one qubit (this makes the optimistic assumption that coherence between different qubits is as stable as coherence of a single qubit). Thus, one might expect that the best way to store the state of k entangled qubits is to store them in k physical qubits. Our results show that if we use quantum error-correcting codes, it is possible to store the k qubits in $n > k$ qubits so that the decoherence time for the encoded quantum state is a small constant fraction of the decoherence time of one qubit. These results thus show that some measurable non-local properties of entangled systems are much more stable under decoherence than is the entire entangled system.

Physical quantum channels will be unlikely to leave $n-t$ qubits perfectly untouched and subject the remaining t qubits to decoherence. To analyze the behavior of our error-correcting code for physical quantum channels, we must make some assumptions about the decoherence process. In Section VI, we will show that our error correction method performs well if the decoherence of different qubits occurs independently, i.e., if each of the qubits is coupled to a separate environment. Our error-correction method will actually work for more general channels, as it can tolerate coupled decoherence behavior among small groups of qubits.

The lower bound of $1-2H_2(2t/n)$ shown in our paper should be compared with theoretical upper bounds of

$$\min\left[1-H_2(2t/3n), H_2\left(\tfrac{1}{2}+\sqrt{(1-t/n)t/n}\right)\right]$$

for $t/n < \frac{1}{2}$, and 0 for $t/n \geq \frac{1}{2}$. These are obtained from bounds on the quantum information capacity of a quantum channel, which we derive in Section VI from results of Refs. [10,11]. These bounds are plotted in Fig. 1 in Section VI.

II. DEFINITIONS

Our constructions of quantum error-correcting codes rely heavily on the properties of classical error-correcting codes. We will thus first briefly review certain definitions and properties related to binary linear error-correcting codes. We only consider vectors and codes over F_2, the field of two elements, so we have $1+1=0$. A binary vector $v \in \mathsf{F}_2$ with d 1's is said to have *Hamming weight* d, denoted by $\mathrm{wt}(v) = d$. The *Hamming distance* $d_H(v, w)$ between two binary vectors v and w is $\mathrm{wt}(v+w)$. The *support* of a vector v, denoted by $\mathrm{supp}(v)$, is the set of coordinates of v where the corresponding entry is not 0, that is, $\mathrm{supp}(v) = \{i : v_i \neq 0\}$. Suppose that S is a set of coordinates. Then $v|_S$ denotes the projection of v onto S, i.e., the vector that agrees with v on the coordinates in S and is 0 on the remaining coordinates. For a binary vector E we use $v|_E$ to mean $v|_{\mathrm{supp}(E)}$. We also use $e \preceq E$ to mean that $\mathrm{supp}(e) \subseteq \mathrm{supp}(E)$.

A *code* $\mathcal{C}$ of length n is a set of binary vectors of length n, called *codewords*. In a *linear code* the codewords are those vectors in a subspace of F_2^n (the n-dimensional vector space over the field F_2 on two elements). The *minimum distance* $d = d(\mathcal{C})$ of a binary code $\mathcal{C}$ is the minimum distance between two distinct codewords. If $\mathcal{C}$ is linear then this minimum distance is just the minimum Hamming weight of a nonzero codeword.

A linear code with length n, dimension k, and minimum distance d is called an $[n, k, d]$ code. For a code $\mathcal{C}$ with minimum distance d, any binary vector in F_2^n is within Hamming distance $t = \lfloor \frac{d-1}{2} \rfloor$ of at most one codeword; thus, a code with minimum distance d can correct t errors made in the bits of a codeword; such a code is thus said to be a t error-correcting code. The *rate* R of a linear code of length n is $\dim(\mathcal{C})/n$; this is the ratio of the information content of a codeword to the information content of an arbitrary string of length

n. The *dual code* $\mathcal{C}^\perp$ of a code $\mathcal{C}$ is the set of vectors of perpendicular to all codewords, that is, $\mathcal{C}^\perp = \{v \in \mathsf{F}_2^n : v \cdot c = 0 \ \forall c \in \mathcal{C}\}$. From linear algebra, $\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = n$.

In this paper, we will use the $[7, 4, 3]$ Hamming code as an example to illustrate our construction of quantum error-correcting codes. This code contains the following 16 binary vectors of length 7:

$$\begin{array}{cccc} 0000000, & 0001011, & 0010110, & 0011101, \\ 0100111, & 0101100, & 0110001, & 0111010, \\ 1000101, & 1001110, & 1010011, & 1011000, \\ 1100010, & 1101001, & 1110100, & 1111111. \end{array} \tag{1}$$

The minimum distance is the minimum Hamming weight of a non-zero codeword, which is 3, so this is a one-error correcting code. It is easily verified that the dual code consists of all vectors in the Hamming code with an even weight.

The *quantum Hilbert space* $\mathcal{H}_2^n$ over n qubits is the complex space generated by basis vectors $|b_0\rangle$, $|b_1\rangle$, ..., $|b_{2^n-1}\rangle$ where b_i is the representation of the number i in binary. This Hilbert space has a natural representation as a tensor product of n copies of $\mathcal{H}_2$, with the ith copy corresponding to the ith bit of the basis vectors. We refer to each of these copies of $\mathcal{H}_2$ as a *qubit*.

We define a *quantum error-correcting code* $\mathcal{Q}$ with rate k/n to be a unitary mapping of $\mathcal{H}_2^k$ into $\mathcal{H}_2^n$. Strictly speaking, this is actually a unitary mapping of $\mathcal{H}_2^k$ into a 2^k-dimensional subspace of $\mathcal{H}_2^n$; it can alternatively be viewed as a unitary mapping of $\mathcal{H}_2^k \otimes \mathcal{H}_2^{n-k}$ into $\mathcal{H}_2^n$, where the quantum state in $\mathcal{H}_2^{n-k}$ is taken to be that where all the qubits have quantum state $|0\rangle$. In our model of error analyzed in Section IV, we will assume that the decoherence process affects only t bits; that is, the decoherence is modeled by first applying an arbitrary unitary transformation D to the space consisting of the tensor product $\mathcal{H}_2^t \otimes \mathcal{H}_{\text{env}}$ of any t of the qubits and some arbitrary Hilbert space $\mathcal{H}_{\text{env}}$ designating the environment, and then tracing over the environment $\mathcal{H}_{\text{env}}$ to obtain the output of the channel, which will thus in general be an ensemble of states in $\mathcal{H}_2^k$. We say that a quantum code can correct t errors if the original state $|x\rangle \in \mathcal{H}_2^k$ can be recovered from the decohered encoded state $D\mathcal{Q}|x\rangle$

by applying a unitary transformation $\mathcal{R}$ (independent of D) to $\mathcal{H}_2^n \otimes \mathcal{H}_{\text{anc}}$, where $\mathcal{H}_{\text{anc}}$ is a Hilbert space representing the state of an ancilla (i.e., a supplementary quantum system). It turns out that if our quantum code will correct an *arbitrary* decoherence of t or fewer qubits, it will also be able transmit information with high fidelity for a large class of channels with physically plausible decoherence processes; this is discussed in Section VI.

Since the error correction must work for any encoded state $\mathcal{Q}|x\rangle$, the property of being a quantum error-correcting code depends only on the subspace $\mathcal{Q}\mathcal{H}_2^k$ of $\mathcal{H}_2^n$, and not on the actual mapping $\mathcal{Q}$. However, for ease of explanation, we will nonetheless define an orthogonal basis of this subspace of $\mathcal{H}_2^n$, which can be used to obtain an explicit mapping $\mathcal{Q}$, and call the elements of this basis codewords.

III. QUANTUM CODES

We will now define our quantum code. Suppose that we have a linear code $\mathcal{C}_1 \subset \mathsf{F}_2^n$. We let $\mathcal{H}_{\mathcal{C}_1}$ be the subspace of $\mathcal{H}_2^n$ generated by vectors $|c\rangle$ with $c \in \mathcal{C}_1$. Let M be a generator matrix for $\mathcal{C}_1$; this means that $\mathcal{C}_1$ is the row space of M, so that vM ranges over all the codewords in $\mathcal{C}_1$ as v ranges over all vectors in $\mathsf{F}_2^{\dim(\mathcal{C}_1)}$. For $w \in \mathsf{F}_2^n$, we define a quantum state $|c_w\rangle$ by

$$|c_w\rangle = 2^{-\dim(\mathcal{C}_1)/2} \sum_{v \in \mathsf{F}_2^{\dim(\mathcal{C}_1)}} (-1)^{vMw} |vM\rangle. \tag{2}$$

Note that if $w_1 + w_2 \in \mathcal{C}_1^\perp$, then $|c_{w_1}\rangle = |c_{w_2}\rangle$, since $vMw_1 = vMw_2$ for all $v \in \mathsf{F}_2^{\dim(\mathcal{C}_1)}$. Further note that $\langle c_{w_1}|c_{w_2}\rangle = 0$ if $w_1 + w_2 \notin \mathcal{C}_1^\perp$. This follows since $\sum_v (-1)^{vMw} = 0$ unless $vMw = 0$ for all $v \in F_2^{\dim(\mathcal{C}_1)}$ Thus, for $w \in \mathsf{F}_2^n/\mathcal{C}_1^\perp$ the vectors $|c_w\rangle$ form a basis for the space $\mathcal{H}_{\mathcal{C}_1}$. (Here $F_2^n/\mathcal{C}_1^\perp$ stands for the cosets of $\mathcal{C}_1^\perp$ in F_2^n, which are the sets $\mathcal{C}_1^\perp + w$ where $w \in \mathsf{F}_2^n$; there are $2^{\dim(\mathcal{C}_1)}$ of these cosets and they form the natural index set for the quantum states $|c_w\rangle$.)

Suppose now that we have another linear code $\mathcal{C}_2$ with $\{0\} \subset \mathcal{C}_2 \subset \mathcal{C}_1 \subset \mathsf{F}_2^n$. Our quantum code will be constructed using codes $\mathcal{C}_1$ and $\mathcal{C}_2$. We define the codewords of our quantum code $\mathcal{Q}_{\mathcal{C}_1,\mathcal{C}_2}$ as the set of $|c_w\rangle$ for all $w \in \mathcal{C}_2^\perp$, Recall that two codewords $|c_w\rangle$ and $|c_{w'}\rangle$ are equal if $w + w' \in \mathcal{C}^\perp$. The natural index set for the codewords is thus over $\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$, the cosets of $\mathcal{C}_1^\perp$ in $\mathcal{C}_2^\perp$. This code thus contains $2^{\dim(\mathcal{C}_1)-\dim(\mathcal{C}_2)}$ orthogonal vectors. Since its length is n qubits, it has rate $(\dim(\mathcal{C}_1) - \dim(\mathcal{C}_2))/n$. To construct a quantum error-correcting code from the Hamming code given in Eq. (1), we will take $\mathcal{C}_1$ to be this code and $\mathcal{C}_2$ to be $\mathcal{C}_1^\perp$. Thus, $\dim(\mathcal{C}_1) = 4$ and $\dim(\mathcal{C}_2) = 3$, so our quantum error-correcting code will map $4 - 3 = 1$ qubit into 7 qubits. There are thus two codewords. The first is

$$\begin{aligned}|c_0\rangle = \frac{1}{4}\Big(& |0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle \\ & +|1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \\ & +|0001011\rangle + |0010110\rangle + |0101100\rangle + |0110001\rangle \\ & +|1000101\rangle + |1011000\rangle + |1100010\rangle + |1111111\rangle \Big),\end{aligned} \tag{3}$$

and the second is

$$\begin{aligned}|c_1\rangle = \frac{1}{4}\Big(& |0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle \\ & +|1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \\ & -|0001011\rangle - |0010110\rangle - |0101100\rangle - |0110001\rangle \\ & -|1000101\rangle - |1011000\rangle - |1100010\rangle - |1111111\rangle \Big).\end{aligned} \tag{4}$$

Note that in $|c_1\rangle$ all the codewords of the Hamming code with an odd weight have a negative amplitude, and all the codewords with even weight have positive amplitude. This is the effect of the $(-1)^{vMw}$ term in Eq. (2).

We will show that if $\mathcal{C}_1$ and $\mathcal{C}_2^\perp$ have minimum distance d, then the quantum code $\mathcal{Q}_{\mathcal{C}_1,\mathcal{C}_2}$ can correct $t = \lfloor \frac{d-1}{2} \rfloor$ errors. (For our example code, $\mathcal{C}_1 = \mathcal{C}_2^\perp$ has minimum distance 3, so our quantum code will correct one error.) In the remainder of this section, we will give some intuition as to why this should be true; while in the next section, we will work out this calculation in detail.

To show why our codes are error-correcting, we must first give another representation of our codewords. If we perform the following change of basis,

$$|0\rangle \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{5}$$
$$|1\rangle \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

to each of the bits of our codeword $|c_w\rangle$ we obtain the state

$$|s_w\rangle = 2^{(\dim(\mathcal{C}_1)-n)/2} \sum_{u\in\mathcal{C}_1^\perp} |u+w\rangle. \tag{6}$$

We can see this since if $|x\rangle$ is any basis state in the rotated basis given by Eq. (5), then

$$\langle x|c_v\rangle = 2^{-(n+\dim\mathcal{C}_1)/2} \sum_{v\in\mathsf{F}_2^{\dim(\mathcal{C}_1)}} (-1)^{vM(w+x)}, \tag{7}$$

and this sum is 0 unless $w+x \in \mathcal{C}_1^\perp$. Letting $u = w+x$, we get Equation (6). For our example quantum code,

$$\begin{aligned} |s_0\rangle = \frac{1}{2\sqrt{2}}\Big(& |0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle \\ & +|1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \Big) \end{aligned} \tag{8}$$

and

$$\begin{aligned} |s_1\rangle = \frac{1}{2\sqrt{2}}\Big(& |0001011\rangle + |0010110\rangle + |0101100\rangle + |0110001\rangle \\ & +|1000101\rangle + |1011000\rangle + |1100010\rangle + |1111111\rangle \Big). \end{aligned} \tag{9}$$

We can now see how these codes are able to correct errors. In the $|c_w\rangle$ representation, all the codewords are superpositions of basis vectors $|v\rangle$ with $v \in \mathcal{C}_1$. Thus, any t bit errors (those errors taking $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$) can be corrected by performing a classical error-correction process for the code $\mathcal{C}_1$ in the original basis. In the $|s_w\rangle$ representation, all the codewords are superpositions of basis vectors $|v\rangle$ with $v \in \mathcal{C}_2^\perp$. Thus, any t bit errors in the rotated basis can be corrected by performing a classical error-correction process for the code $\mathcal{C}_2^\perp$ in the rotated basis. However, phase errors in the original basis (errors taking $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow -|1\rangle$) are bit errors in the rotated basis and vice versa. Thus, our quantum code can correct t bit errors and t phase errors in the original basis.

The correction process we use for our quantum error-correcting codes is indeed to first correct bit errors in the $|c_v\rangle$ basis classically and then to correct bit errors in the $|s_v\rangle$ basis classically. It remains to be shown that the correction process for the bit errors does not interfere with the correction process for the phase errors, and that arbitrary non-unitary errors on t or fewer quantum bits of our code will also be corrected by this procedure. This is done through calculations which are performed in Section IV of our paper.

As in Ref. [9], we correct the error by measuring the decoherence without disturbing the encoded information. Intuitively, what we do is to measure the decoherence without observing the encoded state; this then lets us correct the decoherence while leaving the encoded state unchanged. In our decoding procedure, we thus learn which qubits had bit errors and which had phase errors, which tells us something about the decoherence process but which gives no information about our encoded state. Linear codes are very well suited for this application: each codeword has the same relation to all the other words in the code, and this property is what enables us to measure the error without learning which codeword it is that is in error.

Since this paper was submitted, we learned that related work has been done by Steane [12]. Steane generates his quantum code using codewords

$$|s'_w\rangle = 2^{-\dim(\mathcal{C}_2)/2} \sum_{v \in \mathcal{C}_2} |v + w\rangle, \tag{10}$$

where w is chosen from $\mathcal{C}_1/\mathcal{C}_2$. This is the same as our $|s_w\rangle$ basis if the codes $\mathcal{C}_1$ and $\mathcal{C}_2^{\perp}$ are interchanged. It should also be noted that these codewords $|s'_w\rangle$ generate exactly the same subspace of $\mathcal{H}_2^n$ as the codewords $|c_w\rangle$ given by Eq. 2, and thus effectively give a different basis for the same quantum code.

IV. DECODING QUANTUM CODES

In this section we will show that errors in any t qubits of our quantum codes can be corrected by first correcting bit errors in the $|c\rangle$ basis, and then correcting bit errors in the $|s\rangle$ basis. For this section and the remainder of this paper, we will assume for simplicity that $\dim(\mathcal{C}_1) = n - k$ and $\dim(\mathcal{C}_2) = k$; thus, the rate of our codes will be $1 - 2k/n$. However, all of our results are easily extendable to quantum codes derived from classical codes $\mathcal{C}_2 \subset \mathcal{C}_1 \subset \mathsf{F}_2^n$ of any dimension.

In order to prove that errors in quantum codes can be corrected, we first need a lemma about purely classical codes.

Lemma 1. Suppose that $\mathcal{C}$ is a binary linear code of length n. Let e, $E \in \mathsf{F}_2^n$, with $e \preceq E$ and $\mathrm{wt}(E) < d(\mathcal{C}^\perp)$. Then there exists a vector $v_e \in \mathcal{C}$ such that $v_e|_{\mathrm{supp}(E)} = e$.

Proof. The projection of $\mathcal{C}$ onto E has to have full rank, because otherwise $\mathcal{C}^\perp$ would contain a vector w with $\mathrm{wt}(w) \leq \mathrm{wt}(E) < d(\mathcal{C}^\perp)$. □

We now need the following lemma about the states $|c_w\rangle$.

Lemma 2. Suppose that $\mathcal{C}_1$ has minimum distance d. Let e, $E \in \mathsf{F}_2^n$ with $e \preceq E$. Let P be the projection onto the subspace of $\mathcal{H}_2^n$ generated by all $|v\rangle$ where v is in the set $\{v \in \mathsf{F}_2^n : v|_E = e\}$, that is, with v equal to e on $\mathrm{supp}(E)$. Then

$$\langle c_{w_1}|P|c_{w_2}\rangle = 2^{-(n-k)} \sum_{v: vM|_E = e} (-1)^{vM(w_1+w_2)} \tag{11a}$$

$$= \begin{cases} (-1)^{e\cdot(c+w_1+w_2)}/2^{\mathrm{wt}(E)} & \text{if } \exists c \in \mathcal{C}_1^\perp \text{ such that } c+w_1+w_2 \preceq E, \\ 0 & \text{otherwise.} \end{cases} \tag{11b}$$

Proof. From the definition of $|c_w\rangle$ in Eq. (2), it is straightforward to show Eq. (11a). We must now show that this is equal to Eq. (11b). Since $\mathrm{wt}(e) < d(\mathcal{C}_1^\perp)$, by Lemma 1 there is a vector v_e such that $v_e M|_E = e$. We can obtain the linear space $\{v \in \mathsf{F}_2^{n-k} : v|_E = e\}$ by taking every vector in the set $\{v \in \mathsf{F}_2^{n-k} : v|_E = 0\}$ and adding the vector v_e. Using this substitution in Eq. (11a) gives

$$\langle c_{w_1}|P|c_{w_2}\rangle = 2^{-(n-k)} \sum_{v: vM|_E = 0} (-1)^{(v+v_e)M(w_1+w_2)} \tag{12a}$$

$$= 2^{-(n-k)} (-1)^{v_e M(w_1+w_2)} \sum_{v: vM|_E = 0} (-1)^{vM(w_1+w_2)}. \tag{12b}$$

Now, because the set $\{vM : vM|_E = 0\}$ is an $n-k-\mathrm{wt}(E)$ dimensional subspace of F_2^k, the sum (12b) is 0 unless $vM(w_1+w_2) = 0$ for all vM in this subspace. It is clear that if there is a $c \in \mathcal{C}_1^\perp$ such that $w_1+w_2+c \preceq E$, then $vM(w_1+w_2) = 0$ if $vM|_E = 0$, and $v_e M(w_1+w_2) = e\cdot(c+w_1+w_2)$. This shows the first part of Eq. (11b).

We now prove the other direction. Suppose that $vM(w_1 + w_2) = 0$ for all v with $vM|_E = 0$. Let e_j be the vector that is 1 on the jth coordinate of E and 0 on the other coordinates. We know from Lemma 1 that there is a vector $v_j \in \mathsf{F}_2^{n-k}$ such that $v_j M|_E = e_j$. Let $\sigma_j = v_j M(w_1 + w_2)$. We consider the vector $c' = w_1 + w_2 + \sum_{j=1}^{\mathrm{wt}(E)} \sigma_j e_j$; we will show that this vector satisfies the conditions for the c in Eq. (11b). Clearly, $w_1 + w_2 + c' \preceq E$. We need also to show that $c' \in \mathcal{C}_1^{\perp}$. Consider any vector $v \in \mathsf{F}_2^{n-k}$. We can decompose it into $v = v_0 + \sum_{i=1}^{\mathrm{wt}(E)} \alpha_i v_i$ where $v_0 M|_E = 0$, and α_i is 0 or 1. Note that $v_i M e_j = \delta(i,j)$ where δ is the Kronecker delta function. Now,

$$
\begin{aligned}
vMc' &= (v_0 + \sum_{i=1}^{\mathrm{wt}(E)} \alpha_i v_i) M (w_1 + w_2 + \sum_{j=1}^{\mathrm{wt}(E)} \sigma_j e_j) && \text{(13a)}\\
&= (\sum_{i=1}^{\mathrm{wt}(E)} \alpha_i v_i) M (w_1 + w_2 + \sum_{j=1}^{\mathrm{wt}(E)} \sigma_j e_j) && \text{(13b)}\\
&= \sum_{i=1}^{\mathrm{wt}(E)} \alpha_i v_i M (w_1 + w_2) + \sum_{i=1}^{\mathrm{wt}(E)} \alpha_i \sigma_i && \text{(13c)}\\
&= 0,
\end{aligned}
$$

proving the second part of Eq. (11b). The terms containing v_0 vanish in Eq. (13a) because $v_0 M(w_1 + w_2) = 0$ since $v_0 M|_E = 0$, and $v_0 M e_i = 0$ since $e_i \prec E$. The two terms in Eq. (13c) cancel because of the definition of σ_i. □

We are now ready to prove the following theorem.

Theorem 1. If $\mathcal{C}_1$ and $\mathcal{C}_2^{\perp}$ are both linear $[n, n-k, d]$ codes with $\{0\} \subset \mathcal{C}_2 \subset \mathcal{C}_1 \subset \mathsf{F}_2^n$, then the quantum code $\mathcal{Q}_{\mathcal{C}_1,\mathcal{C}_2}$ is a t-error correcting code, where $t = \lfloor \frac{d-1}{2} \rfloor$.

Proof. We show how to correct any t errors. Let us start with a codeword $|c_w\rangle$ for $w \in \mathcal{C}_2^{\perp}$. Now, let E be the binary vector such that $\mathrm{supp}(E)$ is the set of qubits that have decohered. By our hypothesis that at most t qubits decohere, we can take $\mathrm{wt}(E) = t$. We denote states of the environment by $|a_i\rangle$. Since the decoherence only operates on those qubits in $\mathrm{supp}(E)$, the most general decoherence D is a unitary process operating on a binary vector u and the initial state of the environment $|a_0\rangle$ as follows:

$$D|u, a_0\rangle = \sum_{e \preceq E} |u + e\rangle |a_{u|_E, e}\rangle, \tag{14}$$

where the states of the environment $|a_i\rangle$ are not necessarily normalized. Now, we let this decoherence act on $|c_w\rangle|a_0\rangle$. We get

$$D|c_w, a_0\rangle = 2^{-(n-k)/2} \sum_{v \in \mathsf{F}_2^{n-k}} (-1)^{vMw} \sum_{e \preceq E} |vM + e\rangle |a_{vM|_E, e}\rangle. \tag{15}$$

Now, we know $vM \in \mathcal{C}_1$, which is a code with minimum distance $d > 2\mathrm{wt}(e)$. Thus, we can restore $vM + e$ to a unique codeword $vM \in \mathcal{C}_1$. Intuitively, this corrects bits that have flipped from 0 to 1 or *vice versa*. We can do this using a unitary operator $\mathcal{R}_f$ provided we make the operation reversible; to do this we record the error e in a set of ancilla qubits A. After this process, the quantum state of our system is

$$\mathcal{R}_f D|c_w\rangle = 2^{-(n-k)/2} \sum_{v} (-1)^{vMw} \sum_{e \preceq E} |vM\rangle |a_{vM|_E, e}\rangle |A_e\rangle. \tag{16}$$

Note that since $vM \in \mathcal{C}_1$, we have now corrected our state to some state in the Hilbert space $\mathcal{H}_{\mathcal{C}_1}$. Recall that the vectors $|c_u\rangle$ with $u \in \mathsf{F}_2^n$ generated $\mathcal{H}_{\mathcal{C}_1}$. What we do now is to consider the Hilbert space $\mathcal{H}_{\mathcal{C}_1}$ in terms of the basis elements $|c_u\rangle$ for $u \in \mathsf{F}_2^n/\mathcal{C}_1^\perp$ instead of the basis elements $|vM\rangle$. We do this by substituting the identity

$$|vM\rangle = 2^{-(n-k)/2} \sum_{u \in \mathsf{F}_2^n/\mathcal{C}_1^\perp} (-1)^{vMu} |c_u\rangle \tag{17}$$

in Eq. (16). This gives the same type of effect as the change of basis in Eq. (5) in that it produces a representation in which it is easier to deal with phase errors. The substitution (17) gives the equation

$$\mathcal{R}_f D|c_w\rangle = 2^{-(n-k)} \sum_{v} (-1)^{vMw} \sum_{u} (-1)^{vMu} |c_u\rangle \sum_{e \preceq E} |a_{vM|_E, e}\rangle |A_e\rangle, \tag{18}$$

which can be rewritten as

$$\mathcal{R}_f D|c_w\rangle = 2^{-(n-k)} \sum_{e \preceq E} |A_e\rangle \sum_{e' \preceq E} |a_{e', e}\rangle \sum_{u} |c_u\rangle \sum_{v : vM|_E = e'} (-1)^{vMw} (-1)^{vMu} \tag{19}$$

Now, by Lemma 2, the inner sum is 0 unless there exists $c \in \mathcal{C}_1^\perp$ for which $c + w + u \preceq E$. This means that $|c_w\rangle$ can only decohere to $|c_u\rangle$ if there is a $c \in \mathcal{C}_1^\perp$ such that $\mathrm{wt}(u + w + c) \leq t$. We now show this means that for each $|c_u\rangle$ there is a unique $|c_w\rangle$ with $w \in \mathcal{C}_2^\perp/\mathcal{C}_1^\perp$ which it could have arisen from. Suppose that we have two such w's, w_1 and w_2 with $w_1+u+c_1=e_1$ and $w_2+u+c_2=e_2$. Then,

$$e_1+e_2=w_1+w_2+c_1+c_2\in\mathcal{C}_2^\perp. \tag{20}$$

However,

$$\mathrm{wt}(e_1+e_2)\le\mathrm{wt}(e_1)+\mathrm{wt}(e_2)\le 2t. \tag{21}$$

But $\mathcal{C}_2^\perp$ has minimum distance $d>2t$; thus $e_1=e_2$, so $w_1+w_2\in C_1^\perp$ and $|c_{w_1}\rangle=|c_{w_2}\rangle$.

This means that we can unitarily express the state in Eq. (19) in terms of $|c_u\rangle$, where $u\in\mathsf{F}_2^n/C_1^\perp$, and then correct the state $|c_u\rangle$ to $|c_w\rangle$, since there is at most one w with $d_H(w,u)<t$. As before, to unitarily correct $|c_u\rangle$ to $|c_w\rangle$ we need to use a second ancilla A' to record which bits we needed to flip to get from u to w. These flipped bits correspond to phase errors in the original basis. Denoting this correction operator by $\mathcal{R}_p$, we get

$$\begin{aligned}
\mathcal{R}_p\mathcal{R}_f D|c_w\rangle &= 2^{-(n-k)}\sum_{e\preceq E}|A_e\rangle\sum_{e'\preceq E}|a_{e',e}\rangle\sum_{v:vM|_E=e'}\sum_{e''\preceq E}(-1)^{vMw}(-1)^{vM(w+e'')}|c_w\rangle|A'_{e''}\rangle\\
&= 2^{-(n-k)}|c_w\rangle\sum_{e\preceq E}|A_e\rangle\sum_{e'\preceq E}|a_{e',e}\rangle\sum_{e''\preceq E}|A_{e''}\rangle\sum_{v:vM|_E=e'}(-1)^{vMe''}\\
&= 2^{-\mathrm{wt}(E)}|c_w\rangle\sum_{e\preceq E}|A_e\rangle\sum_{e''\preceq E}|A'_{e''}\rangle\sum_{e'\preceq E}(-1)^{e'\cdot e''}|a_{e',e}\rangle,
\end{aligned}\tag{22}$$

which is just $|c_w\rangle$ tensored with a state of the ancillae and the environment that *does not depend* on w. We have thus unitarily restored the original state and corrected t decohered bits. □

V. WEAKLY SELF-DUAL CODES

To show that a family of codes contains codes that meet the Gilbert-Varshamov bound we can often employ a very simple greedy argument; this argument appears in Ref. [6], pp. 557–558 (proof of Thm. 31 of Chap. 17).

Lemma 3. Let ϕ_i be a set of $[n_i,k_i]$ codes such that

1. $k_i/n_i>R$

2. each nonzero vector of length n_i belongs to the same number of codes in ϕ_i.

Then there are codes in the family that asymptotically meet the Gilbert-Varshamov bound:

$$R \geq 1 - H_2(\tfrac{d}{n}) \quad \text{as } n \to \infty \tag{23}$$

Proof. Let W_i be the number of codes in ϕ_i that contain a particular vector v. By hypothesis,

$$(2^{n_i} - 1)W_i = (2^{k_i} - 1)|\phi_i|. \tag{24}$$

The number of vectors with weight less than d is

$$\sum_{j=0}^{d-1} \binom{n_i}{j}. \tag{25}$$

If

$$W_i \sum_{j=0}^{d-1} \binom{n_i}{j} < W_i(2^{n_i} - 1)/(2^{k_i} - 1) = |\phi_i| \tag{26}$$

then there is a code in ϕ_i with minimum distance $\geq d$. *Q.E.D.*

This proof is not constructive in that it does not produce codes satisfying this bound, but merely shows that they exist. In fact, explicit constructions for classical codes that attain the Gilbert–Varshamov bound asymptotically are not known.

Consider towers of codes as shown below:

$$\{0\} \subseteq \langle\langle 1^n \rangle\rangle \subseteq \mathcal{C} \subseteq \mathcal{C}^\perp \subseteq F_2^n \tag{27}$$

where $\dim \mathcal{C} = k$ and $\dim \mathcal{C}^\perp = n - k$. Here $\langle\langle 1^n \rangle\rangle$ denotes the subspace of F_2^n generated by the vector 1^n containing all ones. The codes $\mathcal{C}$ and $\mathcal{C}^\perp$ correspond to $\mathcal{C}_2$ and $\mathcal{C}_1$, respectively, in the Section III; we have now added the requirement that $\mathcal{C}_1^\perp = \mathcal{C}_2$. We follow MacWilliams et al. [13]. They call a code *weakly self-dual* if

$$\langle\langle 1^n \rangle\rangle \subseteq \mathcal{C} \subseteq \mathcal{C}^\perp. \tag{28}$$

Given a vector v with even weight we need that the number of k-dimensional weakly self-dual codes for which $v \in \mathcal{C}^\perp$ is independent of v. In other words, the number of k-dimensional weakly self-dual codes $\mathcal{C}$ contained in a given hyperplane $v^\perp$ is independent of v.

We apply Theorem 2.1 of Ref. [13] (actually a stronger statement established in the proof).

Let $\sigma_{n,k,s}$ be the number of k-dimensional weakly self-dual codes $\mathcal{C}_{[n,k]}$ that contain a given s-dimensional code $\mathcal{C}_{[n,s]}$. Then the numbers $\sigma_{n,k,s}$ are independent of the code $\mathcal{C}_{[n,s]}$ that was chosen.

We separate the case $v \in \mathcal{C}_{[n,k]} \subseteq \mathcal{C}^\perp_{[n,k]}$ from the case $v \in \mathcal{C}^\perp_{[n,k]} \backslash \mathcal{C}_{[n,k]}$. The number of k-dimensional weakly self-dual codes $\mathcal{C}_{[n,k]}$ for which $v \in \mathcal{C}_{[n,k]}$ is just $\sigma_{n,k,2}$, the number of codes containing the 2-dimensional space $\langle\langle 1^n, v\rangle\rangle$. Next we consider pairs $(\mathcal{C}_{[n,k]}, v)$ where $\mathcal{C}_{[n,k]}$ is a k-dimensional weakly self-dual code and $v \in \mathcal{C}^\perp_{[n,k]} \backslash \mathcal{C}_{[n,k]}$. In this case $\mathcal{C}_{[n,k]}$ and v generate a $(k-1)$-dimensional weakly self-dual code $\mathcal{C}_{[n,k+1]}$ containing the 2-dimensional space $\langle\langle 1^n, v\rangle\rangle$. The number of choices for $\mathcal{C}_{[n,k+1]}$ is $\sigma_{n,k+1,2}$. Every code $\mathcal{C}_{[n,k+1]}$ contains 2^k k-dimensional weakly self-dual codes of which 2^{k-1} do not contain the 2-dimensional space $\langle\langle 1^n, v\rangle\rangle$. Hence given a vector v with even Hamming weight, the number of k-dimensional weakly self-dual codes contained in $v^\perp$ is independent of v. This is all that is needed to apply the greedy argument used to establish the Gilbert-Varshamov bound.

The statement that there are codes meeting the Gilbert–Varshamov bound is that given a ratio d/n (where d denotes minimum distance), we may achieve a rate

$$(n-k)/n \geq 1 - H_2\left(\tfrac{d}{n}\right). \tag{29}$$

The redundancy k/n satisfies $k/n \leq H_2(d/n)$, so that the quantum codes achieve a rate

$$R = (n-2k)/n \geq 1 - 2H_2\left(\tfrac{d}{n}\right). \tag{30}$$

This function is plotted in Fig. 1.

VI. QUANTUM CHANNELS

In order to carry Shannon's theory of information to the quantum regime, it is necessary to have some reasonable definition of a noisy quantum channel. We will define a quantum channel W by a probability distribution $\mathcal{P}$ on unitary transformations U_W mapping $\mathcal{H}_{\rm sig} \otimes \mathcal{H}_{\rm env}$. For any pure input state $|x\rangle$ the channel produces as output a mixed state by first obtaining an ensemble of states in $\mathcal{H}_{\rm sig} \otimes \mathcal{H}_{\rm env}$ by applying the transformation U_W to $|x\rangle$ with probability distribution $\mathcal{P}$, and secondly tracing over $\mathcal{H}_{\rm env}$. While the initial state of $\mathcal{H}_{\rm env}$ could be given by an ensemble of states, it may also without loss of generality be taken to be a fixed pure state, as the probability distribution given by an ensemble of initial states may be absorbed into the probability distribution on the unitary transformation U_W. The probability distribution could also be concentrated entirely in the inital mixed state of $\mathcal{H}_{env}$, and a fixed unitary transform U be used, but this leads to a slightly less intuitive description of the one quantum channel that we later discuss in detail.

Actual quantum channels are unlikely to produce output that differs from the input exactly by the decoherence of at most t qubits, and thus are unlikely to be able to transmit quantum states perfectly using this scheme. However, if the average behavior of the channel results in the decoherence of fewer than t qubits, a channel may still be able to transmit quantum states very well. A measure of the success of transmission of quantum states that has previously been successful applied in quantum information theory is fidelity [14,11]. In this paper, we define fidelity slightly differently from the definition in Refs. [14]; we make this change as these previous papers discuss channels that transmit some distribution of quantum states given *a priori*, whereas we want our channel to faithfully transmit any pure input state. Suppose that we have a noisy channel W that transmits quantum states in a Hilbert space $\mathcal{H}_{\rm sig}$. We define the fidelity of the channel to be

$$\min_{|x\rangle \in \mathcal{H}_{\rm sig}} \mathrm{E}\langle x|W|x\rangle, \tag{31}$$

where the expectation is taken over the output of the channel. In other words, we are measuring the fidelity of transmission of the pure state transmitted with least fidelity. We could also measure the fidelity of transmission of a typical state in $\mathcal{H}_{\mathrm{sig}}$; this average fideleity is a quantity which is closer to the previous definition, and may be more useful in some situations.

Assume that a channel W transmits qubits with a fidelity of F and is that the decoherence process affects each qubit independently, i.e., each the decoherence of one qubit has no correlation with the decoherence of any other qubit. This would follow from the assumption that each qubit has a different environment, and this situation corresponds to memoryless channels in classical information theory. Then $\mathrm{E}_W\langle x|W|x\rangle \geq F$ for every state $|x\rangle \in \mathcal{H}_2$. If the output of our channel is a pure state, our error-correction procedure $\mathcal{R}_p\mathcal{R}_f$ will be successful with probability equal to the length of the projection of the state onto the subspace of $\mathcal{H}_2^n$ which results from decoherence of any t or fewer qubits. Since the decoherence process for each qubit is independent, we can use the binomial theorem to calculate the probability that the state $W^n|y\rangle$ is projected onto the correctable subspace of $\mathcal{H}_2^n$, where $|y\rangle$ is in our quantum code $\mathcal{C}$. We thus have a channel which transmits states $|y\rangle$ with fidelity

$$\mathrm{E}\langle y|\mathcal{R}_p\mathcal{R}_f W^n|y\rangle \geq \sum_{j=0}^{t}\binom{n}{j}F^{n-j}(1-F)^j \tag{32}$$

for all $|y\rangle$ in our quantum code $\mathcal{C}$. This quantity is close to 1 as long as $t/n > 1-F$. Thus, if the fidelity F for each transmitted qubit is large enough, our quantum codes guarantee high fidelity transmission for our encoding of k qubits. Our quantum codes will give good results for any channel W that transmits states $|y\rangle \in \mathcal{H}_2^n$ well enough that $W|y\rangle$ has an expected projection of length at least $1-\epsilon$ onto the subspace of $\mathcal{H}_2^n$ obtained from $|x\rangle$ by the decoherence at most t qubits. Our encoding and decoding schemes then give a channel on the Hilbert space $\mathcal{H}_2^k$ which has fidelity $1-\epsilon$. We will next use this observation to obtain an upper bound on the channel capacity of quantum channels.

An upper bound for the amount of classical information carried by a quantum channel is given by the Levitin–Holevo theorem [10]. If the output of the channel is a signal that has density matrix ρ_a with probitility p_a, the Levitin–Holevo bound on the information content of this signal is

$$H(\rho) - \sum_a p_a H(\rho_a), \tag{33}$$

where $\rho = \sum_a p_a \rho_a$ (the density matrix for the ensemble of signals), and where $H(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$ is the von Neumann entropy. Since quantum information can be used to carry classical information, the Levitin–Holevo bound can be used to obtain an upper bound for the rate of a quantum error-correcting code.

Consider the following quantum channel discussed in Ref. [11]; this channel treats each qubit independently. With probability $1-p$, a qubit is unchanged, corresponding to the identity transformation $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Otherwise, with each possibility having probability $p/3$, the qubit is acted on by the unitary transformation corresponding to one of the three matrices: $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. That is, each of the following possibilities has probability $p/3$: the qubit is negated, or its phase is changed, or it is both negated and its phase is changed. If $t/n > p + \epsilon$ for $\epsilon > 0$, the length projection of the output of this channel onto the subspace of $\mathcal{H}_2^n$ with at most t errors approaches 1 as n grows, so the quantum error-correcting codes given earlier in this paper guarantee high fidelity. This channel can alternatively be described as transmitting a qubit error-free with probability $1 - \frac{4}{3}p$, and producing a random quantum state with probability $\frac{4}{3}p$. This description shows that the entropy of the output of the channel is at least $H_2(\frac{2}{3}p)$, so by the Levitin–Holevo theorem an upper bound on the classical information capacity of this channel is $1 - H_2(\frac{2}{3}p)$. This bound is plotted in Fig. 1. For this channel, the bound is achievable for classical information, but we believe it is unlikely to be tight for quantum information.

Another question that has been studied is: how much entanglement can be transmitted over a quantum channel [11]. Since any means of transmitting quantum states with high fidelity can also be used to transmit entanglement, upper bounds for entanglement transmission also apply to the quantum information capacity of a quantum channel. For the above channel, the upper bound proved in Ref. [11] is $H_2(\frac{1}{2} + \sqrt{p(1-p)})$ for $p < \frac{1}{2}$ and 0 if $p \geq \frac{1}{2}$. This bound is also plotted in Fig. 1.

ACKNOWLEDGMENTS

We would like to thank Peter Winkler for helpful discussions on quantum error-correcting codes, and David DiVincenzo for advice on the presentation of these results.

REFERENCES

[1] D. Deutsch, Proc. R. Soc. Lond. Ser. A **400,** 96 (1985); D. Simon, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science,* edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994) p. 116; P. W. Shor, *ibid.*, p. 124; A. Ekert and R. Jozsa, Rev. Mod. Phys. (to be published).

[2] S. Lloyd, Science **261,** 1569 (1993); D. P. DiVincenzo, Phys. Rev. A **51,** 1015 (1995); A. Barenco, D. Deutsch, A. Ekert and R. Jozsa, Phys. Rev. Lett. **74,** 4083 (1995); T. Sleator and H. Weinfurter, *ibid.* **74,** 4087 (1995); I. L. Chuang and Y. Yamamoto, Phys. Rev. A **52,** 3489 (1995).

[3] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74,** 4091 (1995).

[4] W. G. Unruh, Phys. Rev. A **51,** 992 (1995); G. M. Palma, K.-A. Suominen, and A. K. Ekert, Proc. R. Soc. London A, (to be published). R. Landauer, Philos. Trans. R. Soc. London Ser. A **353,** 367 (1995). R. Landauer, in *Proceedings of the Drexel-4 Symposium on Quantum Nonintegrability — Quantum Classical Correspondence,* edited by D. H. Feng and B.-L. Hu, (International Press, in press); I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, Science **270,** 1635 (1995).

[5] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano and D. J. Wineland, Phys. Rev. Lett. **75,** 4714 (1995).

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).

[7] R. L. Dobrushin and S. I. Ortyukov, Probl. Peredachi Inf. **13**(1), 82 (1977) [Probl. Inf. Transm. (USSR) **13,** 59 (1977)]; Probl. Peredachi Inf. **13**(3), 56 (1977) [Probl. Inf. Transm. (USSR) **13,** 203 (1977)]; N. Pippenger, J. Assoc. Comput. Mach., **36,** 531 (1989); N. Pippenger, G. D. Stamoulis and J. N. Tsitsiklis, IEEE Trans. Inf. Theory **37,** 639 (1991), U. Feige, P. Raghavan, D. Peleg, and E. Upfal, SIAM J. Comput. **23,**

1001 (1994).

[8] W. K. Wooters and W. H. Zurek, Nature **299,** 802 (1982); D. Dieks, Phys. Lett. A **92,** 271 (1982).

[9] P. W. Shor, Phys. Rev. A **52,** 2493 (1995).

[10] L. B. Levitin, in *Proceedings of the Fourth All-Union Conference on Information Theory,* Tashkent (1969), p. 111, in Russian; A. S. Kholevo, Probl. Peredachi Inf. **9**(3), 3 (1973) [Probl. Inf. Transm. (USSR) **9,** 177 (1973)].

[11] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wooters, Phys. Rev. Lett. **76,** 722 (1996).

[12] A. M. Steane, Proc. R. Soc. London A (to be published).

[13] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, Discrete Math., **3,** 153 (1972).

[14] B. Schumacher, Phys. Rev. A **51,** 2738 (1995); R. Jozsa and B. Schumacher, J. Mod. Opt. **41,** 2343 (1994).

FIGURES

FIG. 1. The solid line shows the asymptotic rate R of our quantum codes versus the error rate of the channel t/n. Two upper bounds for this quantity are also plotted: the Levitin–Holevo upper bound with a dashed line and the entanglement upper bound with a dotted line.