Entanglement required in achieving entanglement-assisted channel capacities

Garry Bowen*
Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, United Kingdom

(Received 22 May 2002; published 21 November 2002)

Entanglement shared between the two ends of a quantum-communication channel has been shown to be a useful resource in increasing both the quantum and classical capacities for these channels. The entanglement-assisted capacities were derived assuming an unlimited amount of shared entanglement per channel use. In this paper, bounds are derived on the minimum amount of entanglement required per use of a channel, in order to asymptotically achieve the capacity. This is achieved by introducing a class of entanglement-assisted quantum codes. Codes for classes of qubit channels are shown to achieve the quantum entanglement-assisted channel capacity when an amount of shared entanglement per channel given by, $\mathcal{E}_Q^{\mathrm{Random}} \geqslant 1 - Q_E$, is provided. It is also shown that for very noisy channels, as the capacities become small, the amount of required entanglement converges for the classical and quantum capacities.

DOI: 10.1103/PhysRevA.66.052313 PACS number(s): 03.67.Hk, 03.65.Ud, 89.70.+c

I. INTRODUCTION

Quantum-information theory is a generalization of the classical theory of information transmission and processing, where the encoding of information into a quantum system is taken into account [1]. The quantum phenomenon of entanglement, when utilized in quantum-information theory, allows for uniquely quantum phenomena, such as quantum dense coding [2] and quantum teleportation [3]. Dense coding was the first demonstration that entanglement could increase the classical communication capacity of a noiseless quantum channel by encoding twice as much information than would be possible without shared entanglement. This protocol required the use of one maximally entangled bipartite system, shared by sender and receiver, per use of the noiseless channel.

If the two ends of a quantum channel share unlimited prior entanglement, then the quantum capacities of the channel are known exactly [4,5]. The entanglement-assisted classical capacity of a channel, Λ, is given by,

$$C_E = \max_{\rho} [S(\rho) + S(\Lambda\rho) - S((\mathbb{I} \otimes \Lambda)|\phi\rangle\langle\phi|)], \tag{1}$$

where $|\phi\rangle$ is any purification of ρ, and $S(\rho)$ the von Neumann entropy of the state ρ, given by, $S(\rho) = \mathrm{Tr}\rho \log_2 \rho$. Traditionally the logarithm is taken to be base 2, giving the information in *bits*. The equation is the analog of Shannon's equation for the classical information capacity of a noisy classical channel [6]. The term on the right-hand side of Eq. (1) has previously been labeled as the von Neumann capacity of a quantum channel, and properties such as additivity have been shown to hold [7]. It is known that if the maximum is obtained for $\rho = (1/d)\mathbb{I}$, for a d-dimensional channel, then dense coding suffices to obtain the given capacity.

The entanglement-assisted quantum-information capacity for a channel is related to the classical quantity in Eq. (1), by [4],

$$Q_E = \frac{1}{2} C_E, \tag{2}$$

and the capacity is given in *qubits*. The equality is derived by utilizing teleportation and dense coding to give a lower bound to C_E of $2Q_E$, and then bound Q_E from below by $\frac{1}{2}C_E$.

In this paper, we examine whether the capacities in Eqs. (1) and (2) can be achieved if the shared entanglement per channel is restricted to a predetermined amount, $0 < \mathcal{E} < \infty$, per use of the channel. We assume that the amount of entanglement is determined by sharing m copies of a maximally entangled state, per n copies of the channel, with $m/n \to \mathcal{E}$ as $n \to \infty$. Shared pure entangled states that are nonmaximally entangled can be converted to maximally entangled states with an equivalent amount of entanglement in the asymptotic limit with vanishing amounts of classical communication [8], and can therefore be considered equivalent. The question of whether the distillable entanglement of shared mixed entangled resources is interconvertable with vanishing classical communication in the asymptotic limit is yet to be determined. The two quantities of interest are therefore the minimal amounts of shared entanglement required per channel in order to achieve the entanglement assisted channel capacities in the asymptotic limit. These quantities are denoted by $\mathcal{E}_C$ and $\mathcal{E}_Q$, for the classical and quantum requirements, respectively, and are defined as the limit, $\lim_{n\to\infty} \inf\{\mathcal{E} : R_{\mathcal{E}} = R_\infty\}$, where $R_{\mathcal{E}}$ is the channel capacity attainable with an amount of shared entanglement per channel equal to $\mathcal{E}$.

An upper bound on the entanglement required is obtained by introducing a class of entanglement-assisted quantum codes. These codes are based on the stabilizer formalism, with the exception that the ancillas used to encode the state are replaced by shared maximally entangled states. The ex-

*Electronic address: g.bowen@qubit.org

amination of these entangled quantum codes may also give insight into the behavior of degenerate as well as nondegenerate quantum codes. The introduction of degeneracy into entanglement-assisted codes acts to give a lower bound on the capacity of a channel without entanglement.

II. QUANTUM ERROR-CORRECTING CODES

Quantum states may be protected against decoherence, by encoding the state in a larger Hilbert space, thereby creating redundancy in the states that is resistant to noise. The theory of such quantum error-correcting codes is a rapidly growing area of research [9–21]. The standard method of encoding involves introducing many ancilla quantum states in a known preparation.

A quantum code works by embedding a state in a subspace of a larger Hilbert space, that is invariant under the encoding and decoding operations. A binary quantum code is designated by three parameters $[n,k,d]$, where k logical qubits are encoded in n physical qubits, and the code has a distance d, which means the code can correct $t=\frac{1}{2}(d-1)$ errors at unknown locations in the code block. This means when expanded in terms of error operators E, a t error correcting code reverses all errors E that have weight t or less.

For codewords $|i\rangle,|j\rangle$ and errors E_a,E_b, it is necessary that,

$$\langle i|E_a^\dagger E_b|j\rangle=0, \tag{3}$$

for $i\neq j$, otherwise the error E_a on $|i\rangle$ is indistinguishable from the error E_b on $|j\rangle$, and we would not know which error to correct for. In the case of *nondegenerate* quantum codes, a sufficient condition is also,

$$\langle i|E_a^\dagger E_b|j\rangle=\delta_{ab}\delta_{ij}, \tag{4}$$

so each error takes the code subspace to mutually orthogonal error subspaces $\mathcal{H}_a=E_a\mathcal{H}_{code}$. For *degenerate* quantum codes the sufficient condition becomes,

$$\langle i|E_a^\dagger E_b|j\rangle=M_{ba}\delta_{ij} \quad , \tag{5}$$

where $M_{ba}=\langle i|E_b^\dagger E_a|i\rangle$ is a Hermitian matrix.

A number of bounds exist for codes, including the quantum Hamming bound and quantum Gilbert-Varshamov bound [11], the no-cloning bound [22,23], the quantum Singleton bound [15], and the Rains bound [24]. The quantum Hamming bound only applies for nondegenerate quantum codes, whereas the quantum Singleton bound and the Rains shadow enumerator bound both apply to degenerate and nondegenerate codes. The linear programming bound applies by converting any additive quantum code to a classical code over $GF(4)$ [14].

A. Additive quantum codes

Additive quantum codes (or stabilizer codes) are obtained by utilizing the group structure of the set of errors acting on the Hilbert space in which the state is encoded [25]. Using random stabilizer codes it has been shown that there exist codes that achieve rates arbitrarily close to the nondegenerate quantum Hamming bound in the asymptotic limit.

For a group G acting on a Hilbert space $\mathcal{H}$, the stabilizer of an element of the space, $s\in\mathcal{H}$, denoted by S, is the set of elements in G for which s is an eigenvector of eigenvalue 1, under the action of S. In the case of stabilizer codes on qubits, the group in question is referred to as the Pauli group, G_n, and consists of the n-tensor products of the Pauli matrices. To make the group easier to deal with we assume, $X=\sigma_x$, $Y=-i\sigma_y$, and $Z=\sigma_z$, which gives, $XY=Z$. For the group to be closed, we must include the element -1, the negative of the identity. However, this acts trivially on the quantum states, as it simply takes, $\alpha|0\rangle+\beta|1\rangle\rightarrow-\alpha|0\rangle-\beta|1\rangle$, which is the same state modulo the phase. Hence, taking the subgroup $H=\{\pm1\}$, we can actually assume for the most part we are working with the group modulo the signs, G_n/H, with the major exception being the determination whether elements *commute* or *anticommute*. Since, $(-g)h=h(-g)$, if g and h commute (similarly for anticommutation), we can generally say that g and h commute or anticommute (in G_n) whilst considering the group of errors as a subset of G_n/H.

If we take our codespace to be a basis of the stabilized Hilbert space $\mathcal{H}_S$, for an Abelian subgroup S of G_n, then it is easy to see that these codewords are unaffected by any error contained in S. Hence, we have a degeneracy in the code for the errors in S, these errors do nothing. The set of errors, $E\in G_n$, that commute with S, that is, $gE=Eg$, for all $g\in S$, is known as the centralizer of S in G_n and denoted $Z(S)$. In the case of the error group G_n, there exists an equivalence between the centralizer and normalizer, $N(S)$, of the subgroup S, that is, $Z(S)=N(S)$ [1]. Elements of the normalizer not in the stabilizer, $N(S)\backslash S$, give all the errors that result in a logical error on the encoded qubits, which can be seen by the fact that $g(E|\psi\rangle)=Eg|\psi\rangle=E|\psi\rangle$ for all $g\in S$ and $|\psi\rangle$ in $\mathcal{H}_S$, and hence $E|\psi\rangle$ is in the codespace of S.

For all the errors that anticommute with at least one element of the stabilizer, then,

$$\langle i|F|j\rangle=\langle i|FE|j\rangle=-\langle i|EF|j\rangle=0, \tag{6}$$

for E in the stabilizer, and $F\in G_n\backslash N(S)$, and the error F takes the codewords to subspaces orthogonal to the code subspace. The act of (complete) decoding gives a map, $\kappa:G_n\rightarrow N(S)$, as it takes all the errors which map the code subspace to orthogonal spaces back to the code subspace. The map from the logical errors to the decoded qubits, $\phi:N(S)\rightarrow G_k$, is then a homomorphism, where G_k is the group of errors on the message qubits. Hence, $|N(S)|=|G_k||S|=4^k|S|$, and the errors in $N(S)$ are divided into 4^k cosets of equal size, with each coset of errors corresponding to one of the 4^k logical errors.

The error correction map κ is determined by choice of the particular inverse map h^{-1} that takes a nondegenerate error subspace back to the code space. We can choose the basis in the error subspace, $\{|\tilde{k}_E\rangle\}$, for a particular error h, such that

$h|\tilde{k}\rangle = |\tilde{k}_E\rangle$, which gives all the other errors that map the code space to this error space a grouping according to the logical error in this basis. Suppose s is an element of the stabilizer, then $h=hs$ on the code space, and hence $\kappa(hs)$ acts as the identity on the code subspace. A similar mapping occurs for all the logical errors on the code subspace. Hence, under the mapping $\kappa_{h^{-1}}$, if $g\in N(S)\cong g'\in G_k$ then $hg \cong g'\in G_k$. Since $hN(S)$ is a coset of $N(S)$ in G_n, then the map $\phi\circ\kappa : G_n \rightarrow G_k$, divides G_n up into 4^k sets of equal size, with all the members of each set corresponding to a different logical error.

In summary, a complete error correction scheme determines a map κ, which we choose to correct a particular member of each coset of $N(S)$, which in turn corrects all members of the image of S in that coset. Obviously we would like this set to contain the typical errors contained in the given coset of $N(S)$. A diagrammatic representation of this for a single encoded qubit is shown in Fig. 1.

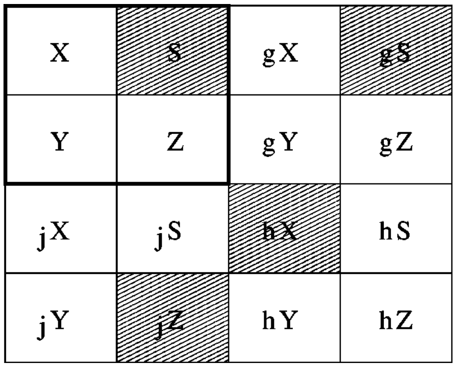


FIG. 1. Representation of the stabilizer and coset structure for a single encoded qubit. The stabilizer S, and logical errors X,Y, and Z, form the normalizer of the stabilizer (enclosed in the box). From each coset of the normalizer $N(S)$, a single coset of the stabilizer S may be mapped back to the stabilizer, representing a correction of the errors in that coset, the rest of the cosets are mapped to the corresponding logical errors. In this figure the error cosets gS, hX, and jZ are the corrected cosets of errors.

III. ENTANGLEMENT-ASSISTED CODES

By utilizing part of bipartite entangled states as the ancillas used in coding, the encoder and decoder may be able to create correlations between the encoded state and the reference states held by the receiver. These correlations enhance the ability of the receiver to decode the state without a logical error on the encoded states, thereby possibly increasing the quantum and classical capacities of a noisy channel.

A. A simple entanglement-assisted code

The simplest quantum error correcting code is the three qubit-repetition code, which encodes a single qubit, and corrects against a single bit flip on any of the three qubits. The qubit is encoded by using a controlled-NOT gate (CNOT) on the state with each of the two ancilla qubits. By adjusting the encoding procedure to use half of maximally entangled state, $|\Psi^+\rangle_{AB}=(1/\sqrt{2})(|00\rangle+|11\rangle)$, instead of the pure state ancillas, and encoding the pure state, $|\phi\rangle_A=\alpha|0\rangle+\beta|1\rangle$, we obtain the codeword,

$$|\Phi\rangle\rangle = \frac{\alpha}{2}(|000\rangle_A|00\rangle_B+|001\rangle_A|01\rangle_B+|010\rangle_A|10\rangle_B + |011\rangle_A|11\rangle_B)+\frac{\beta}{2}(|111\rangle_A|00\rangle_B+|110\rangle_A|01\rangle_B + |101\rangle_A|10\rangle_B+|100\rangle_A|11\rangle_B), \tag{7}$$

which can easily be seen to correct a single bit flip on the first three qubits of the codeword. However, in addition, if any combination of the second and third qubits undergoes a phase flip, then these errors are also correctable. For bit flip errors, we can see that the structure of the entanglement code depends on the labels attributable to the nontransmitted portion of the codewords, and we essentially break the coding subspaces down to a classical (3,1,3) code for these labeled spaces. If we look at the stabilizer formalism for the three-qubit repetition code, we can see that the elements of the stabilizer act on the code space to take it to an orthogonal subspace by flipping the phases of the components of the logical zero and one. For each of the codewords we see that the phases change as

$$111 \rightarrow ++++, \tag{8}$$

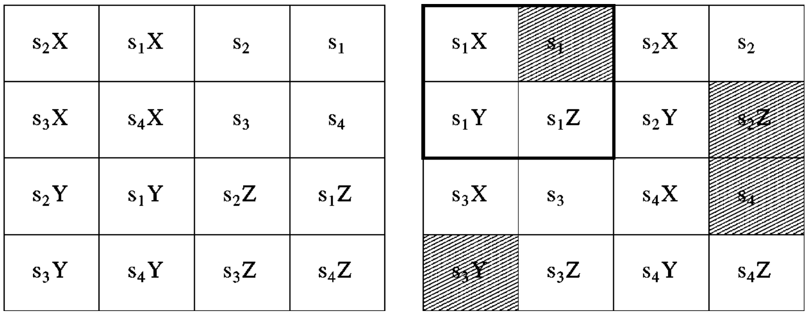
$$Z1Z \rightarrow +-+-, \tag{9}$$

$$1ZZ \rightarrow +--+, \tag{10}$$

$$ZZ1 \rightarrow ++--. \tag{11}$$

However, the code in the example is not a single error correcting, $t=1$, code as the single qubit error $Z11$ is a logical error on the codeword, and hence cannot be corrected. The obvious candidate for a $k=1$ single error-correcting entangled code is the five-qubit $k=1$ single error-correcting code [26]. The codewords for this code can be generated using a pair of entangled ancillas using a local unitary operation on the encoded state and the local halves of the two entangled states. The unitary transformation is determined by the change of basis,

$$\begin{aligned}
|000\rangle &\rightarrow |000\rangle-|011\rangle+|101\rangle-|110\rangle,\\
|001\rangle &\rightarrow |001\rangle+|010\rangle-|100\rangle-|111\rangle,\\
|010\rangle &\rightarrow -|001\rangle+|010\rangle+|100\rangle-|111\rangle,\\
|011\rangle &\rightarrow -(|000\rangle+|011\rangle+|101\rangle+|110\rangle),\\
|100\rangle &\rightarrow -(|001\rangle+|010\rangle+|100\rangle+|111\rangle),\\
|101\rangle &\rightarrow -|000\rangle+|011\rangle+|101\rangle-|110\rangle,\\
|110\rangle &\rightarrow -|000\rangle-|011\rangle+|101\rangle+|110\rangle,\\
|111\rangle &\rightarrow -|001\rangle+|010\rangle-|100\rangle+|111\rangle,
\end{aligned} \tag{12}$$



s$_2$X	s$_1$X	s$_2$	s$_1$
s$_3$X	s$_4$X	s$_3$	s$_4$
s$_2$Y	s$_1$Y	s$_2$Z	s$_1$Z
s$_3$Y	s$_4$Y	s$_3$Z	s$_4$Z

s$_1$X	s$_1$	s$_2$X	s$_2$
s$_1$Y	s$_1$Z	s$_2$Y	s$_2$Z
s$_3$X	s$_3$	s$_4$X	s$_4$
s$_3$Y	s$_3$Z	s$_4$Y	s$_4$Z

FIG. 2. The left-hand figure represents the normalizer from FIG. 1, subdivided into the individual elements of the stabilizer and its cosets. Under an entangled code these all map to orthogonal subspaces, and hence the new stabilizer $S' = s_1$, and logical errors X, Y and Z, form the normalizer of a new stabilizer. The increased ability to choose correctable errors allows us to attain the entanglement-assisted capacity for certain classes of qubit channels.

which gives the codewords for the five-qubit single error-correcting code. The five-qubit code is thus equivalent to an entanglement-assisted three-qubit code, with an unassisted stabilizer, $S=\{111, X1X, ZYY, YYZ\}$. As the five-qubit single error-correcting code can correct single errors on the last two qubits of the codewords, and these qubits are noiseless in the entangled code, the code is not very efficient in maximizing the number of errors that can be corrected. In order to examine the error-correcting capability of additive entangled codes we must look again at the quantum Hamming bound.

B. Revising the quantum hamming bound

The reason that entanglement-assisted codes are better than their nonentangled counterparts, is that the entanglement allows us to increase the dimension of the decoding Hilbert space to 2^{2m+k} dimensions, for m the number of entangled ancillas, compared to the 2^{m+k} dimensions for m unentangled ancilla qubits. This gives a revised quantum Hamming bound for entanglement-assisted codewords as [7]

$$2^k \sum_{j=0}^{t} 3^j \binom{n}{j} \leqslant 2^{2n-k}, \tag{13}$$

which is easily satisfied for the three-qubit code above, with $k=1$, $n=3$, and $t=1$.

The asymptotic form of Eq. (13) is given by

$$\frac{k}{n} \leqslant \frac{m}{n} + 1 - \frac{t}{n}\log_2 3 - H_2\left(\frac{t}{n}\right), \tag{14}$$

where $m=n-k$, which can be seen to exceed the normal quantum Hamming bound. Substituting the rate and error probability, for $R=k/n$, and $p=t/n$, we have,

$$R \leqslant 1 - \frac{p}{2}\log_2 3 - \frac{1}{2}H_2(p), \tag{15}$$

which corresponds to the entanglement-assisted quantum capacity for the depolarizing channel.

C. General entangled additive codes

For general stabilizer codes we must prove that the elements of the stabilizer act to take the codewords to orthogonal subspaces, which are also orthogonal to the other error spaces generated by the elements outside the normalizer (Fig. 2). As a code is constructed by a unitary transformation, if we act on the states $|k\rangle \otimes |00\ldots0\rangle$ and $|k\rangle \otimes |00\ldots1\rangle$, for $|k\rangle$, $|l\rangle$, basis states for the state to be encoded, we find,

$$\langle k| \otimes \langle 0\ldots00| U^\dagger U |l\rangle \otimes |00\ldots1\rangle = 0, \tag{16}$$

and the code states with orthogonal ancillas are obviously orthogonal. Hence, by introducing the set of bit flip operators, $P(X)$, and applying them to the ancillas, we then have,

$$\langle k| \otimes \langle 0\ldots00| P_i(X) U^\dagger U P_j(X) |l\rangle \otimes |00\ldots0\rangle = \delta_{ij}\delta_{kl}, \tag{17}$$

which holds for all possible combinations of bit flip operators. By combining these states with the basis, $\{|k\rangle\}$, for the message qubits we then have a basis for the encoder's Hilbert space. When the ancillas consist of the shared entangled states, $|\Psi^+\rangle_{AB}$, then we encode a linear combination of orthogonal states,

$$|\tilde{k}\rangle = \sum_{P(X)} U_A(|k_A\rangle \otimes P(X)|00\ldots0_A\rangle) \otimes P(X)|00\ldots0_B\rangle, \tag{18}$$

where the sum is over the set of all possible bit flips on the ancillas. Now, suppose, $E \in S$, is an element of the stabilizer, then,

$$\langle k| \otimes \langle 0\ldots00| U^\dagger E U P(X) |l\rangle \otimes |00\ldots0\rangle = 0, \tag{19}$$

for $P(X) \neq \mathbb{I}$, this is because $E=E^\dagger$ for $E \in S$, and so acting to the left the error leaves the bra invariant. This also applies for the encoding of all the basis states of the message, and so these states are orthogonal to the code space. Also, the encoding operation has the freedom to ensure,

$$\begin{aligned}\langle \tilde{k}|E|\tilde{l}\rangle = &\sum_{P_1(X),P_2(X)} \langle \mathbf{0}_B|P_2(X)\langle \mathbf{0}_A|P_2(X) \\ &\times \langle k_A|U_A^\dagger E U_A|l_A\rangle P_1(X)|\mathbf{0}_A\rangle P_1(X)|\mathbf{0}_B\rangle \qquad (20) \\ = &\sum_{P(X)} \langle \mathbf{0}_A|P(X)\langle k_A|U_A^\dagger E U_A|l_A\rangle P(X)|\mathbf{0}_A\rangle \qquad (21) \\ = &\,0, \qquad (22)\end{aligned}$$

where the final line follows from the fact that, since the state, $\{P(X)|\mathbf{0}\rangle\}$, tensored with a basis for the space to be encoded, forms a basis for the total encoding space, we can choose the encoding U such that the encoded basis states form a basis consisting of the eigenvectors of S (which is possible as all the elements of S commute), ensuring half are $+1$ eigenvectors and half -1 eigenvectors of any, $E\in S$, excluding the identity. For any two stabilizer elements, $E,F\in S$, the product, $E^{\dagger}F=EF$, is also in the stabilizer, and hence the argument above shows that any two different elements of the stabilizer map codewords to orthogonal subspaces for the entangled code.

Furthermore, we can also choose the basis, such that for each given $P(X)$, the states $\{U|k\rangle P(X)|\mathbf{0}\rangle\}$, all sit in the same eigenspace. To see this, note that for the 2^{n-k} generators of the stabilizer, we write out binary strings with each element of the string corresponding to whether the given basis state is a $+1$ or -1 eigenstate of that element. Each of these strings then corresponds to a given $P(X)$, and the remaining 2^k bits required to label the basis can then correspond to each of the 2^k basis states of the message space $|j\rangle$. The fact that the subspaces generated by the stabilizer elements are then orthogonal to the subspaces generated by errors outside the normalizer can then be shown by substituting $EF=EFE^2$ into Eqs. (20)–(22), and noting that the states for each term in Eq. (21) are both ± 1 eigenvectors of E with the same sign, and then noting that $EF=-FE$. The proofs that there exist entangled stabilizer codes that attain the capacities for both unital qubit channels and the qubit erasure channel, with an amount of entanglement per channel given by $\mathcal{E}_Q^{\mathrm{Random}}=1-Q_E$, are outlined in the Appendix.

D. Entangled codes and degeneracy

For an entangled additive code that encodes k qubits using m entangled ancillas and a nonentangled ancillas, there are, $|\mathcal{C}|=2^{n-k}=2^{2m+a}$ copies of the code space, $|E|=4^{k+m+a}$ physical errors, and, $|N(S)|/|S|=4^k$ logical errors on each subspace, hence,

$$|S|=\frac{|E|}{|\mathcal{C}|\times 4^k}=2^a, \tag{23}$$

and the number of elements in the stabilizer is determined by the number of nonentangled ancillas used for the encoding. The case of every ancilla being an entangled state, $a=0$, reduces Eq. (23) to, $|S|=1$, and there are no degenerate errors for such an entangled code. The parameter $\mathcal{A}=a/n$, therefore, gives a measure of the degeneracy possible with the encoding, as the size of the stabilizer scales as $|S|=2^{n\mathcal{A}}$.

E. "Teleportation" codes

The next entanglement-assisted codes we look at are teleportation codes, based on the structure of the standard teleportation protocol. The classical channel may be modeled by a "classical" quantum channel such as the total dephasing channel, $\Lambda\rho=\frac{1}{2}(\rho+\sigma^Z\rho\sigma^Z)$, which has classical capacities of $C=C_E=1$, but a zero quantum capacity. The entanglement-assisted quantum capacity of Λ is, therefore, $Q_E(\Lambda)=\frac{1}{2}C_E=\frac{1}{2}$.

First, we examine the standard teleportation protocol using this channel. For a single entangled resource, and a single qubit, $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$, we undertake the transformation,

$$|00_A\rangle\otimes|\psi_A\rangle\otimes|\Psi^+_{AB}\rangle\rightarrow U_A|00_A\rangle\otimes|\psi_A\rangle\otimes|\Psi^+_{AB}\rangle, \tag{24}$$

where the unitary encoding operation is given by

$$\begin{aligned}U_A={}&\mathbb{I}\otimes\mathbb{I}\otimes|\Psi^+\rangle\langle\Psi^+|+\mathbb{I}\otimes\sigma_x\otimes|\Phi^+\rangle\langle\Phi^+|+\sigma_x\otimes\mathbb{I}\otimes|\Phi^-\rangle\\ &\times\langle\Phi^-|+\sigma_x\otimes\sigma_x\otimes|\Psi^-\rangle\langle\Psi^-|.\end{aligned} \tag{25}$$

The first two qubits in Eq. (24) are sent through the quantum channel Λ, and the operation V_{AB} applied to the three qubits at the receivers end of the channel, where,

$$\begin{aligned}V_{AB}={}&|00_A\rangle\langle 00_A|\otimes\mathbb{I}_B+|01_A\rangle\langle 01_A|\otimes\sigma_{xB}\,,+|10_A\rangle\langle 10_A|\otimes\sigma_{yB}\\ &+|11_A\rangle\langle 11_A|\otimes\sigma_{zB}\,,\end{aligned} \tag{26}$$

to give the resultant decoded state. The codeword generated in Eq. (24) can be written explicitly as

$$\begin{aligned}|\Phi\rangle\rangle={}&|00\rangle|\Psi^+\rangle|\psi\rangle+|01\rangle|\Phi^+\rangle\sigma_x|\psi\rangle,+|10\rangle|\Phi^-\rangle\sigma_y|\psi\rangle\\ &+|11\rangle|\Psi^-\rangle\sigma_z|\psi\rangle,\end{aligned} \tag{27}$$

and we may note that the label states consisting of the Bell states that are not sent through the channel can be considered redundant, and so we may encode the state by ignoring the ancillas, and using a CNOT followed by a Hadamard transformation on the encoded qubit. Thus,

$$|\Phi\rangle\rangle=|00\rangle|\psi\rangle+|01\rangle\sigma_x|\psi\rangle+|10\rangle\sigma_y|\psi\rangle,+|11\rangle\sigma_z|\psi\rangle, \tag{28}$$

and the label states $|00\rangle,|01\rangle,|10\rangle$, and $|11\rangle$, are each invariant, up to a global phase, under the action of the channel Λ. Upon measurement of the first two qubits of $\Lambda\rho_{AB}$ we obtain an "error syndrome," which is then corrected by application of the appropriate unitary transformation. The code thus requires two uses of the channel Λ for each state sent, giving a rate $R=1/2$, which attains the entanglement-assisted capacity for this channel. We can also note that the amount of entanglement required per channel is simply one e-bit per two channels or, $\mathcal{E}_Q=1-Q_E=1/2$. However, it is apparent that teleportation codes can only be optimal if, $C_E=C$, for the channel. An example when they are not optimal is given by a dephasing channel for $p\neq 1/2$, where the teleportation code still only has a rate $R=1/2$, whilst entangled codes attain $Q_E=1-\frac{1}{2}H(p)>1/2$.

There is, however, a notable difference between the teleportation code compared to the entangled linear codes for the $p=1/2$ dephasing channel, in that the channel created by the teleportation code is noiseless in the case of a finite number of uses of the channel, whereas the entangled linear codes obtain arbitrarily high fidelity only in the asymptotic limit. In this sense the teleportation code is an analog of a zero error code [6], but this relies on the ability of the channel to transmit a zero error classical code.

IV. ENTANGLEMENT PER CHANNEL REQUIREMENTS

The entanglement quantum Hamming bound for m e-bits in a length n code includes the terms, $n=k+m+a$, where a is the number of unentangled ancillas required in the code. Therefore,

$$2^k\sum_{j=0}^{t} 3^j\binom{n}{j}\leqslant 2^{2m+k+a}, \tag{29}$$

which in the asymptotic limit gives

$$R\leqslant 1+\mathcal{E}-p\log_2 3-H(p). \tag{30}$$

Since $m\leqslant n-k$ equality gives the entanglement-assisted capacity for the depolarizing channel in Eq. (13), and so this requires a minimum entanglement of $\mathcal{E}=1-R$ e-bits per channel to reach capacity with a nondegenerate code. If the entanglement per channel is given by $\mathcal{E}=(1/M)(1-R)$, then we obtain a family of entanglement Hamming bounds, where,

$$R\leqslant 1-\frac{M}{M+1}[p\log_2 3+H(p)], \tag{31}$$

corresponding to the limits for nondegenerate codes with the given amount of entanglement per channel. As the amount of entanglement per channel decreases, the size of the stabilizer increases, and hence the possibility of using degeneracy in codes to increase the capacity beyond the corresponding Hamming bound is also presumed to increase.

Whenever $C_E>C$, the entanglement-assisted classical capacity is generally assumed to require $\mathcal{E}=S(\rho)$ e-bits per channel in order to achieve the capacity, where ρ is the state that achieves the maximum in Eq. (1). In the case of unital qubit channels, if standard dense coding is used with halves of shared maximally entangled pairs, which are then sent via entangled quantum codes, the capacity, $C_E=2Q_E$, can be achieved with $\mathcal{E}=1$. This is not a very useful fact, as for this type of channel it is already well known that dense coding achieves this capacity, with $\mathcal{E}_{DC}=1$ [4,13]. However, if a degenerate entangled code can be found with, $\mathcal{E}<1-Q_E$, then the capacity C_E could be achieved with $\mathcal{E}<1$. With this in mind, we examine what bounds exist on the entanglement requirements $\mathcal{E}_Q$ and $\mathcal{E}_C$.

A. Upper and lower bounds on the required entanglement

Given $n\mathcal{E}_Q$ shared e-bits, we can simulate nQ_E noiseless quantum channels with n noisy channels. Therefore, if we are given extra nQ_E shared e-bits, we can utilize dense coding with these extra e-bits to obtain a capacity of $nC'=2nQ_E=nC_E$, and hence, $\mathcal{E}_Q\geqslant\mathcal{E}_C-Q_E$. Obtaining a lower bound on $\mathcal{E}_C$ therefore gives a lower bound on $\mathcal{E}_Q$. Similarly, given $\mathcal{E}_C$ e-bits per channel means we can simulate nC_E noiseless classical channels with n noisy quantum channels, hence with $nC_E/2=nQ_E$ e-bits of extra entanglement we can teleport to create nQ_E noiseless quantum channels, and so we obtain the bound $\mathcal{E}_Q\leqslant\mathcal{E}_C+Q_E$. Hence, a lower bound on $\mathcal{E}_Q$ gives a lower bound on $\mathcal{E}_C$. Putting this two inequalities together gives the relationship,

$$Q_E\geqslant|\mathcal{E}_C-\mathcal{E}_Q|, \tag{32}$$

which relates the capacities to the minimum entanglement requirements. From this inequality it is easily seen that as the channel becomes so noisy that the entanglement-assisted capacities become small, the entanglement requirements converge, that is, $Q_E\rightarrow 0\Rightarrow\mathcal{E}_C\rightarrow\mathcal{E}_Q$.

When coupled with a noiseless channel, the capacity of any noisy quantum channel is additive [13]. If we have n copies of a noisy channel, and we add m noiseless channels, such that, $m/n\simeq\mathcal{E}_Q$, then sending maximally entangled states through the noiseless channel will give us enough entanglement to achieve the entanglement-assisted capacity for the noisy channels. Hence, $m+nQ\simeq n\mathcal{E}_Q+nQ\geqslant nQ_E$, and,

$$\mathcal{E}_Q\geqslant Q_E-Q, \tag{33}$$

giving a lower bound on the required entanglement in terms of the channel capacities. Similarly, the classical capacity version of this inequality also applies, where, $\mathcal{E}_C\geqslant C_E-C$. As the classical capacity of a channel is at least as great as the quantum capacity, the ratio $Q/C\leqslant 1$. Thus,

$$\mathcal{E}_C\geqslant\frac{Q}{C}(C_E-C). \tag{34}$$

The combination of Eqs. (33) and (34) gives upper and lower bounds on the quantum capacity of a channel based on the entanglement capacities, classical capacity, and required entanglement, where,

$$\frac{\mathcal{E}_C}{C_E/C-1}\geqslant Q\geqslant Q_E-\mathcal{E}_Q, \tag{35}$$

although the upper bound may not be very tight for many channels.

B. Examples for particular channels

The quantum erasure channel has known quantum and classical capacities [27,28]. The entanglement-assisted capacities are $C_E=2-2\epsilon$ and, $Q_E=1-\epsilon$, for a channel erasure probability ϵ [4]. Using Eq. (33) we can show that if $\mathcal{E}_Q=\epsilon-\delta$ for $\delta>0$, then this implies $Q>1-2\epsilon$, a contradiction. Hence, we have a lower bound on $\mathcal{E}_Q$, which combined with the random coding bound $\mathcal{E}_Q\leqslant 1-Q_E=\epsilon$, gives the equality $\mathcal{E}_Q=\epsilon$ for the erasure channel. For the erasure channel we can therefore see that whilst Q_E is attainable with ϵ e-bits per channel, the classical capacity C_E is only attainable with more than $\mathcal{E}_C\geqslant 1-\epsilon$ e-bits (if not 1 e-bit), and so for $\mathcal{E}=\epsilon<1/2$ e-bits per channel the factor of two relationship between these capacities no longer holds, and hence, $C_{\mathcal{E}}<2Q_{\mathcal{E}}=C_E$.

For the dephasing channel, $\Lambda=(1-p)\mathbb{I}+pZ$, for Z a phase flip of the qubit, we can also calculate bounds on the required entanglement, where,

$$1-H(p)\leqslant\mathcal{E}_C\leqslant 1, \tag{36}$$

$$\mathcal{E}_Q=\frac{1}{2}H(p), \tag{37}$$

where equality is obtained in the second case as the upper and lower bounds again coincide.

The entanglement-assisted capacities for unital qubit channels are determined by sending half of the maximally entangled state through the channel [13,29]. This gives a lower bound on the entanglement of the Bell diagonal state generated by sending half the maximally entangled state through the channel, where,

$$E(\rho)\geqslant C_E-1=1-S(\rho), \tag{38}$$

and this quantity is equivalent to the distillable entanglement of ρ using the Hashing protocol. This bound is derived for $\mathcal{E}_Q=1-Q_E$, however, if $\mathcal{E}_Q=1-Q_E-\delta$ for $\delta>0$, then the lower bound on the entanglement is higher. This is because obtaining the capacity with less entanglement per channel requires degeneracy in the code, and the degeneracy is what allows us to beat the Hashing bound [30].

Finally, note that for entanglement breaking channels the two entanglement-assisted capacities are bounded by $C_E\leqslant 1$ and $Q_E\leqslant 1/2$, otherwise the ratio of entanglement that can be sent through the channel $E'=Q_E$ and the initial entanglement $E=1-Q_E$ would be larger than 1, allowing us to create entanglement through the channel.

V. DISCUSSION

At this point we make the conjecture that the unassisted quantum capacity of a channel is given by

$$Q=Q_E-\mathcal{E}_Q=C_E-\mathcal{E}_C, \tag{39}$$

whenever $Q_E\geqslant\mathcal{E}_Q$ (and both $C_E\geqslant\mathcal{E}_C$ and $C_E>C$ in the second equality), and zero otherwise. The first equality holds for the dephasing and erasure channels, and the second equality will hold for both the dephasing and erasure channels, provided $\mathcal{E}_C=1$ and $p\neq 1/2$. The second equality requires the condition $C_E>C$, and would imply the equality $Q_E=\mathcal{E}_C-\mathcal{E}_Q$. If this conjecture is true, then calculating the capacity of a quantum channel could be achieved by calculating C_E from Eq. (1), and either $\mathcal{E}_C$ or $\mathcal{E}_Q$. Calculating either of these two quantities, however, may be just as difficult as determining the unassisted quantum capacity itself. So far it has been shown in this paper that

$$Q\geqslant Q_E-\mathcal{E}_Q, \tag{40}$$

$$C_E-\mathcal{E}_C\geqslant Q_E-\mathcal{E}_Q, \tag{41}$$

so the reverse inequalities need to be shown for both of these equations to prove the conjecture. The second of these is likely to be a problem, as it breaks down whenever $C_E=C$, as this implies $Q=C$, which is not true for many known channels. However, we do have the relationship

$$Q\geqslant\frac{Q}{C}C_E-\mathcal{E}_C, \tag{42}$$

for $Q>0$, that gives $Q\geqslant Q-\mathcal{E}_C$ whenever $C_E=C$.

The existence of degenerate entangled codes for unital qubit channels would also imply that the entanglement-assisted classical capacity for such channels could be achieved with an amount of entanglement per channel $\mathcal{E}_C<1$. This would be a surprising result, as it is well known that dense coding achieves the capacity with $\mathcal{E}=1$, and this protocol has been assumed to be optimal.

VI. CONCLUSION

In this paper bounds on the minimum amount of shared entanglement necessary per channel required to achieve the entanglement-assisted capacities were derived. An upper bound on the entanglement required, for classes of qubit channels, was obtained by introducing entanglement-assisted additive quantum codes. The difference between the amounts of entanglement required were shown to vanish as the entanglement-assisted capacities became small.

It was then shown that the unassisted capacities of the channel were bounded from below by the difference in the entanglement-assisted capacities and the amount of entanglement required to achieve them. The introduction of degeneracy into these entanglement-assisted codes would therefore give a lower bound on the unassisted capacity for some of these channels that is higher than currently known lower bounds. The use of such codes would also allow the entanglement-assisted classical capacity, for classes of unital qubit channels, to be attained with less than one *e*-bit per channel. Whether or not the generation of degenerate entangled codes will be easier than simply determining classes of unassisted degenerate quantum codes is not known, but this method does provide a second avenue for investigation.

Finally, a conjecture was made that there exists an equality between the unassisted quantum capacity of a channel and the difference in the entanglement-assisted capacity and the respective minimum required entanglement attaining that capacity. If this conjecture is shown to hold, then it provides a further link between entanglement as a resource and quantum communication.

ACKNOWLEDGMENTS

I thank Luke Rallan and Sougato Bose for very helpful discussions. G.B. is supported by the Oxford-Australia Trust, the Harmsworth Trust, and the CVCP.

APPENDIX: SUMMARY OF THE PROOF FOR ENTANGLEMENT-ASSISTED CODES ACHIEVING Q_E

By taking random stabilizer codes, and showing that the average probability of error can be made vanishingly small in the limit of large block sizes, we may infer the existence of stabilizer codes that have a vanishingly small maximal failure probability, with rates arbitrarily close to the capacity. First, we outline the case of the unital qubit channels. For such a channel, the number of typical errors with total probability bounded by, $P \geqslant 1-\eta$, for $\eta > 0$, is bounded above by

$$N \leqslant 2^{nS[(\mathbb{I}\otimes\Lambda)|\Psi^+\rangle\langle\Psi^+|]+2n\delta}, \tag{A1}$$

for any $\delta > 0$, with n sufficiently large. The total probability of failure is then given by,

$$\begin{aligned} P(\text{fail}) &\leqslant 2^{nS[(\mathbb{I}\otimes\Lambda)|\Psi^+\rangle\langle\Psi^+|]+2n\delta} 2^{-(2n-2k)} + \eta \\ &\leqslant 2^{n\{S[(\mathbb{I}\otimes\Lambda)|\Psi^+\rangle\langle\Psi^+|]+2R-2+2\delta\}} + \eta, \end{aligned} \tag{A2}$$

where the first term gives the probability of two typical errors having the same syndrome, and the second term is the probability of an atypical error. The number of syndromes is determined by the fact that there are 2^{2n-k} dimensions divided amongst 2^k encoded qubits. Hence, the average probability of failure becomes arbitrarily small, for large n, for any, $R < 1 - \frac{1}{2}S(\rho) - \delta$, where $\rho = (\mathbb{I}\otimes\Lambda)|\Psi^+\rangle\langle\Psi^+|$. As the rate for the average over stabilizer codes attains rate R there must exist particular codes with rate R and arbitrarily small average failure probability. Expurgation, that is, removal of half of the codewords corresponding to the highest probabilities of error, may then be used on such codes to assure that the maximal probability of block error for such a code is also arbitrarily small, with minimal effect on the rate of the new code [31]. Thus the capacity is given by

$$Q_E = 1 - \frac{1}{2}S(\rho), \tag{A3}$$

for entanglement-assisted codes using $\mathcal{E} = \frac{1}{2}S(\rho)$ e-bits per channel.

In the case of the qubit erasure channel, with erasure probability ϵ, the location of each of the errors is known. For large n the number of typical errors approaches $4^{n\epsilon}$, giving a average failure probability

$$P(\text{fail}) \leqslant 2^{2n\epsilon+2n\delta} 2^{-(2n-2k)} + \eta \leqslant 2^{2n(\epsilon-1+R+\delta)} + \eta, \tag{A4}$$

which vanishes for large n, provided $R < 1-\epsilon-\delta$ for any $\delta > 0$. Hence, the capacity obtained in this case is

$$Q_E = 1 - \epsilon, \tag{A5}$$

using $\mathcal{E} = \epsilon$ e-bits per channel.

The amount of entanglement required in both these cases stems from the number of entangled states, $m = n-k$, utilized in the code. Dividing through by the number of channels n we have an amount of entanglement $\mathcal{E} = 1 - R > 1 - Q_E + \delta$ per channel in the random coding derivation. Hence, in these cases the required entanglement is given by $\mathcal{E}_Q^{\text{Random}} = 1 - Q_E$.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[2] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[3] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[4] C.H. Bennett, P.W. Shor, J.A. Smolin, and A.V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).

[5] C.H. Bennett, P.W. Shor, J.A. Smolin, and A.V. Thapliyal, IEEE Trans. Inf. Theory **48**, 2637 (2002).

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).

[7] C. Adami and N.J. Cerf, Phys. Rev. A **56**, 3470 (1997).

[8] H.-K. Lo and S. Popescu, Phys. Rev. Lett. **83**, 1459 (1999).

[9] P.W. Shor, Phys. Rev. A **52**, R2493 (1995).

[10] A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[11] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).

[12] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[13] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[14] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).

[15] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[16] R. Cleve, Phys. Rev. A **55**, 4054 (1997).

[17] P. Shor and R. Laflamme, Phys. Rev. Lett. **78**, 1600 (1997).

[18] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[19] D.A. Lidar, D. Bacon, and K.B. Whaley, Phys. Rev. Lett. **82**, 4556 (1999).

[20] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).

[21] P. Zanardi, Phys. Rev. A **63**, 012301 (2001).

[22] D. Bruß, D.P. DiVincenzo, A. Ekert, C.A. Fuchs, C. Macchiavello, and J.A. Smolin, Phys. Rev. A **57**, 2368 (1998).

[23] N.J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).

[24] E.M. Rains, IEEE Trans. Inf. Theory **44**, 1388 (1998).

[25] D. Gottesman, e-print quant-ph/9705052.

[26] R. Laflamme, C. Miquel, J.P. Paz, and W.H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).

[27] C.H. Bennett, D.P. DiVincenzo, and J.A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).

[28] H. Barnum, J.A. Smolin, and B.M. Terhal, Phys. Rev. A **58**, 3496 (1998).

[29] G. Bowen and S. Bose, Phys. Rev. Lett. **87**, 267901 (2001).

[30] D.P. DiVincenzo, P.W. Shor, and J.A. Smolin, Phys. Rev. A **57**, 830 (1998).

[31] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms* (Cambridge University Press, London, 2001), URL: http://wol.ra.phy.cam.ac. uk/mackay/itprnn/book. html