Theory of quantum error-correcting codes

Emanuel Knill[1,*] and Raymond Laflamme[2,†]
[1]CIC-3, Mail Stop B265, Los Alamos National Laboratory, New Mexico 87545
[2]T-6, Mail Stop B288, Los Alamos National Laboratory, New Mexico 87545

(Received 14 June 1996)

Quantum error correction will be necessary for preserving coherent states against noise and other unwanted interactions in quantum computation and communication. We develop a general theory of quantum error correction based on encoding states into larger Hilbert spaces subject to known interactions. We obtain necessary and sufficient conditions for the perfect recovery of an encoded state after its degradation by an interaction. The conditions depend only on the behavior of the logical states. We use them to give a recovery-operator-independent definition of error-correcting codes. We relate this definition to four others: the existence of a left inverse of the interaction, an explicit representation of the error syndrome using tensor products, perfect recovery of the completely entangled state, and an information theoretic identity. Two notions of fidelity and error for imperfect recovery are introduced, one for pure and the other for entangled states. The latter is more appropriate when using codes in a quantum memory or in applications of quantum teleportation to communication. We show that the error for entangled states is bounded linearly by the error for pure states. A formal definition of independent interactions for qubits is given. This leads to lower bounds on the number of qubits required to correct e errors and a formal proof that the classical bounds on the probability of error of e-error-correcting codes applies to e-error-correcting quantum codes, provided that the interaction is dominated by an identity component. [S1050-2947(97)07501-X]

PACS number(s): 03.65.Bz, 89.70.+c, 89.80.+h, 02.70.−c

I. INTRODUCTION

Within the past few years, quantum computation and communication have undergone a dramatic evolution. From being subjects of primarily academic interest, they have become fields having an enormous potential for revolutionizing computer science and cryptography, as well as an impact on issues of national security, and even potentially commercializable applications. This has resulted not only from the development of new algorithms such as quantum factoring [1], but also as a consequence of recent experimental work on implementations of individual quantum gates [2–4] and of quantum cryptography [5].

Unfortunately, the quantum states required to carry out a computation are very sensitive to the imperfections of the hardware, and above all, to the decoherence [6] caused by interaction with the environment (by environment we mean all the degrees of freedom which can have unwanted interactions with the computer). This fragility of a quantum computer [7–9] is closely tied to its function: it acts as a sophisticated, nonlinear interferometer. The coherent interference pattern between the multitude of superpositions is essential for taking advantage of quantum parallelism, which is the key feature allowing one to explore aspects of an exponentially large number of possible solutions.

To ensure that the fragility of quantum states does not destroy our ability to extract the desired interference pattern requires techniques for correcting errors. It is interesting to draw a parallel between the state of the art in quantum computation today and that of classical computers in the 1940s. At that time it was often said that classical computers would not be very useful because errors in the computer itself would render the result untrustworthy [10]. These doubts disappeared after the discovery of powerful error-correction techniques. Similar doubts are being expressed about the feasibility of the large scale application of quantum computers. These doubts are partially based on the belief that to perform an error-correction step, knowledge of the exact state of the computer is required. Such knowledge would destroy the quantum mechanical properties of the state. However, Shor [11] has shown that in a restricted model of errors (similar to that which is assumed for classical error correction) it is possible to restore a state using only partial knowledge of the state of the quantum computer. Many codes have since been discovered which correct for specific interactions [12–18]. As a result, it may now be possible to implement practical quantum memories and achieve very reliable quantum communication. These ideas have opened the path to a general theory of quantum error correction: the subject of this paper.

This manuscript is organized as follows: In Sec. II, we give an intuitive approach to the theory of quantum error correction and introduce some simple examples of the basic concepts. These concepts are formalized in Sec. III, where the notions of fidelity and error of a code are introduced. Instead of considering explicit encoding and decoding operators, we introduce recovery superoperators. These operators allow us to study the most general physical processes which can be used for error correction. Quantum error-correcting codes which permit complete restoration of the encoded state can then be characterized. We give necessary and sufficient conditions for being able to recover the state of a system after it has evolved through a superoperator. These conditions depend only on the subspace of the code. Several equivalent characterizations are possible and we give four:

[*] Electronic address: knill@lanl.gov

[†] Electronic address: laf@time.lanl.gov

one based on the existence of a left inverse of the interaction superoperator, one using the explicit representation of the coding space as a tensor product of the code with a quantum error syndrome, one exploiting the effect of the operators on a completely entangled state, and, finally, one using an information theoretic identity. In Sec. IV we discuss several methods for implementing the recovery operator in practice and point out that if certain additional properties hold, the recovery operator can be substantially simplified. Next, in Sec. V we discuss independent interactions for strings of qubits (or other systems). These types of interactions are the natural generalization of classical independent errors. After a short discussion of the physical interpretation and relevance we give a proof that it is not possible to obtain a one-error-correcting code for one qubit using a coding space of only four qubits. This is generalized in a theorem about correcting e errors and a characterization of e-error-correcting codes. Finally we address the important issue of the fidelity of codes with imperfect recovery operators. We observe that a correct measure of fidelity must take into account any entanglements of the state. We show that the fidelity of the recovery of an entangled state can be bounded below in terms of the pure state fidelity. An example is provided to show that our bound is best possible. We end this section by proving a bound on the fidelity of codes where one of the interaction operators is proportional to the identity. In Sec. VI we conclude the paper with a final summary of the results and their implications.

II. AN INTUITIVE APPROACH

Coherent quantum states are used in quantum communication and quantum computation. Both situations involve the manipulation of states by unitary operations where some desired information is eventually extracted from parts of the state by measurement. Quantum communication involves multiple parties with limited communication capabilities and focuses more on the transmission of states over potentially noisy channels, while quantum computation involves only one party and focuses on the unitary transformations involved in achieving the final state. In both cases, loss of coherence occurs while executing the necessary operations, and when some of the systems are either transmitted or temporarily preserved in memory. This loss of coherence results in a reduction of the probability of getting the correct answer after completion of the required operations. For short distance communication or small scale computations, the best way to avoid errors is to minimize this loss by isolating the state as well as possible and improving the accuracy of the unitary transformation used. For larger distances and long calculations errors in the state are inevitable and it is necessary to devise a scheme for returning the state to the desired one. Here we focus on the problem of preserving a coherent state subject to unwanted interactions in a quantum memory or channel.

In classical communication and computer memories, corrupted information can be restored by introducing redundancy, for example by copying all or part of the information to be preserved [19]. Unfortunately, it is not possible to use a simple redundancy scheme for quantum states, primarily because the ‘‘no-cloning’’ theorem [20] prevents the duplication of quantum information. However, it has recently been realized [11] that it is possible to correct a state against certain known errors by spreading the information over many qubits through an encoding. The goal is to find an encoding which behaves in a specific way (described below) under evolution by the interaction superoperator. The behavior is such that it permits recovery of the original state. This works only for specific types of superoperators. In practice, error-correction schemes cannot correct all errors perfectly but only a subset of them. The quality of a scheme can be evaluated by its fidelity, i.e., the overlap between the corrected state with the wanted one.

An essential part of the error-correction scheme is the encoding of the quantum information. Consider the simplest nontrivial case of encoding a single qubit. In this case the general state to be protected is of the form $|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle$. The idea is to map $|\Psi\rangle$ into a higher dimensional Hilbert space (using ancilla qubits which are assumed to be in their $|0\rangle$ states initially):

$$(\alpha|0\rangle+\beta|1\rangle)|000\cdots\rangle\rightarrow\alpha|0_L\rangle+\beta|1_L\rangle. \tag{1}$$

This defines the code. $|0_L\rangle$ and $|1_L\rangle$ are called the logical zero and the logical one of the qubit which we want to preserve, respectively. The new state in Eq. (1) should be such that any error induced by an incorrect functioning of the computer maps it into one of a family of two-dimensional subspaces which preserve the relative coherence of the quantum information (i.e., in each subspace, the state of the computer should be in a tensor product state with the environment). A measurement is then performed which projects the state into one of these subspaces. The original state can be recovered by a unitary transformation which depends on which of these subspaces has been observed. A fact to be established in Sec. IV is that for every error-correcting code, the original state can be recovered by a measurement followed by a unitary operation determined by the outcome of the measurement.

In order to find good encodings, it is essential to understand the types of error which can occur. We assume that the initial state is Ψ_i, which undergoes interaction with an environment. This leaves the computer in the reduced density matrix

$$\rho_f=\$(|\Psi_i\rangle), \tag{2}$$

where \$ is the superoperator associated with the interaction. In the case where the environment is not initially entangled with the system ρ_f can be written in the form [21]

$$\rho_f=\sum_a A_a\rho_i A_a^\dagger. \tag{3}$$

A choice of operators A_a can be determined from an orthonormal basis $|\mu_a\rangle$ of the environment, the environment's initial state $|e\rangle$, and the evolution operator U of the whole system as follows:

$$A_a=\langle\mu_a|U|e\rangle. \tag{4}$$

With A_a written in this way, it can be seen that

$$\sum_a A_a^\dagger A_a = I. \tag{5}$$

The A_a are linear operators of the Hilbert space of the system and describe the effect of the environment. The A_a are called interaction operators. Any family of operators A_a which satisfies Eq. (5) defines a superoperator. Note that the choice of interaction operators is not unique; they depend on the choice of the basis $|\mu_a\rangle$ of the environment. Two sets of interaction operators which differ only by this choice are physically equivalent.

If there is no prior knowledge of the interaction operators which corrupt an encoded state, it is not possible to recover $|\Psi_i\rangle$ consistently. However, in many physical systems the A_a are of a restricted form. For example, a reasonable approximation for systems of qubits is that the interaction with the environment is independent for each qubit. In this case the interaction operators are tensor products of one-qubit interaction operators. For small error rates, it might also be that one of the one-qubit interaction operators, say A_0, is near the identity. One can then define the number of errors of an interaction by counting the number of operators in the tensor product which are not A_0. If there is a sufficiently small number of errors, it may be possible to retrieve the original state just as for classical error correction.

Necessary and sufficient conditions for recovery of the state $|\Psi_i\rangle$ are (see Sec. III)

$$\langle 0_L|A_a^\dagger A_b|1_L\rangle = 0, \tag{6}$$

$$\langle 0_L|A_a^\dagger A_b|0_L\rangle = \langle 1_L|A_a^\dagger A_b|1_L\rangle. \tag{7}$$

The first condition states that the logical zero and one must go to orthogonal states under any error. The second one implies that the length and inner products of the projections of the corrupted logical zero and one should be the same.

A sufficient but not necessary condition is that Eq. (7) is zero if A_a and A_b are different. This implies that each error maps the initial state to orthogonal subspaces. Obviously this permits retrieval of the original state by projecting on these subspaces. The more general Eq. (7) leaves room for two different errors to be mapped on the same two-dimensional subspace. This possibility is allowed by the superposition principle of quantum mechanics but cannot occur in classical error correction.

For realistic quantum computers only a subset of possible errors can be corrected. An appropriate measure of the quality of a recovered code is the fidelity [22]. Fidelity is the overlap between the final state ρ_f of a system ρ and the original state $|\Psi_i\rangle$. If the combined superoperator consisting of an interaction with the environment followed by a recovery operation is given by $\mathcal{A}=\{A_0,\ldots\}$, then the fidelity is

$$F(|\Psi_i\rangle,\mathcal{A}) = \langle\Psi_i|\rho_f|\Psi_i\rangle = \sum_a \langle\Psi_i|A_a|\Psi_i\rangle\langle\Psi_i|A_a^\dagger|\Psi_i\rangle. \tag{8}$$

It gives the probability that the final state would pass a test checking whether it agrees with the initial state. As we are thinking of encoding arbitrary states, we do not know in advance the state that will be used. We therefore use the minimum fidelity (that is, the worst-case fidelity)

$$F_{\min} = \min_{|\Psi\rangle}\langle\Psi|\rho_f|\Psi\rangle. \tag{9}$$

The best quantum code maximizes $F_{\min}$. Hereafter we will drop the subscript min to denote the fidelity of a code.

We now turn to a simple but important example to illustrate some of the points mentioned above. We investigate decoherence [6], i.e., the randomization of the phase of the initial state $|\Psi_i\rangle$. The effect of decoherence is to decrease the size of the diagonal element of the density matrix in a basis determined by the interaction Hamiltonian with the environment. For one qubit, decoherence takes the form

$$|\Psi_i\rangle = \alpha|0\rangle + \beta|1\rangle \to \rho\begin{pmatrix} \alpha\alpha^* & \alpha\beta^* e^{-\gamma} \\ \alpha^*\beta e^{-\gamma} & \beta\beta^* \end{pmatrix}, \tag{10}$$

where $e^{-\gamma}$ ($\gamma \geqslant 0$) parametrizes the amount of decoherence. Decoherence can be understood in terms of the following interaction with the environment:

$$|e\rangle|0\rangle \to |e_0\rangle|0\rangle,$$

$$|e\rangle|1\rangle \to |e_1\rangle|1\rangle, \tag{11}$$

with $\langle e_0|e_1\rangle = e^{-\gamma}$. Using the environment basis $|\mu_0\rangle = |e_0\rangle$ and $|\mu_1\rangle = (|e_1\rangle - e^{-\gamma}|e_0\rangle)/\sqrt{1-e^{-2\gamma}}$ we obtain the interaction operators

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\gamma} \end{pmatrix}; \quad A_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{1-e^{-2\gamma}} \end{pmatrix}. \tag{12}$$

For a single qubit which is corrupted by decoherence the minimum fidelity can be seen to be given by

$$F = \frac{1+e^{-\gamma}}{2} \sim 1 - \frac{\gamma}{2} + \cdots , \tag{13}$$

where the last approximation is valid for small γ.

In what follows we assume that the different qubits have independent environments (a physically reasonable approximation) so that the interaction operators are tensor products of the ones given in Eq. (12).

A one-qubit code to correct this type of error by using three qubits has been devised in Refs. [11,12]. To understand how it works, it is better to change the basis state of the environment to $|\mu_+\rangle = (|e_0\rangle + |e_1\rangle)/\sqrt{2(1+e^{-\gamma})}$ and $|\mu_-\rangle = (|e_0\rangle - |e_1\rangle)/\sqrt{2(1-e^{-\gamma})}$. This gives the one-qubit interaction operators

$$A_+ = a_+\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad A_- = a_-\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{14}$$

where $a_+ = \sqrt{(1+e^{-\gamma})/2}$ and $a_- = \sqrt{(1-e^{-\gamma})/2}$. In this basis, the effect of the environment is either to leave the system alone or flip the sign if the qubit is in the state $|1\rangle$. The encoding has the form

$$|0_L\rangle = (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle),$$

$$|1_L\rangle = (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle). \tag{15}$$

This code is such that if one qubit is corrupted by the environment, then it is possible to detect it by using a majority rule.

Assuming at most one incorrect qubit, the interaction with the environment maps the initial state to one of the following possibilities:

$$A_+|0_L\rangle = a_+^{3/2}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle),$$

$$A_-^1|0_L\rangle = a_+^2 a_-^{1/2}(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle),$$

$$A_-^2|0_L\rangle = a_+^2 a_-^{1/2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle),$$

$$A_-^3|0_L\rangle = a_+^2 a_-^{1/2}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle-|1\rangle), \quad (16)$$

where the superscripts on the operator A_- indicate which qubit is being affected. A similar result applies to $|1_L\rangle$. The recovery operator is the superoperator determined by the interactions

$$R_+ = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|),$$

$$R_-^1 = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|)\sigma_z^1,$$

$$R_-^2 = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|)\sigma_z^2,$$

$$R_-^3 = (|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|)\sigma_z^3, \quad (17)$$

where σ_z^r is the z Pauli matrix for the rth qubit. In practice the recovery operator is implemented by first performing a measurement to determine which error has occurred. This can be achieved by using a series of controlled-NOT gates and measurements (with the possible involvement of ancilla qubits) [12]. The measurements establish the relative signs in Eq. (16). Note that these relative signs are the same for the logical zero and one after the same operator has acted and therefore the measurements collapse the system to two-dimensional subspaces. Once the measurements reveal which subspace has actually occurred, it is straightforward to recover the initial state with an appropriate unitary transformation.

It is important to realize that this code corrects perfectly only if at most one error occurs. In general, however, decoherence can induce more than one error [as can be deduced from the fact that the A_a in Eq. (16) do not form a superoperator]. As long as the decoherence is small (i.e., γ is small), the probability of having two or more errors will be much smaller than that of having one error. The minimum fidelity can be bounded below by

$$F = 1-(a_-^3 + 3a_-^2 a_+) \approx 1 - \tfrac{3}{4}\gamma^2 + \cdots . \quad (18)$$

This scheme is thus an improvement over the single qubit evolution for a small enough γ. Using a $2n+1$ bit generalization of the code in Eq. (15), it is possible to have fidelity be given by $1-O(\gamma^{n+1})$ for small γ, but with a potentially large hidden constant.

III. QUANTUM ERROR-CORRECTING CODES

A. Fundamentals of quantum error-correcting codes

It is now time to give a formal treatment of quantum codes. We want to preserve a 2^k-dimensional subspace against some known errors. This is accomplished by mapping the states into a larger, 2^n-dimensional Hilbert space. First, let us define an (n,k) quantum code as a 2^k-dimensional subspace of an 2^n-dimensional Hilbert space. The latter is called the coding space and denoted by $\mathcal{H}$. The symbol $\mathcal{C}$ is used for the code. An encoding operator for $\mathcal{C}$ is a unitary operator E from a k-dimensional Hilbert space $\mathcal{Q}$ onto $\mathcal{C}$. A decoding operator is a right inverse of an encoding operator.

The encoding operator can be implemented as a unitary operator on $Q^{\otimes k}\otimes Q^{\otimes n-k}\otimes Q^{\otimes a}$, where the last factor has a ancillary qubits whose state before and after the operation is intended to be $|0\rangle$. The ancillas can be used as scratch pad memory during the process of measurement needed to recover $\mathcal{C}$. In this case, the space $\mathcal{Q}$ to be encoded is a ''standard'' subspace of the coding space, and the encoding operator maps it to the intended code. Note that there are many encoding operators which have the same effect on $\mathcal{Q}$. This is because the encoding defines only a part of the unitary transformation needed. Which choice is actually used depends on efficiency (e.g., the number of gates in a physical situation) as well as the desired error-correcting properties.

For the purpose of discussing error-correcting properties of codes, instead of focusing on encoding and decoding operators, we introduce the recovery superoperator. A recovery (super)operator $\mathcal{R}$ is a superoperator on the coding space. A recovery operator is used to restore a state to the code after it has been affected by an interaction with the environment. Note that except for their intended use, recovery and interaction operators are the same type of object.

Use of a recovery operator instead of an explicit unitary operator allows us to ignore many of the details of implementing a code which are not relevant to its error-correcting properties. It is general enough to represent potentially unintended or unavoidable side effects of the more traditional decode-encode operations. In practice, a recovery operator may be implemented by a combination of unitary operations and classical measurements or by unitary operations alone.

A quantum error-correcting code is a pair $(\mathcal{C},\mathcal{R})$ consisting of a quantum code and a recovery operator. The correcting properties of an error-correcting code depend on the interaction with the environment. Let $\mathcal{A}$ be a family of linear operators as described in Eq. (3). The fidelity of the code is determined by the fidelity of the composition $\mathcal{R}\mathcal{A}$ restricted to $\mathcal{C}$. The fidelity of the error-correcting code is thus defined as

$$F(\mathcal{C},\mathcal{R}\mathcal{A}) = \min_{|\Psi\}\in\mathcal{C}} F(|\Psi\rangle,\mathcal{R}\mathcal{A}) = \min_{|\Psi\rangle\in\mathcal{C}} \sum_{r,a} |\langle\Psi|R_r A_a|\Psi\rangle|^2,$$

where the R_r are the interaction operators for the superoperator $\mathcal{R}$. It is useful to consider families of linear operators which do not necessarily satisfy the superoperator constraint Eq. (5). In that case the fidelity as defined above is not correctly normalized and instead we consider the error of the code. The error of the code is defined as

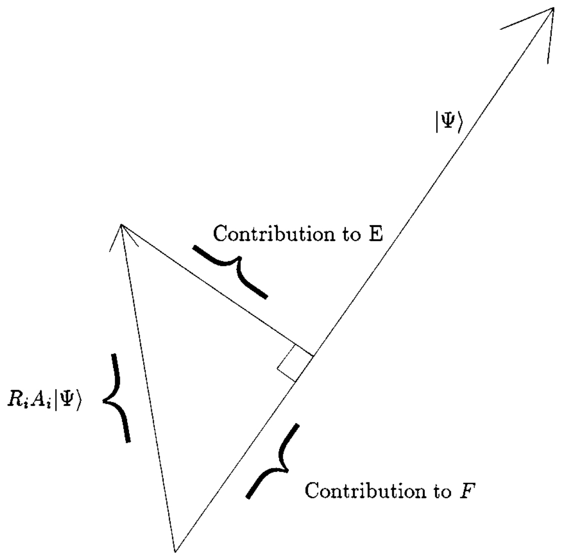

FIG. 1. Geometric relation between fidelity and error. The fidelity is the sum of the projections (for each interaction operator) along the state. The error gives the ''distance'' from the original state for each interaction operator.

$$E(\mathcal{C},\mathcal{R}\mathcal{A})=\max_{|\Psi\rangle\in\mathcal{C}}\sum_{r,a}|(R_rA_a-\langle\Psi|R_rA_a|\Psi\rangle)|\Psi\rangle|^2.$$

Figure 1 gives a geometric picture of the notion of fidelity and error of a code. The error of the code makes sense for arbitrary families $\mathcal{A}$. For superoperators, it is given by $1-F(\mathcal{C},\mathcal{R}\mathcal{A})$, which is the worst-case probability of not observing the desired state if we were to attempt to measure it directly.

We first focus on the ideal case where the code corrects all errors, i.e., when the initial state is recovered perfectly for all operators in $\mathcal{A}$. The case of imperfect recovery will be discussed later. The pair $(\mathcal{C},\mathcal{R})$ is an $\mathcal{A}$-correcting code if $E(\mathcal{C},\mathcal{R}\mathcal{A})=0$. Note that this is equivalent to saying that for each A_a, $E(\mathcal{C},\mathcal{R}A_a)=0$. Thus we can speak of $\mathcal{A}$-correcting codes even if $\mathcal{A}$ is not finite. In the next subsection we use characterizations of $\mathcal{A}$-correcting codes to slightly modify this definition by omitting explicit mention of the recovery operator.

Before we characterize $\mathcal{A}$-correcting codes, let us turn the problem around and ask what the family $\mathcal{A}(\mathcal{C},\mathcal{R})$ of operators A for which $(\mathcal{C},\mathcal{R})$ is $\mathcal{A}$-correcting looks like. The next result gives an answer.

Theorem III.1. The operator A_a is in $\mathcal{A}(\mathcal{C},\mathcal{R})$ iff when restricted to $\mathcal{C}$, $R_rA_a=\lambda_{ra}I$ for each $R_r\in\mathcal{R}$. The family $\mathcal{A}(\mathcal{C},\mathcal{R})$ is linearly closed and $(\mathcal{C},\mathcal{R})$ is $\mathcal{A}(\mathcal{C},\mathcal{R})$ correcting.

Proof. To be A_a correcting requires that for $|\Psi\rangle\in\mathcal{C}$,

$$|(R_rA_a-(\langle\Psi|R_rA_a|\Psi\rangle))|\Psi\rangle|=0.$$

This implies that $R_rA_a|\Psi\rangle=\lambda_{ra}(|\Psi\rangle)|\Psi\rangle$. By linearity of R_rA_a, $\lambda_{ra}(|\Psi\rangle)$ cannot depend on $|\Psi\rangle$. The rest of the theorem is immediate. QED.

B. Characterizations of $\mathcal{A}$-correcting codes

So far we have defined $\mathcal{A}$-correcting codes both in terms of the code and the recovery operator. One of the most important consequences of the characterizations of $\mathcal{A}$-correcting codes below is to allow defining $\mathcal{A}$-correcting codes without reference to the recovery operator. Let $|i_L\rangle$ denote the elements of an orthonormal basis of the code $\mathcal{C}$. The first characterization has proved the most useful so far for finding good codes by systematic searches such as that in [15] or by exploiting linear techniques from the classical theory of error-correcting codes [12,13].

Theorem III.2. The code $\mathcal{C}$ can be extended to an $\mathcal{A}$-correcting code iff for all basis elements $|i_L\rangle$, $|j_L\rangle$ $(i\neq j)$ and operators A_a, A_b in $\mathcal{A}$

$$\langle i_L|A_a^\dagger A_b|i_L\rangle=\langle j_L|A_a^\dagger A_b|j_L\rangle \tag{19}$$

and

$$\langle i_L|A_a^\dagger A_b|j_L\rangle=0. \tag{20}$$

These conditions are more general than the ones given in [23], which are sufficient but not necessary. Since they are independent of a recovery operator, we can define an $\mathcal{A}$-correcting code as one which satisfies Eq. (19) and Eq. (20) for any one (and therefore every) basis of the code.

Proof. Assume that $(\mathcal{C},\ \mathcal{R})$ is an $\mathcal{A}$-correcting code. We compute $\langle i_L|A_a^\dagger A_b|j_L\rangle$ explicitly.

$$\begin{aligned}\langle i_L|A_a^\dagger A_b|j_L\rangle&=\langle i_L|A_a^\dagger IA_b|j_L\rangle=\left\langle i_L\left|A_a^\dagger\sum_r R_r^\dagger R_rA_b\right|j_L\right\rangle\\&=\sum_r\langle i_L|A_a^\dagger R_r^\dagger R_rA_b|j_L\rangle=\sum_r\langle i_L|\overline{\lambda_{ar}}\lambda_{br}|j_L\rangle\\&=\alpha_{ab}\delta_{ij},\end{aligned}$$

where we have used the superoperator properties of $\mathcal{R}$ and Theorem III.1. The forward direction of the theorem now follows by inspection.

Let us now show how to construct a recovery operator given that Eq. (19) and Eq. (20) hold. Call $\mathcal{V}^i$ the subspace spanned by $A_a|i_L\rangle$ (for all a). By Eq. (20), the $\mathcal{V}^i$ are orthogonal subspaces. Let $|\nu_r^i\rangle$ be an orthonormal basis for $\mathcal{V}^i$. We shall shortly impose additional conditions on the $|\nu_r^i\rangle$. For now, observe that the $|\nu_r^i\rangle$ are mutually orthogonal. Hence there exist unitary V_r which return $|\nu_r^i\rangle$ to the corresponding state $|i_L\rangle$:

$$V_r|\nu_r^i\rangle=|i_L\rangle. \tag{21}$$

The recovery operator is given by the interaction operators

$$\mathcal{R}=\{\mathcal{O},R_1,\ldots,R_r,\ldots\}, \tag{22}$$

where $\mathcal{O}$ is the projection onto the orthogonal complement of $\oplus_i\mathcal{V}^i$, i.e., the part of the Hilbert space which is not reached by acting on the code with the A_a, and

$$R_r=V_r\sum_i|\nu_r^i\rangle\langle\nu_r^i|. \tag{23}$$

That $\mathcal{R}$ is a superoperator follows from the observation that it is a sum of orthogonal projections followed by unitary operators where the projections span the Hilbert space.

To show that $\mathcal{R}$ recovers the state, we need unitary operators U_i such that $U_i|\nu^0_r\rangle = |\nu^i_r\rangle$ and for all A_a, $U_iA_a|0_L\rangle = A_a|i_L\rangle$. The existence of unitary operators satisfying the second condition follows from Eq. (19), according to which the inner-product relationships between the $A_a|0_L\rangle$ and the $A_a|i_L\rangle$ are identical [24]. Given such U_i, $|\nu^i_r\rangle$ can be made to satisfy the remaining condition by choosing the basis $|\nu^0_r\rangle$ of $\mathcal{V}^0$ and defining $|\nu^i_r\rangle = U_i|\nu^0_r\rangle$.

We show that $\mathcal{R}$ does indeed recover the state, i.e., for $\Psi\in\mathcal{C}$, $R_rA_a|\Psi\rangle$ is proportional to Ψ. We can write

$$A_a|\Psi\rangle \equiv A_a\sum_i \alpha_i|i_L\rangle = \sum_i \alpha_i A_a|i_L\rangle = \sum_i \alpha_i U_i A_a|0_L\rangle$$

$$\equiv \sum_{i,r} \alpha_i U_i \beta^0_{ar}|\nu^0_r\rangle = \sum_{i,r} \alpha_i \beta^0_{ar}|\nu^i_r\rangle, \qquad (24)$$

where the identities define α_i and β^0_{ar} by expansion in terms of the corresponding basis elements. The introduction of the operators U_i is what allows us to obtain the expansion in the last line where the β's show no dependence on i. We can now compute $R_rA_a|\Psi\rangle$ as

$$R_rA_a|\Psi\rangle = \sum_i V_r|\nu^i_r\rangle\left\langle \nu^i_r \middle| \sum_{j,s} \alpha_j\beta^0_{as} \middle| \nu^j_s\right\rangle = \sum_i \alpha_i\beta^0_{ar}V_r|\nu^i_r\rangle$$

$$= \sum_i \beta^0_{ar}\alpha_i|i_L\rangle = \beta^0_{ar}|\Psi\rangle. \qquad (25)$$

This implies that R_rA_a is a multiple of the identity operation on $\mathcal{C}$. Since $\mathcal{O}$ is null on all $A_a|j_L\rangle$, the fact that $\mathcal{R}$ is a recovery operator for $\mathcal{A}$ follows. QED.

An interesting observation about Eq. (19) is that it does not require that the logical states have zero scalar products when two different interactions are applied, but merely that the scalar products are the same. For two-dimensional codes, this means that parts of the subspaces spanned by $A_a|0_L\rangle$ and $A_a|1_L\rangle$ to which the states are mapped may overlap. If we identify each A_a with a distinct error, then this possibility allows the correction of more than one error per two-dimensional subspace. This is a novel feature of quantum error-correcting codes which does not exist in their classical counterparts. The fact that nontrivial overlap is possible is demonstrated by the following example.

Let us consider the code $\{|0_L\rangle = |00\rangle, |1_L\rangle = |11\rangle\}$ subject to the interaction operators

$$A_0 = \begin{pmatrix} \sqrt{1-2q} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \sqrt{1-2q} \end{pmatrix}, \qquad (26)$$

$$A_1 = \begin{pmatrix} \sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{q/2} \\ \sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{q/2} \end{pmatrix},$$

$$A_2 = \begin{pmatrix} \sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{q/2} \\ -\sqrt{q/2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\sqrt{q/2} \end{pmatrix},$$

for some fixed $0<q<1$. It is easy to check that these operators form a superoperator. They are linearly independent and therefore cannot be reduced to a smaller, equivalent interaction. The A_i map the logical states as follows:

$$|0_L\rangle \rightarrow \sqrt{1-2q}|00\rangle, \quad \sqrt{q/2}(|00\rangle + |10\rangle),$$

$$\sqrt{q/2}(|00\rangle - |10\rangle),$$

$$|1_L\rangle \rightarrow \sqrt{1-2q}|11\rangle, \quad \sqrt{q/2}(|01\rangle + |11\rangle),$$

$$\sqrt{q/2}(|01\rangle - |11\rangle). \qquad (27)$$

Naively, one might expect that the states on the right hand sides are linearly independent, but in fact, one of them is linearly dependent on the other two in each case. We therefore need only two recovery operators to retrieve the initial state. They are given by

$$R_0 = |00\rangle\langle 00| + |11\rangle\langle 11|; \quad R_1 = |00\rangle\langle 10| + |11\rangle\langle 01|. \qquad (28)$$

Whether there are any such examples of practical significance is under investigation.

We return to the problem of characterizing quantum error-correcting codes. If $\mathcal{A}$ is a superoperator, then a simple characterization of $\mathcal{A}$-correcting codes is in terms of left invertible superoperators.

Theorem III.3. Let $\mathcal{A}$ be a superoperator. $\mathcal{C}$ is an $\mathcal{A}$-correcting code iff the restriction of $\mathcal{A}$ to $\mathcal{C}$ has a left superoperator inverse.

Proof. By Theorem III.1, $\mathcal{C}$ is an $\mathcal{A}$-correcting code if and only if there exists a superoperator $\mathcal{R}$ such that on $\mathcal{C}$, $R_rA_a = \lambda_{ra}I$ for all r and a. This means that $\mathcal{R}\mathcal{A}$ is a superoperator equivalent to the identity (by a change of basis on the environment). QED.

Interestingly, to check that an operator $\mathcal{B}=\mathcal{R}\mathcal{A}$ has error 0 on any state, it suffices to apply $I\otimes\mathcal{B}$ to a completely entangled state. In other words, checking that the operator $\mathcal{B}$ has zero error for all pure states of a system is equivalent to checking only one state which is completely entangled with a copy of the system.

Theorem III.4. $\mathcal{B}$ has error 0 on $\mathcal{C}$ if and only if $I\otimes\mathcal{B}\Sigma_i|i_L\rangle|i_L\rangle = \lambda\Sigma_i|i_L\rangle|i_L\rangle$.

The equality in the theorem is to be interpreted in terms of state ensembles: Two state ensembles are equivalent iff they induce the same density matrix.

Proof. Let B_r be a member of $\mathcal{B}$. Then $I\otimes B_r$ is a member of $I\otimes\mathcal{B}$. If $\mathcal{B}$ has error 0 on $\mathcal{C}$, then

$$I\otimes B_r\sum_i |i_L\rangle|i_L\rangle = \sum_i |i_L\rangle B_r|i_L\rangle = \sum_i |i_L\rangle\lambda_r|i_L\rangle$$

$$= \lambda_r\sum_i |i_L\rangle|i_L\rangle.$$

This implies that the ensemble $I\otimes\mathcal{B}\Sigma_i|i_L\rangle|i_L\rangle$ is equivalent to a scalar multiple of $\Sigma_i|i_L\rangle|i_L\rangle$.

Now suppose that the identity in the theorem holds. The fact that the left hand side is equivalent (as a set of states) to the right hand side implies that for each r,

$$I\otimes B_r\sum_{\imath}\ |i_L\rangle|i_L\rangle=\lambda_r\sum_{i}\ |i_L\rangle|i_L\rangle.$$

By applying the operator $I\otimes B_r$ to each summand and using the fact that the $|i_L\rangle|i_L\rangle$ are independent, this gives $B_r|i_L\rangle=\lambda_r|i_L\rangle$. The result follows. QED.

An interesting and concise method of describing a code which hides the recovery operator without removing it entirely involves expressing the coding space as a sum of two terms, the first of which is a tensor product of the code with another space. As we will see, this perspective has several interesting consequences. One of these consequences is the explicit distinction between correctable versus detectable errors.

Theorem III.5. $\mathcal{C}$ is an $\mathcal{A}$-correcting code if and only if there is an isomorphism $\sigma:\mathcal{H}\rightarrow\mathcal{C}\otimes\mathcal{E}\oplus\mathcal{D}$ such that for all $A_a\in\mathcal{A}$ and $|\Psi\rangle\in\mathcal{C}$, $A_a|\Psi\rangle=\sigma(|\Psi\rangle\otimes|\mathcal{E}(a)\rangle)$ for some vector $|\mathcal{E}(a)\rangle$ depending on A_a alone.

The idea is to ensure that under each interaction operators the effect of the environment is clearly separated from the state to be preserved. This is essential for the logical state to keep their coherence. $|\Psi\rangle$ is the wave function of a collective degree of freedom which represents the logical state and the state of the remaining degrees of freedom is given by $|\mathcal{E}(a)\rangle$. $\mathcal{E}$ takes up all the information from the environment and final state in $\mathcal{E}$ encodes the environment's effect on the code. The final state $\mathcal{E}$ is called the error syndrome. $\mathcal{D}$ is the summand of $\mathcal{H}$, which is normally never reached by $\mathcal{A}$, but which can be used for error detection if so desired. A perfect quantum code is one for which $\mathcal{D}$ is empty and the $|\mathcal{E}(a)\rangle$ span $\mathcal{E}$. Note that in many cases of interest, a multiple of the identity map is in $\mathcal{A}$ (given by A_0 for example). In this case, $\mathcal{C}=\sigma(\mathcal{C}\otimes|\mathcal{E}(0)\rangle)$.

Proof. Let $\mathcal{C}$ be an $\mathcal{A}$-correcting code in $\mathcal{H}$. We use the notation from the proof of Theorem III.2. Let $\mathcal{D}$ be the orthogonal complement of the subspace spanned by the $|\nu_r^i\rangle$. Let $\mathcal{E}$ be the Hilbert space spanned by $\{|\nu_r^0\rangle\}_r$. The isomorphism between $\mathcal{H}$ and $\mathcal{C}\otimes\mathcal{E}\oplus\mathcal{D}$ is established by letting $\sigma(|i_L\rangle|\nu_r^0\rangle)=|\nu_r^i\rangle$ and defining σ to be the identity map on $\mathcal{D}$. Let $A_a\in\mathcal{A}$ and $|\Psi\rangle=\Sigma_j\alpha_j|j_L\rangle\in\mathcal{C}$. Write $A_a|0_L\rangle=\Sigma_r\beta_{ra}^0|\nu_r^0\rangle$. Applying the properties discussed in the proof of Theorem III.2 gives

$$A_a|\Psi\rangle=\sum_{jr}\ \alpha_j\beta_{ar}^0|\nu_r^j\rangle=\sigma\left(\sum_j\ \alpha_j|j_L\rangle\otimes\sum_r\ \beta_{ar}^0|\nu_r^0\rangle\right)$$

$$=\sigma\left(|\Psi\rangle\otimes\sum_r\ \beta_{ra}^0|\nu_r^0\rangle\right).$$

Thus we can let $|\mathcal{E}(a)\rangle=\Sigma_r\beta_{ar}^0|\nu_r^0\rangle$ to prove the ‘‘only if’’ part of the theorem.

For the other direction we show how to construct a recovery operator which restores the code after action of $\mathcal{A}$. Let $|\nu_r^0\rangle$ be a basis of $\mathcal{E}$ and let R_r be the projection onto $\sigma(\mathcal{C}\otimes|\nu_r^0\rangle)$ followed by a unitary operator which maps $\sigma(|i_L\rangle\otimes|\nu_r^0\rangle)$ to $|i_L\rangle$. Let $\mathcal{O}$ be the projection onto $\sigma(\mathcal{D})$. Then the conditions on the A_a imply that R_rA_a is a scalar multiple of the identity, which gives the desired result. QED.

Finally, we mention that for superoperators $\mathcal{A}$, there is a simple information theoretic characterization of $\mathcal{A}$-correcting codes due to Nielsen and Schumacher [25]. Let $|e\rangle=(1/\sqrt{k})\Sigma_i|i_L\rangle|i_L\rangle$ be the perfectly entangled state of the code from which we can define the density matrices:

$$\overline{\rho}=\frac{1}{k}\sum_{ai}\ A_a|i_L\rangle\langle i_L|A_a^\dagger\quad\text{and}\quad\rho=\sum_a\ I\otimes A_a|e\rangle\langle e|A_a^\dagger\otimes I. \tag{29}$$

The entropy of a density matrix σ is denoted by $S(\sigma)$.

Theorem III.6. Let $\mathcal{A}$ be a superoperator. Then $\mathcal{C}$ is an $\mathcal{A}$-correcting code if and only if $S(\overline{\rho})-S(\rho)=\log_2 k$.

The quantity $S(\overline{\rho})-S(\rho)$ is introduced as a natural notion of mutual information in [25]. The proof of the theorem can be found there.

IV. IMPLEMENTING RECOVERY OPERATORS

Let us begin by observing that the recovery operator constructed in Theorem III.2 consists only of projections followed by unitary operators conditional on the result of the projections. Implementing such an operator is conceptually straightforward: First you perform a measurement corresponding to the set of projections, then, depending on the outcome of the measurement, you perform an appropriate unitary operation. However, in quantum computation, it is customary to assume that direct measurements can only be performed in a standard basis of each system. This means that a suitable unitary transformations must be applied first in order to rotate the measurement subspaces.

To discuss various methods for implementing the recovery operator we need the notion of a unitary extension. Let $W=\Sigma_iV_iP_i$, where the P_i are orthogonal projections, and $P_j^\dagger V_j^\dagger V_iP_i=0$ for $i\neq j$. Then a unitary extension of W is any unitary W' which agrees with W on the range of the P_i. The conditions ensure that W' exists.

Let $\mathcal{R}$ be described by the interaction operators $(U_0P_0,\ldots,U_{r_m}P_{r_m})$, where the P_r are projections onto the orthogonal subspaces $\mathcal{P}_r$, and the U_r are unitary. Let $\mathcal{M}$ be a separate (ancillary) system with standard basis $|r_M\rangle$. Let V_r be a unitary operator on $\mathcal{M}$ with the property that $V_r|0_M\rangle=|r_M\rangle$ (i.e., V_r is a unitary extension of $|r_M\rangle\langle 0_M|$). The operator $V=\Sigma_rP_r\otimes V_r$ is unitary and has the property that $\mathcal{P}_r\otimes|0_M\rangle$ goes to $\mathcal{P}_r\otimes|r_M\rangle$. (This is a generalization of the standard controlled-NOT operations in quantum computing.) If $\mathcal{M}$ starts in the state $|0_M\rangle$, then we can perform $\mathcal{R}$ by first applying V, then measuring $\mathcal{M}$ in the standard basis, and finally applying U_r to the coding space if the outcome of the measurement is $|r_M\rangle$. This is in fact the implementation of the recovery operator suggested in [11,12]. If it is necessary to represent the recovery operator by unitary operators without measurement, then the measurement and the final rotation step can be replaced by application of the unitary operator $\Sigma_rU_r\otimes|r_M\rangle\langle r_M|$. However, note that with this procedure, the information about the environment's interaction with the coding space is transferred completely to $\mathcal{M}$. The only effective way in which $\mathcal{M}$ can be reused for subsequent operations is to dissipate that information by a measurement.

Usually when using a code, there will be a time when it is desirable to decode the state into a separate system $\mathcal{C}'$ of the same dimension as $\mathcal{C}$ with standard basis $|i\rangle$. The purpose of decoding the state in this fashion may be to measure it, or to perform unitary operations which cannot easily be applied in the coding space directly, or as the first step in a recovery operation where the second step is to reencode the state. Given an implementation of the recovery operator, one can perform this decoding by following the recovery operator with the application of a unitary extension of the operator $\Sigma_i|0_L\rangle\langle i_L|\otimes|i\rangle\langle 0|$ to $\mathcal{H}\otimes|0\rangle$. This in effect swaps the state from $\mathcal{C}$ to $\mathcal{C}'$ after recovery.

Here is a potentially useful method for decoding without use of ancillas. We use the notation from Theorem III.2. Let Q_i be the projection onto $\mathcal{V}^i$. First apply a unitary extension of $\Sigma_i Q_\iota\otimes|i\rangle\langle 0|$ to $|\psi\rangle\otimes|0\rangle$ in $\mathcal{H}\otimes\mathcal{C}'$. Then apply $\Sigma_i U_i^\dagger \otimes|i\rangle\langle i|$. Finally (if desired) measure $\mathcal{H}$ to put the coding system into a known state. As an alternative to the last unitary transformation, one can measure $\mathcal{H}$ in a special basis and follow the measurement by a unitary operation on $\mathcal{C}'$. One choice for such a basis is given by an arbitrary extension of the set

$$|e_{ir}\rangle=\sum_j \omega^{ij}|\nu_r^j\rangle,$$

where ω is a kth root of unity (we have neglected normalization factors). If the outcome of the measurement is $|e_{ir}\rangle$, then the unitary transformation $\Sigma_j\omega^{-ij}|j\rangle\langle j|$ needs to be applied to $\mathcal{C}'$ to complete the decoding step. If a $k\times k$ Hadamard matrix [19] exists, one can choose the coefficients of $|\nu_r^i\rangle$ and of $|i\rangle\langle i|$ to be 1 or -1.

In many applications, $\mathcal{C}'$ is in fact a subsystem of $\mathcal{H}$, that is, $\mathcal{H}=\mathcal{C}'\otimes\mathcal{E}'$. In that case we can decode a state by using the isomorphism of Theorem III.5. First identify $\mathcal{E}$ with a subspace of $\mathcal{E}'$ and apply a unitary extension D of the operator which takes $\sigma(|i_L\rangle|a\rangle)$ to $|i\rangle|a\rangle$. This can be followed by a measurement of $\mathcal{E}$ to dissipate the error. Note that in the case where the identity map is corrected, such that $\mathcal{C}=\sigma(\mathcal{C}\otimes|a_0\rangle)$, we can apply D^{-1} to $|\psi\rangle|a_0\rangle$ to perform the encoding operation. Now the same circuit can be used for both encoding and decoding. Recovery can be accomplished by applying D, a measurement of $\mathcal{E}$, a restoration of $\mathcal{E}$ to $|a_0\rangle$, and finally reencoding using D^{-1}. The first example of such a configuration was given in [15].

We end this section by making a comment on codes such as the ones suggested by Steane [12] and Calderbank and Shor [13]. These codes have the property that $\mathcal{H}$ can be represented as in Theorem III.5, with the additional property that for a basis $|e_\iota\rangle$ of $\mathcal{E}$ and unitary operators U_{ij},

$$A_a\sigma(|\psi\rangle|e_i\rangle)=\sigma\left(\sum_j U_{ij}|\psi\rangle\alpha_{aj}|e_j\rangle\right)$$

independent of ψ. This implies that each subspace $\sigma(\mathcal{C}\otimes|e_i\rangle)$ is an $\mathcal{A}$-correcting code. This property is particularly useful in iterated applications of the code, where recovery operators and interactions alternate. Effectively, it suffices to project the state after the interaction onto the subspaces $\sigma(\mathcal{C}\otimes|e_i\rangle)$ by using a recovery operator consisting of these projections. The result of the projection is a correct state in an alternative code, so it is not necessary to follow up with a unitary operator. It is, however, necessary to keep track of the sequence of outcomes of the projections, since the U_{ij} change the required interpretation of the logical basis of $\mathcal{C}$.

V. PROPERTIES OF CODES CORRECTING INDEPENDENT INTERACTIONS

A. Independent interactions

It is difficult to discover quantum error-correcting codes for general types of interactions. In the classical theory of error correction, it is often assumed that errors occur independently for each symbol. This assumption seems physically reasonable in many situations. In cases where it is not strictly true it can still lead to a systematic approach for finding high-fidelity error-correcting codes. We now discuss the implications of a similar assumption for the quantum theory. In this case, the set of symbols is replaced by a fixed system such as the qubit. The coding space is a tensor product of independent systems. To say that the interaction operator acts independently on each component system means that it is a tensor product of single system interactions. We shall focus on the case where each system is a qubit to simplify the discussion. Generalizations to larger systems are straightforward. Let $\mathcal{H}=\mathcal{Q}^{\otimes r}=\mathcal{Q}_1\otimes\cdots\otimes\mathcal{Q}_r$. Given a one-qubit superoperator $\mathcal{A}$, we say that $\mathcal{A}^{\otimes r}$ acts independently on each qubit with

$$\mathcal{A}^{\otimes r}=\{A_{i_1}\otimes A_{i_2}\otimes\cdots\}_{i_1,i_2,\ldots}.$$

The assumption of independent interaction is reasonable for the case of spontaneous emission where we can take $\mathcal{A}$ to consist of

$$S_0=\begin{pmatrix}1 & 0\\ 0 & \sqrt{1-p^2}\end{pmatrix},\quad S_1=\begin{pmatrix}0 & p\\ 0 & 0\end{pmatrix}.$$

For phase randomization (decoherence) independence is a good approximation when the effective wavelength of the environment is smaller than the interspacing of the physical system used as qubits. For example, if the environment is modeled by a bath at finite temperature, the condition is that the De Broglie wavelength is smaller than the qubit's interspacing. The one-qubit phase randomization interactions were given in Eq. (12).

As in classical error correction with fixed error rates, it is in general not possible to correct $\mathcal{A}^{\otimes r}$ with error 0. And just as in the classical case, it is useful to consider codes which correct well the ''important'' members of $\mathcal{A}^{\otimes r}$, that is, those which strongly affect only a few of the qubits. This leads to the study of e-error-correcting quantum codes.

An operator A acting on $\mathcal{H}$ is said to induce (at most) e errors if it is an r-fold tensor product of one-qubit operators where all but e of them are the identity. An e-error-correcting code is one which can recover from all interaction operators inducing at most e errors.

To discuss e error correction in more detail, we need a linear basis for the one-qubit interactions. One such basis with the additional property that each operator is unitary is given by

$$A_0=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix};\quad A_1=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix};$$

$$A_2=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix};\quad A_3=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}. \tag{30}$$

These A_a operators physically correspond to: (0) leaving the system unchanged, (1) changing the sign of the bit if it is in the $|1\rangle$ state, (2) flipping the bit, (3) flipping the bit and changing its sign if it was in the $|1\rangle$ state.

Another useful basis for the one qubit interactions is given by

$$\widetilde{A}_0=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix};\quad \widetilde{A}_1=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix};$$

$$\widetilde{A}_2=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix};\quad \widetilde{A}_3=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}. \tag{31}$$

The operators $\widetilde{A}_0$ and $\widetilde{A}_1$ implement an ideal measurement on the qubit. $\widetilde{A}_2$ and $\widetilde{A}_3$ implement an ideal measurement followed by a bit flip.

The basis in Eq. (30) is the one used in [15] to find the one-error-correcting five-qubit code.

B. Simple lower bound

One of the simplest lower bounds on the number of classical code words given that at least e errors are to be corrected is the Hamming bound. It is obtained by counting the number b_e of words within e errors of each code word. The product of b_e and the number of code words cannot exceed the size of the coding space.

For quantum codes, one can attempt a similar argument. Assume that we have written the superoperator $\mathcal{A}$ in a minimal form so that each A_a is independent. In the special case where Eq. (19) is solved by setting both sides to 0, it is clear that all states of the form $A_a|i_L\rangle$ are independent. This implies that the total dimension of the space has to be at least $2^k|\mathcal{A}|$. This argument fails because no such independence is implied by Eq. (19) and Eq. (20). One can, however, use Theorem III.5 to see that the total dimension has to exceed $2^k e$, where e is the dimension of $\mathcal{E}$. If a lower bound on $\dim(A_0|\Psi\rangle,\ldots,A_{a_m}|\Psi\rangle)$ is known, then this is a lower bound on e.

As an example, consider the question of whether there are $(2^r,2)$ codes with $r\leqslant 4$ qubits such that any operator which induces at most one error can be corrected. A natural basis for this family of operators can be derived from the basis in Eq. (30) and consists of $1+3r$ operators. Solving $2(1+3r)\leqslant 2^r$ suggests that r must be at least 5. See [15] for an example of a code with $r=5$. As was pointed out in the previous paragraph, this argument is incomplete.

We present here a different argument which proves that $r=5$ is the minimum for one-error-correcting codes. Assume a code with $r=4$ exists. We use the necessary and sufficient conditions given in Eqs. (19) and (20) and expand the logical zero and one as

$$|0_L\rangle=\sum_{ijkl}\alpha_{ijkl}|ijkl\rangle,$$

$$|1_L\rangle=\sum_{ijkl}\beta_{ijkl}|ijkl\rangle, \tag{32}$$

and use the interaction operators described in Eq. (31). Let us define the reduced density matrices

$$\rho^0_{i'j'ij}=\sum_{kl}\alpha^*_{i'j'kl}\alpha_{ijkl},$$

$$\rho^1_{i'j'ij}=\sum_{kl}\beta^*_{i'j'kl}\beta_{ijkl}. \tag{33}$$

Using those operators which induce an error on the last two qubits in Eq. (20) we get

$$\sum_{ij}\alpha^*_{ij00}\beta_{ij00}=0,$$

$$\sum_{ij}\alpha^*_{ij10}\beta_{ij00}=0,$$

$$\vdots$$

$$\sum_{ij}\alpha^*_{ij11}\beta_{ij11}=0, \tag{34}$$

from which we conclude that the density matrices are orthogonal, i.e.,

$$(\rho^0\rho^1)_{iji'j'}=\sum_{klk'l'}\alpha^*_{ijkl}\underbrace{\sum_{i''j''}\alpha_{i''j''kl}\beta^*_{i''j''k'l'}}_{=0\ \text{by Eq. (34)}}\beta_{i'j'k'l'}=0. \tag{35}$$

On the other hand, Eq. (19) implies that these two density matrices are equal: Using those operators which induce an error in the first two qubits, we get

$$\sum_{ij}\alpha^*_{00ij}\alpha_{00ij}=\sum_{ij}\beta^*_{00ij}\beta_{00ij},$$

$$\sum_{ij}\alpha^*_{10ij}\alpha_{10ij}=\sum_{ij}\beta^*_{10ij}\beta_{10ij},$$

$$\vdots$$

$$\sum_{ij}\alpha^*_{11ij}\alpha_{11ij}=\sum_{ij}\beta^*_{11ij}\beta_{11ij}, \tag{36}$$

from which we deduce

$$\rho^0_{iji'j'}=\sum_{kl}\ \alpha^*_{ijkl}\alpha_{i'j'kl}$$

$$=\sum_{kl}\ \beta^*_{ijkl}\beta_{i'j'kl}$$

$$=\rho^1_{iji'j'}. \tag{37}$$

Equation (35) and Eq. (37) are inconsistent and imply that no such code exists.

The argument presented above can be generalized to the following theorem.

Theorem V.1. A(n,k) e-error-correcting quantum code must satisfy $n\geqslant 4e+k$.

The task of proving this theorem is much simplified by characterizing e-error correction in terms of the reduced density matrices of the code words. Let the qubits of the coding space be labeled by $1,\ldots,r$. For $U\subseteq\{1,\ldots,r\}$, let $\rho(|x\rangle,U)$ be the reduced density matrix of $|x\rangle$ on the qubits labeled by elements of U. The complement of U is denoted by U.

Theorem V.2. $\mathcal{C}$ is an e-error-correcting code if and only if for all $U\subseteq\{1,\ldots,r\}$ with $|U|=2e$: (i) for all i, j, $\rho(|i_L\rangle,U)=\rho(|j_L\rangle,U)$ and (ii) for $i\neq j$, $\rho(|i_L\rangle,U)\rho(|j_L\rangle,U)=0$.

The proofs of Theorems V.1 and V. 2 will be given elsewhere using a straightforward generalization of the techniques in the earlier proof of the bound on one error correction.

C. Relationship between the pure state and entangled state fidelity

We have studied the recovery of corrupted states using error-correction codes. It is anticipated that the states to be protected involve only a subset of the entangled qubits of the computer or communication channel. This means that in discussions of fidelity and error, the whole state, not just the component being protected, must be considered. Naturally we can compute the fidelity of a code taking into account any part of the state not directly involved in the interaction and recovery. The worst-case fidelity for such states is referred to as the entangled state fidelity to distinguish it from the pure state fidelity introduced earlier.

If the pure state fidelity after recovery of the coded subsystem is one, then the entangled state fidelity is one also; it does not matter if the state is pure or if it is entangled with other systems. This observation is invalid if we have imperfect fidelity.

Theorem V.3. If the pure state fidelity is $F_p=1-\epsilon$, then the entangled state fidelity is $F_e\geqslant 1-3\epsilon/2$. There are examples where this bound is achieved.

Proof. We give the proof for the case where the system is two-dimensional. We have

$$F_p=\min_{|\psi\rangle\in\mathcal{C}}\langle\Psi|\rho|\Psi\rangle=1-\epsilon, \tag{38}$$

and we would like to put a bound on the entangled state fidelity

$$F_e=\min_{|\Psi_e\rangle\in\mathcal{H}\otimes\mathcal{C}}\langle\Psi_e|\rho_e|\Psi_e\rangle. \tag{39}$$

Here ρ and ρ_e are the final density matrix after interaction and recovery if the initial state is $|\Psi\rangle$ and $|\Psi_e\rangle$, respectively. Write the entangled state in the Schmidt basis as $|\Psi_e\rangle=\Sigma_i\sqrt{p_i}|\psi_i^{\mathcal{C}}\rangle|\psi_i^{\mathcal{H}}\rangle$ (the label $\mathcal{C}$ characterizes the system on which we want to do error correction and the label $\mathcal{H}$ the system with which it is entangled). We assume that only the system $\mathcal{C}$ is affected by an interaction with the environment and subsequent recovery and that the system $\mathcal{H}$ has trivial dynamics. In this case the interaction operators are tensor products of the identity operator for the system $\mathcal{H}$ and the ones given by the interactions for the system $\mathcal{C}$. We can therefore rewrite Eq. (39) as

$$F_e=\sum_{ij,a}\ p_ip_j\langle\psi_i^{\mathcal{C}}|A_a|\psi_i^{\mathcal{C}}\rangle\langle\psi_j^{\mathcal{C}}|A_a^\dagger|\psi_j^{\mathcal{C}}\rangle. \tag{40}$$

To obtain the bound we calculate the pure state fidelity for a superposition of the form $\sqrt{p_1}\psi_1^{\mathcal{C}}+e^{i\theta}\sqrt{p_2}\psi_2^{\mathcal{C}}$. Thus

$$F_p\leqslant(\sqrt{p_1}\psi_1^{\mathcal{C}}+e^{i\theta}\sqrt{p_2}\psi_2^{\mathcal{C}})$$

$$=\sum_a\ \langle\sqrt{p_1}\psi_1^{\mathcal{C}}+e^{i\theta}\sqrt{p_2}\psi_2^{\mathcal{C}}|A_a|\sqrt{p_1}\psi_1^{\mathcal{C}}+e^{i\theta}\sqrt{p_2}\psi_2^{\mathcal{C}}\rangle$$

$$\times\langle\sqrt{p_1}\psi_1^{\mathcal{C}}+e^{i\theta}\sqrt{p_2}\psi_2^{\mathcal{C}}|A_a^\dagger|\sqrt{p_1}\psi_1^{\mathcal{C}}+e^{i\theta}\sqrt{p_2}\psi_2^{\mathcal{C}}\rangle. \tag{41}$$

We can now average uniformly the last equation over all values of θ to get

$$F_p\leqslant F_e+p_1p_2(\langle\psi_1^{\mathcal{C}}|A_a|\psi_2^{\mathcal{C}}\rangle\langle\psi_2^{\mathcal{C}}|A_a^\dagger|\psi_1^{\mathcal{C}}\rangle \tag{42}$$

$$+\langle\psi_2^{\mathcal{C}}|A_a|\psi_1^{\mathcal{C}}\rangle\langle\psi_1^{\mathcal{C}}|A_a^\dagger|\psi_2^{\mathcal{C}}\rangle). \tag{43}$$

Finally, Eq. (5) puts a bound on the last term in Eq. (43) using the normalization of the interaction operator, i.e.,

$$\sum_{i,a}\ \langle\psi_i^{\mathcal{C}}|A_a|\psi_1^{\mathcal{C}}\rangle\langle\psi_1^{\mathcal{C}}|A_a^\dagger|\psi_i^{\mathcal{C}}\rangle\leqslant 1. \tag{44}$$

(Note that the expression is a partial trace of a density matrix. The trace is partial because the interactions may take the original state into a larger space containing $\mathcal{C}$.) By expanding the sum over i and noting that (1) the term with $i=1$ is at least $1-\epsilon$ by the definition of pure state fidelity and (2) all the terms are positive, we conclude that the terms with $i\neq 1$ are bounded by ϵ. The largest achievable value for p_1p_2 is 1/4. This gives

$$F_e\geqslant 1-\frac{3\epsilon}{2}. \tag{45}$$

For the example of decoherence in Sec. II, it is possible to show that $F_e=F_p$. The following example shows however that the bound in Eq. (45) can be achieved. Consider the interaction consisting of scalar multiples of the Pauli spin matrices,

$$\mathcal{A}=\left\{\frac{1}{\sqrt{3}}\,\sigma_x\,,\ \frac{1}{\sqrt{3}}\,\sigma_y\,,\ \frac{1}{\sqrt{3}}\,\sigma_z\right\}.$$

We show that for this example, $F(\mathcal{A})=1/3$ and $F_e(\mathcal{A})=0$. Let $|u\rangle=\alpha|0\rangle+e^{i\theta}\beta|1\rangle$ with α and β real, and $\alpha^2+\beta^2=1$. The fidelity of $\mathcal{A}$ is obtained by maximizing the expression

$$\begin{aligned}&\tfrac{1}{3}(|\langle u|\sigma_x|u\rangle|^2+|\langle u|\sigma_y|u\rangle|^2+|\langle u|\sigma_z|u\rangle|^2)\\&\quad=\tfrac{1}{3}\ \{[2\alpha\beta\cos(\theta)]^2+[2\alpha\beta\sin(\theta)]^2+(\alpha^2-\beta^2)^2\}\\&\quad=\tfrac{1}{3}\ [(\alpha^2+\beta^2)^2]=\frac{1}{3}.\end{aligned}$$

Hence $F(\mathcal{A})=1/3$. To show that $F_e(\mathcal{A})=0$, apply $\mathcal{A}$ to the second system of the completely entangled state $|e\rangle=1/\sqrt{2}(|0\rangle|0\rangle+|1\rangle|1\rangle)$. We get

$$I\otimes\sigma_x|e\rangle=\frac{1}{\sqrt{2}}\,(|0\rangle|1\rangle+|1\rangle|0\rangle),$$

$$I\otimes\sigma_y|e\rangle=\frac{i}{\sqrt{2}}\,(|0\rangle|1\rangle-|1\rangle|0\rangle),$$

$$I\otimes\sigma_z|e\rangle=\frac{i}{\sqrt{2}}\,(|0\rangle|0\rangle-|1\rangle|1\rangle).$$

These states are all orthogonal to $|e\rangle$, whence $F_e(\mathcal{A})=0$. Thus this example achieves equality in Eq. (45) and our bound is the best possible.

D. Bounds on the fidelity of error-correcting codes for independent interactions

Let $\mathcal{A}$ be one-qubit interaction of the form $\mathcal{A}=\{A_0,A_1,\ldots\}$ with A_0 close to the identity in some sense. In this case we would hope that an e-error-correcting code on n qubits reduces the error after independent interactions of each qubit with $\mathcal{A}$. That this does indeed hold is an important observation for the application of these error-correcting codes. We are about to show that in the case where $A_0=\sqrt{1-p}I$, the classical bounds on the probability of error in the corrected code do apply, as has been discussed by Calderbank and Shor [13], Steane [12], and others. When A_0 is not a scalar multiple of the identity, then additional terms must be added to the bounds. We defer the discussion of this case to future papers.

Assume then that $\mathcal{A}=\{\sqrt{1-p}I,A_1,\ldots\}$. Denote $\mathcal{A}'=\{A_1,\ldots\}$. and note that the strength of $\mathcal{A}'$ is

$$|\mathcal{A}'|^2=\sup_{|x\rangle}\sum_{i\geq 1}\langle x|A_i^\dagger A_i|x\rangle=p.$$

Let $\mathcal{C}\subseteq\mathcal{Q}^{\otimes r}$ be an r-qubit e-error-correcting code with recovery operator $\mathcal{R}$. To estimate the error after recovering from $\mathcal{A}^{\otimes r}$, write

$$\begin{aligned}\mathcal{A}^{\otimes r}&=\{\sqrt{1-p}I,\mathcal{A}'\}^{\otimes r}\\&=\sum_{0\leq k\leq r}\ \sum_{U\subseteq\{1,\ldots,r\},|U|=k}\sqrt{1-p}^{k}(\otimes_{i\notin U}I)\otimes(\otimes_{i\in U}\mathcal{A}'),\end{aligned}$$

with the obvious interpretation of the tensor products and which system each factor is acting on. Let $\mathcal{A}_U=(\otimes_{i\notin U}I)\otimes(\otimes_{i\in U}\mathcal{A}')$ refer to the ensemble of operators obtained by letting I act on the qubits in U and $\mathcal{A}'$ on the qubits not in U. By the properties of the recovery operator, for $|U|\leq e$, the error due to $\mathcal{R}\mathcal{A}_U$ is 0. Thus it suffices to bound the error of the remaining terms in the sum for the interaction. We do this by assuming that the error in each summand is maximal. That is, the contribution to the total error by $\mathcal{A}_U$ is bounded by the strength of $\mathcal{A}_U$ given by the maximum value of $|\mathcal{A}_U|x\rangle|^2$. The strength of the tensor product of operator ensembles can be computed using the next lemma.

Lemma V.4. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be operator ensembles. Then $|\mathcal{B}_1\otimes\mathcal{B}_2|^2=|\mathcal{B}_1|^2|\mathcal{B}_2|^2$.

The lemma can be proved by diagonalizing $\mathcal{B}_1^\dagger\mathcal{B}_1=\Sigma_i B_{1i}^\dagger B_{1i}$ and $\mathcal{B}_2^\dagger\mathcal{B}_2=\Sigma_i B_{2i}^\dagger B_{2i}$.

We deduce that the strength of $\mathcal{A}_U$ is $p^{|U|}$. By evaluating the sums over the U's we obtain the following result.

Theorem V.5. Let $\mathcal{R}$ be the recovery operator of an e-error correcting code $\mathcal{C}$ on n qubits and $\mathcal{A}=\{\sqrt{1-p}I,\mathcal{A}'\}$ a superoperator on one qubit. Then

$$F(\mathcal{C},\mathcal{R}\mathcal{A}^{\otimes r})\geq 1-\sum_{k>e}\binom{r}{k}p^k(1-p)^{r-k}.$$

Note that for applications involving entanglements, the bound needs to be modified in consideration of the relationship between pure state and entangled state fidelity.

VI. CONCLUSION AND FUTURE WORK

We have laid the foundations for a theory of quantum error-correcting codes by providing a general definition of quantum codes and by characterizing those which can correct known interactions with zero error. The main features of our approach include treating a code solely in terms of its subspace in a larger Hilbert space and defining decoding operations in terms of general recovery superoperators. This allows studying codes and their properties for arbitrary interaction superoperator and avoids explicitly dealing with decoding and encoding issues when studying the fidelity of a code given its recovery operator. The treatment in terms of interaction operators directly leads to the characterizations of error-correcting codes given in Sec. III. The characterization in terms of how the operators map individual states (Theorem III.2) has proved useful for finding new codes [15] but also gives the quantum analog to the classical notion of distance between code words.

Our approach is not confined to the study of codes which allow perfect reconstruction of the encoded states. As an example of what can be done, we defined e-error-correcting codes on strings of qubits and considered the effect of independent interactions. We showed that for interactions with an identity component, there is a natural way in which the classical bound on the error can be applied, as has been discussed informally by other authors. This justifies the effort that has been put into finding good e-error-correcting codes. We observe that this classical bound may be more pessimistic than necessary, but leave a careful study of the fidelity of various known codes to future work.

We brought up the important issue of how reliable a predictor the pure state fidelity is for error propagation in entangled systems and showed that the entangled state fidelity is not much less than the pure state fidelity. The fact that it can be less is an important observation, lest one be deceived into believing that a fidelity of 1/3 might be adequate if not compounded by other errors on the same system.

The study of imperfect fidelity codes is far from complete. Both the sources of introduced error, and its propagation when recovery is attempted many times, require further study. Ultimately, these issues determine the circumstances when an advantage may be gained from using error-correction schemes.

We would like to finish by commenting on a general issue. The present work on quantum error correction assumes that no errors are produced during operations. This is a reasonable assumption if the coding, recovery, and decoding operations take a small time compared to the rate at which errors appear (i.e., the interaction strengths), and the error in the operations themselves is small compared to the error corrected by the code. We do not believe that this assumption will remain valid in the context of large scale quantum calculations. It is therefore important to take into account the fact that operations are imperfect. A step in this direction has already been taken in [26]. There the particular case of correcting for decoherence (phase randomization) using the three-bit scheme presented in the Introduction has been investigated.

ACKNOWLEDGMENTS

We would like to thank I. Chuang, C. Miquel, J. Paz, B. Schumacher, J. Smolin, and W. Zurek for useful conversations. R.L. is grateful to J. Gregson for insights on the intuitive approach to error correction. We have both benefited from interaction with the Quantum Computer group at Los Alamos National Laboratory. This work was partially performed under the auspices of the U.S. Department of Energy under Contract No. W-7405-ENG-36.

[1] P. Shor, in *Proceedings, 35th Annual Symposium on Foundations of Computer Science* (IEEE Press, New York, 1994).

[2] C. Monroe *et al.*, Phys. Rev. Lett. **75**, 4714 (1995).

[3] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche, Phys. Rev. Lett. **52**, 3554 (1995).

[4] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).

[5] Richard J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, Contemp. Phys. **36**, 149 (1995).

[6] W. H. Zurek, Phys. Today **40** (10), 36 (1991).

[7] R. Landauer (unpublished).

[8] W. G. Unruh (unpublished); Phys. Rev. A **51**, 992 (1995).

[9] I. L. Chuang, R. Laflamme, P. Shor, and W. H. Zurek, Science **270**, 1633 (1995).

[10] Comments by C. H. Bennet (unpublished).

[11] Peter Shor, Phys. Rev. A **52**, 2493 (1995).

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

[13] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[14] I. L. Chuang and R. Laflamme, Los Alamos National Laboratory Report No. LA-UR-95-3641 (unpublished).

[15] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek, Phys. Rev. Lett. **76**, 198 (1996).

[16] S. L. Braunstein, Report No. quant-phys/9603024.

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

[18] L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. A **54**, R1745 (1996).

[19] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Publishing Company, New York, 1977).

[20] W. K. Wootters and W. H. Zurek, Nature (London) **229**, 802 (1982).

[21] K. Kraus, *States, Effect, and Operations* (Springer-Verlag, New York, 1983).

[22] Benjamin Schumacher, Phys. Rev. A **51**, 2738 (1995).

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

[24] R. A. Horn and I. Olkin, Am. Math. M. **103**, 470 (1996).

[25] M. A. Nielsen and B. Schumacher, Phys. Rev. A **54**, 2629 (1996).

[26] I. Chuang and Y. Yamamoto, Phys. Rev. A **55**, 114 (1997).