Exact performance of concatenated quantum codes

Benjamin Rahn,* Andrew C. Doherty, and Hideo Mabuchi
Institute for Quantum Information, California Institute of Technology, Pasadena, California 91125
(Received 31 October 2001; published 13 September 2002)

When a logical qubit is protected using a quantum error-correcting code, the net effect of coding, decoherence (a physical channel acting on qubits in the codeword) and recovery can be represented exactly by an effective channel acting directly on the logical qubit. In this paper we describe a procedure for deriving the map between physical and effective channels that results from a given coding and recovery procedure. We show that the map for a concatenation of codes is given by the composition of the maps for the constituent codes. This perspective leads us to an efficient means for calculating the exact performance of quantum codes with arbitrary levels of concatenation. We present explicit results for single-bit Pauli channels. For certain codes under the symmetric depolarizing channel, we use the coding maps to compute exact threshold error probabilities for achievability of perfect fidelity in the infinite concatenation limit.

DOI: 10.1103/PhysRevA.66.032304 PACS number(s): 03.67.Hk, 03.65.Yz

I. INTRODUCTION

The methods of quantum error correction [1–3] have, in principle, provided a means for suppressing destructive decoherence in quantum computer memories and quantum communication channels. In practice, however, a finite-sized error-correcting code can only protect against a subset of possible errors; one expects that protected information will still degrade, albeit to a lesser degree. The problem of characterizing a quantum code's performance could thus be phrased as follows: what are the effective noise dynamics of the encoded information that result from the physical noise dynamics in the computing or communication device?

One could address this question by direct simulation of the quantum dynamics and coding procedure. However, for codes of nontrivial size, this approach rapidly becomes intractable. For example, in studies of fault tolerance [4] one often considers families of concatenated codes [3,5]. An N-qubit code concatenated with itself ℓ times yields an N^ℓ-qubit code, providing better error resistance with increasing ℓ. For even modest values of N and ℓ, simulation of the resulting $2^{(N^\ell)}$-dimensional Hilbert space requires massive computational resources; using simulation to find the asymptotic performance as $\ell \to \infty$ (as required for fault-tolerant applications) is simply not on option.

Instead, a quantum code is often characterized by the set of discrete errors that it can perfectly correct [6]. For example, the Shor nine-bit code [1] was designed to perfectly correct arbitrary decoherence acting on a single bit in the nine-bit register. Typical analyses of such codes implicitly assume that the physical dynamics can be described by single-bit errors occurring at some probabilistic rate; if this rate is small [e.g., $O(p)$ for $p \ll 1$], the probability that these errors will accumulate into a multibit uncorrectable error is also small [e.g., $O(p^2)$]. This type of leading-order analysis is limited to a weak-noise regime, and to error models strongly resembling the errors against which the code protects. Outside this regime, these approximation methods fail to accurately describe the evolution of the encoded information.

In this work we take a different approach to characterizing error-correcting codes, which leads to a simple, exact analysis for arbitrary error models. As suggested above, a code transforms the physical dynamics of the device into the effective dynamics of the encoded information. In Sec. II we derive this transformation for arbitrary noise, and present a compact method for its calculation.

In the case of identical, uncorrelated noise on individual qubits, this notion becomes particularly natural: encoding a logical qubit in several physical qubits yields an evolution less noisy than if the logical qubit had been stored, unencoded, in a single physical qubit. Thus a code acts as a map on the space of qubit dynamics, mapping the dynamics of a single *physical* qubit to the dynamics of the encoded *logical* qubit. In Sec. III we show how to calculate this map, and in Sec. IV we use these maps to dramatically simplify the calculation of effective dynamics for concatenated codes when the physical dynamics do not couple code blocks.

In Sec. V, we restrict our attention to uncorrelated single-bit Pauli errors, and in Sec. VI we calculate the exact performance of several codes of interest under these error models. Finally, in Sec. VII we use the coding maps to calculate the performance of certain concatenated codes, and find the exact threshold error probability for perfect fidelity in the infinite concatenation limit. These thresholds serve as important figures of merit for concatenation schemes, and for the codes considered here we find that the traditional approximate methods underestimate these thresholds by up to 44%. Section VIII concludes, suggesting potential future applications for these techniques.

II. DESCRIBING CODE PERFORMANCE WITH EFFECTIVE CHANNELS

In this section we first describe error-correcting codes using a language that will facilitate the subsequent development. We will then present our method for exactly describing the effective dynamics of the encoded information. Though for clarity we restrict our discussion to codes storing a single qubit (sometimes called $k=1$ codes) all the presented meth-

*Electronic address: brahn@caltech.edu

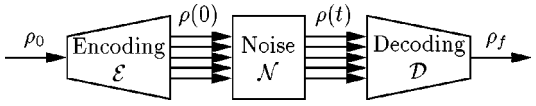

FIG. 1. The error-correction process: a logical single-qubit state ρ_0 is encoded in an N-qubit register as $\rho(0)$. A noise process transforms the register to state $\rho(t)$, which is then decoded to yield the logical single-qubit state ρ_f.

ods generalize naturally to codes storing quantum information of arbitrary dimension.

As an important preliminary, it can be argued [3,7] that all physically possible transformations taking quantum states ρ on a Hilbert space $\mathcal{H}$ to states ρ' on a Hilbert space $\mathcal{H}'$ may be written in the following form:

$$\rho \to \rho' = \sum_j A_j \rho A_j^\dagger \quad \text{with} \quad \sum_j A_j^\dagger A_j = \mathbf{1}, \tag{1}$$

where the A_j are linear operators from $\mathcal{H}$ to $\mathcal{H}'$ and $\mathbf{1}$ denotes the identity operator on $\mathcal{H}$. Such transformations are called *quantum operations* or *channels*, and are necessarily linear, trace preserving, and completely positive. It is easy to see that the composition of quantum operations is also a quantum operation. (One also sees definitions requiring only $\Sigma_j A_j^\dagger A_j \leqslant \mathbf{1}$, corresponding to the weaker requirement that a quantum operation be trace nonincreasing rather than trace preserving. However, the requirement of trace preservation is better suited to our purposes here. See Ref. [3] for a discussion of the distinction.)

A. The error-correction process

The error-correction process, consisting of encoding, noise, and decoding, is depicted in Fig. 1; we consider each stage in turn. An N-qubit code C uses a register of N qubits to encode a single logical qubit $\alpha|0\rangle+\beta|1\rangle$ by preparing the register in the state $\alpha|\overline{0}\rangle+\beta|\overline{1}\rangle$, where $|\overline{0}\rangle$ and $|\overline{1}\rangle$ are orthogonal states in the 2^N-dimensional Hilbert space of the register. The codespace (i.e., the space of initial register states) is spanned by these two states. In what follows it will be convenient to describe states by density matrices: let the logical qubit be given by ρ_0 and the initial register state by $\rho(0)$. Writing $B=|\overline{0}\rangle\langle 0|+|\overline{1}\rangle\langle 1|$, the *encoding operation* $\mathcal{E}:\rho_0 \to \rho(0)$ is given by

$$\rho(0) = \mathcal{E}[\rho_0] = B\rho_0 B^\dagger. \tag{2}$$

As $B^\dagger B = |0\rangle\langle 0|+|1\rangle\langle 1| = \mathbf{1}$, $\mathcal{E}$ is a quantum operation.

After the encoding, the register state evolves due to some noise dynamics. In the setting of a quantum computer memory, the dynamics are continuous in time; assuming evolution for a time t, we have $\rho(t)=\mathcal{N}_t[\rho(0)]$ with $\mathcal{N}_t$ a quantum operation depending continuously on t. (For master equation evolution $\dot{\rho}=\mathcal{L}[\rho]$, we have $\mathcal{N}_t = e^{\mathcal{L}t}$.) We will often omit the subscript t and simply write $\mathcal{N}$. In the setting of a quantum communication channel, the noise process is usually given by the discrete application of a quantum operation $\mathcal{N}$; thus if the transmitted state is $\rho(0)$, the received state is $\mathcal{N}[\rho(0)]$, which we write as $\rho(t)$ for consistency.

After the noise process, an attempt is made to recover the initial register state $\rho(0)$ from the current register state $\rho(t)$ by applying a quantum operation $\mathcal{R}$, which may be written as

$$\mathcal{R}[\rho(t)] = \sum_j A_j \rho(t) A_j^\dagger \quad \text{with} \quad \sum_j A_j^\dagger A_j = \mathbf{1}. \tag{3}$$

As the initial state $\rho(0)$ is known to be in the codespace, it is clearly more beneficial to return the state $\rho(t)$ to the codespace than to do otherwise: lacking any other information, one could at least prepare the completely mixed state in the codespace $\frac{1}{2}(|\overline{0}\rangle\langle\overline{0}|+|\overline{1}\rangle\langle\overline{1}|)$, yielding an average fidelity of $\frac{1}{2}$, rather than leaving the register outside the codespace, yielding a fidelity of 0. We will therefore restrict our attention to error-correction processes $\mathcal{R}$ that take all register states back to the codespace. (That is, we assume no leakage errors during recovery.)

With the above assumption, the postrecovery state $\mathcal{R}[\rho(t)]$ has support entirely on the codespace; thus it can be described by its restriction to the codespace, the logical single-qubit state ρ_f such that $\mathcal{E}[\rho_f]=\mathcal{R}[\rho(t)]$. Call $\mathcal{D}=\mathcal{E}^\dagger \circ \mathcal{R}$ the *decoding operation* (shown to be a quantum operation in Lemma 1 of Appendix B):

$$\mathcal{D}[\rho(t)] = B^\dagger \mathcal{R}[\rho(t)] B = \sum_j B^\dagger A_j \rho(t) A_j^\dagger B. \tag{4}$$

With this definition, $\rho_f = \mathcal{D}[\rho(t)]$. We will consider the logical state ρ_f as the outcome of the error-correction process, and therefore may say that the code is given by its encoding and decoding operations, i.e., $C=(\mathcal{E},\mathcal{D})$.

To build intuition for the decoding operation $\mathcal{D}$, we note that for most codes considered in the literature (and all of the specific codes considered later in this paper) the recovery procedure is given in a particular form. First, a syndrome measurement is made, projecting the register state onto one of 2^{N-1} orthogonal two-dimensional subspaces; let the measurement be specified by projectors $\{P_j\}$. After the measurement (whose outcome is given by j, the index of the corresponding projector), the recovery operator R_j acts on the register, unitarily mapping the subspace projected by P_j back to the codespace. For such codes, the recovery superoperator is given by Eq. (3) with $A_j = R_j P_j$, and $\mathcal{R}[\rho(t)]$ is the expected state that results from averaging over syndrome measurement outcomes.

For codes of this form, let $\{|0_j\rangle,|1_j\rangle\}$ denote the orthonormal basis for the syndrome space projected by P_j such that $R_j|0_j\rangle=|\overline{0}\rangle$ and $R_j|1_j\rangle=|\overline{1}\rangle$. Then $R_j P_j = |\overline{0}\rangle\langle 0_j| + |\overline{1}\rangle\langle 1_j|$, and using the expression for $\mathcal{D}$ given in Eq. (4) yields

$$\mathcal{D}[\rho(t)] = \sum_j B^\dagger R_j P_j \rho(t) P_j^\dagger R_j^\dagger B$$

$$= \sum_j (|0\rangle\langle 0_j| + |1\rangle\langle 1_j|)\rho(t)(|0_j\rangle\langle 0| + |1_j\rangle\langle 1|). \tag{5}$$

Thus $\rho_f = \mathcal{D}[\rho(t)]$ is the sum of the single-qubit density matrices that result from restricting $\rho(t)$ to each of the syndrome spaces, with basis $\{|0_j\rangle, |1_j\rangle\}$ determined by the recovery operator.

As an example, consider the bit-flip code [3], a three-qubit code that protects against single bit-flip errors. The bit-flip code's encoding transformation is given by

$$|0\rangle \mapsto |\overline{0}\rangle = |000\rangle, \quad |1\rangle \mapsto |\overline{1}\rangle = |111\rangle. \tag{6}$$

After the action of some error dynamics, the syndrome measurement then projects the register state into one of four subspaces: the codespace itself, and the three subspaces that result from flipping the first, second, or third bit of states in the codespace. The corresponding recovery operator simply flips the appropriate bit back, attempting to reverse the error. Thus the basis specifying the decoding operation is given by

$$|0_0\rangle = |000\rangle, \quad |1_0\rangle = |111\rangle,$$

$$|0_1\rangle = |100\rangle, \quad |1_1\rangle = |011\rangle,$$

$$|0_2\rangle = |010\rangle, \quad |1_2\rangle = |101\rangle,$$

$$|0_3\rangle = |001\rangle, \quad |1_3\rangle = |110\rangle. \tag{7}$$

We will use the bit-flip code as an example throughout this work.

B. Calculating the effective dynamics

The transformation $\rho_0 \to \rho_f$ gives the effective dynamics of the encoded information resulting from the physical dynamics $\mathcal{N}$. Let $\mathcal{G}$ be the map giving these effective dynamics: $\rho_f = \mathcal{G}[\rho_0]$. From the above discussion, the effective dynamics are simply the result of encoding, followed by noise, followed by decoding, i.e.,

$$\mathcal{G} = \mathcal{D} \circ \mathcal{N} \circ \mathcal{E}. \tag{8}$$

As $\mathcal{G}$ is the composition of quantum operations $\mathcal{E}$, $\mathcal{N}$, and $\mathcal{D}$, it is itself a quantum operation. We may therefore call $\mathcal{G}$ the *effective channel* describing the code $C = (\mathcal{E}, \mathcal{D})$ and physical noise dynamics $\mathcal{N}$.

Because the effective channel $\mathcal{G}$ is only a map on single qubit states, it should have a compact description—in particular, a description much more compact than some arbitrary noise $\mathcal{N}$ acting on N-qubit states. By calculating such a compact description, we may easily find the effective evolution of an arbitrary initial state ρ_0 without explicitly considering the physical noise dynamics. As we now show, $\mathcal{G}$ may be written as a 4×4 matrix with a simple interpretation. (See Ref. [8] for a full discussion of qubit channels represented in this fashion.)

For each Pauli matrix $\sigma \in \{I, X, Y, Z\}$, let $\langle \sigma \rangle_0 = \mathrm{tr}(\sigma \rho_0)$. The Pauli matrices form a basis for qubit density matrices, and so the initial logical qubit ρ_0 may be linearly parametrized by its expectation values $\langle \sigma \rangle_0$ as follows:

$$\rho_0 = \frac{1}{2}\langle I \rangle_0 I + \frac{1}{2}\langle X \rangle_0 X + \frac{1}{2}\langle Y \rangle_0 Y + \frac{1}{2}\langle Z \rangle_0 Z. \tag{9}$$

(As the trace of a density matrix must be 1 we will always have $\langle I \rangle = 1$, but it will be convenient to include this term.) Similarly, the final logical qubit ρ_f may be linearly parametrized by its expectation values $\langle \sigma \rangle_f = \mathrm{tr}(\sigma \rho_f)$. Thus the effective channel $\mathcal{G}$ may be written as the mapping from the expectation values $\langle \sigma \rangle_0$ of ρ_0 to the expectation values $\langle \sigma \rangle_f$ of ρ_f. Writing $\vec{\rho}_0 = (\langle I \rangle_0, \langle X \rangle_0, \langle Y \rangle_0, \langle Z \rangle_0)^{\mathrm{T}}$ and $\vec{\rho}_f = (\langle I \rangle_f, \langle X \rangle_f, \langle Y \rangle_f, \langle Z \rangle_f)^{\mathrm{T}}$, the linearity of $\mathcal{G}$ allows it to be written as the 4×4 matrix such that $\vec{\rho}_f = \mathcal{G}\vec{\rho}_0$. The fidelity of a pure logical qubit ρ_0 through the effective channel is then given by $\mathrm{tr}(\rho_0 \rho_f) = \frac{1}{2}\vec{\rho}_0^{\mathrm{T}}\vec{\rho}_f = \frac{1}{2}\vec{\rho}_0^{\mathrm{T}}\mathcal{G}\vec{\rho}_0$. Thus to fully characterize the effective channel $\mathcal{G}$ we need only find the entries of its 4×4 matrix representation. (More generally, if the code stored a d-dimensional state rather than the two-dimensional state of a qubit, the logical density matrices ρ_0 and ρ_f would be expanded in the basis of the identity matrix and the $d^2 - 1$ generators of SU(d), and $\mathcal{G}$ would be represented as a $d^2 \times d^2$ matrix.)

To find these matrix elements, we consider the encoding and decoding processes in more detail. Letting E_σ denote $\frac{1}{2}\mathcal{E}[\sigma]$, the encoding transformation $\mathcal{E}$ acts on ρ_0 [given by Eq. (9)] to prepare the initial register state

$$\rho(0) = \langle I \rangle_0 E_I + \langle X \rangle_0 E_X + \langle Y \rangle_0 E_Y + \langle Z \rangle_0 E_Z. \tag{10}$$

Thus the encoding operation $\mathcal{E}$ is completely characterized by the E_σ operators, which are easily constructed from the codewords:

$$E_I = \frac{1}{2}(|\overline{0}\rangle\langle\overline{0}| + |\overline{1}\rangle\langle\overline{1}|),$$

$$E_X = \frac{1}{2}(|\overline{0}\rangle\langle\overline{1}| + |\overline{1}\rangle\langle\overline{0}|),$$

$$E_Y = \frac{1}{2}(-i|\overline{0}\rangle\langle\overline{1}| + i|\overline{1}\rangle\langle\overline{0}|),$$

$$E_Z = \frac{1}{2}(|\overline{0}\rangle\langle\overline{0}| - |\overline{1}\rangle\langle\overline{1}|). \tag{11}$$

As expected, $\rho(0)$ is the state ρ_0 on the codespace, and vanishes elsewhere.

Now consider the decoding process, which yields the logical state ρ_f. We may express the expectation values $\langle \sigma \rangle_f$ in terms of $\rho(t)$, the register state prior to recovery, as follows:

$$\langle\sigma\rangle_f = \mathrm{tr}(\sigma\rho_f) = \mathrm{tr}\{\sigma\mathcal{D}[\rho(t)]\} = \mathrm{tr}\left(\sum_j \sigma B^\dagger A_j \rho(t) A_j^\dagger B\right). \tag{12}$$

Exploiting the cyclic property of the trace and noting that $B\sigma B^\dagger = \mathcal{E}[\sigma] = 2E_\sigma$, we have

$$\langle\sigma\rangle_f = \mathrm{tr}(D_\sigma \rho(t)) \quad \text{where} \quad D_\sigma = 2\sum_j A_j^\dagger E_\sigma A_j. \tag{13}$$

Thus the decoding operation $\mathcal{D}$ is completely characterized by the D_σ operators.

Substituting $\rho(t) = \mathcal{N}[\rho(0)]$ into Eq. (13), we have $\langle\sigma\rangle_f = \mathrm{tr}\{D_\sigma \mathcal{N}[\rho(0)]\}$. Substituting in the expression for $\rho(0)$ given by Eq. (10) then yields

$$\langle\sigma\rangle_f = \mathrm{tr}\left(D_\sigma \mathcal{N}\left[\sum_{\sigma'} \langle\sigma'\rangle_0 E_{\sigma'}\right]\right). \tag{14}$$

Letting the matrix elements of $\mathcal{G}$ be given by

$$\mathcal{G}_{\sigma\sigma'} = \mathrm{tr}(D_\sigma \mathcal{N}[E_{\sigma'}]) \tag{15}$$

for $\sigma, \sigma' \in \{I, X, Y, Z\}$, we have $\langle\sigma\rangle_f = \Sigma_{\sigma'} G_{\sigma\sigma'} \langle\sigma'\rangle_0$, i.e., $\vec{\rho}_f = \mathcal{G}\vec{\rho}_0$.

To completely characterize the effective channel $\mathcal{G}$, then, we need to only compute these matrix elements. In fact, trace preservation (i.e., $\langle I\rangle_f = \langle I\rangle_0$) requires $\mathcal{G}_{II} = 1$ and $\mathcal{G}_{IX} = \mathcal{G}_{IY} = \mathcal{G}_{IZ} = 0$. Thus the effect on the logical information of the potentially complex dynamics of the N-qubit register space are characterized by the remaining twelve matrix elements of $\mathcal{G}$. If $\mathcal{N}$ is time dependent, then the only observable effects of this time-dependence will appear in the time dependence of the $\mathcal{G}_{\sigma\sigma'}$, and $\mathcal{G}_t$ gives the effective channel for correction performed at time t. Note that the dynamics $\mathcal{N}$ need not be related to those against which the code was designed to protect.

We have thus shown that the effective dynamics may be calculated by evaluating Eq. (15), which requires constructing the E_σ and D_σ operators. The E_σ operators are easily understood to be the operators that act as $\frac{1}{2}\sigma$ on the codespace and vanish elsewhere; to build intuition for the D_σ operators, consider codes whose recovery is specified by syndrome measurement projectors $\{P_j\}$ and recovery operators $\{R_j\}$ as discussed in Sec. II A. For these codes, we have $A_j = R_j P_j$, and so $D_\sigma = 2\Sigma_j P_j^\dagger R_j^\dagger E_\sigma R_j P_j$. This expression may be simplified by noting that E_σ maps the codespace to itself and vanishes elsewhere, and R_j unitarily maps the space projected by P_j to the codespace. Thus $R_j^\dagger E_\sigma R_j$ unitarily maps the space projected by P_j to itself and vanishes elsewhere, i.e., $P_j R_j^\dagger E_\sigma R_j P_j = R_j^\dagger E_\sigma R_j$. We therefore have

$$D_\sigma = 2\sum_j R_j^\dagger E_\sigma R_j. \tag{16}$$

Using the expressions for E_σ given in Eq. (11) and $R_j = |\overline{0}\rangle\langle 0_j| + |\overline{1}\rangle\langle 1_j|$, we have

$$D_I = \sum_j (|0_j\rangle\langle 0_j| + |1_j\rangle\langle 1_j|),$$

$$D_X = \sum_j (|0_j\rangle\langle 1_j| + |1_j\rangle\langle 0_j|),$$

$$D_Y = \sum_j (-i|0_j\rangle\langle 1_j| + i|1_j\rangle\langle 0_j|),$$

$$D_Z = \sum_j (|0_j\rangle\langle 0_j| - |1_j\rangle\langle 1_j|). \tag{17}$$

Thus we see that in this case D_σ is simply the sum of the operators σ acting on each of the syndrome spaces, with Z eigenstates $|0_j\rangle$ and $|1_j\rangle$ determined by the recovery procedure. Note that D_I is the identity operator on the entire register space.

III. CODING AS A MAP ON CHANNELS

One often considers noise models $\mathcal{N}$ consisting of uncorrelated noise on each of the N physical qubits. This type of model arises naturally in a communication setting, where the register qubits are sent over a noisy transmission line one at a time, and is also appropriate for various physical implementations of a quantum computer. (By contrast, one can also consider error models in which correlated noise dominates [9].) For such models, we may write

$$\mathcal{N} = \mathcal{N}^{(1)} \otimes \mathcal{N}^{(1)} \otimes \cdots \otimes \mathcal{N}^{(1)} = \mathcal{N}^{(1)\otimes N}, \tag{18}$$

where $\mathcal{N}^{(1)}$ is a quantum operation on a single qubit.

The goal of encoding a qubit is to suppress decoherence: multiple qubits are employed to yield an effective channel $\mathcal{G}$, which should be less noisy than the channel resulting from storing information in a single physical qubit, namely, $\mathcal{N}^{(1)}$. A code can thus be seen as a map on channels, taking $\mathcal{N}^{(1)}$ to $\mathcal{G}$. More precisely, for an N-qubit code $C = (\mathcal{E}, \mathcal{D})$, define the corresponding *coding map* Ω^C by

$$\Omega^C : \mathcal{N}^{(1)} \to \mathcal{G} = \mathcal{D} \circ \mathcal{N}^{(1)\otimes N} \circ \mathcal{E}. \tag{19}$$

We now derive an expression for the coding map Ω^C of an arbitrary code $C = (\mathcal{E}, \mathcal{D})$. In Sec. II B we described how $\mathcal{G}$ may be specified by its matrix elements $\mathcal{G}_{\sigma\sigma'}$, given by Eq. (15). Since $\mathcal{N}^{(1)}$ is a single-qubit quantum operation, it may also be written as a 4×4 matrix such that if $\mathcal{N}^{(1)}$ takes ρ to ρ', then $\vec{\rho}' = \mathcal{N}^{(1)}\vec{\rho}$. We seek an expression for the matrix elements of the effective channel $\mathcal{G}$ in terms of the matrix elements of the physical channel $\mathcal{N}^{(1)}$.

Operators on N qubits may be written as sums of tensor products of N Pauli matrices; we may therefore write the E_σ and D_σ operators describing $C = (\mathcal{E}, \mathcal{D})$ as

$$E_{\sigma'} = \sum_{\substack{\mu_i \in \\ \{I,X,Y,Z\}}} \alpha^{\sigma'}_{\{\mu_i\}} (\tfrac{1}{2}\mu_1) \otimes \cdots \otimes (\tfrac{1}{2}\mu_N), \tag{20}$$

$$D_\sigma = \sum_{\substack{\nu_i \in \\ \{I,X,Y,Z\}}} \beta^\sigma_{\{\nu_i\}} \nu_1 \otimes \cdots \otimes \nu_N . \tag{21}$$

For example, for the bit-flip code described in Sec. II A by Eqs. (6) and (7), we may calculate the $E_{\sigma'}$ and D_σ operators using Eqs. (11) and (17); expanding the results in the basis of Pauli operators yields

$$E_I = \frac{1}{8}(III + IZZ + ZIZ + ZZI),$$

$$E_X = \frac{1}{8}(XXX - XYY - YXY - YYX),$$

$$E_Y = \frac{1}{8}(-YYY + YXX + XYX + XXY),$$

$$E_Z = \frac{1}{8}(ZZZ + ZII + IZI + IIZ), \tag{22}$$

and

$$D_I = III,$$

$$D_X = XXX,$$

$$D_Y = \frac{1}{2}(YYY + YXX + XYX + XXY),$$

$$D_Z = \frac{1}{2}(-ZZZ + ZII + IZI + IIZ). \tag{23}$$

To find the matrix elements of the effective channel, we substitute Eqs. (18), (20), and (21) into the expression for these matrix elements given by Eq. (15). Noting that $\mathcal{N}[\frac{1}{2}\mu_1 \otimes \cdots \otimes \frac{1}{2}\mu_N] = \mathcal{N}^{(1)}[\frac{1}{2}\mu_1] \otimes \ldots \otimes \mathcal{N}^{(1)}[\frac{1}{2}\mu_N]$, and $\mathrm{tr}[(A \otimes B)(C \otimes D)] = \mathrm{tr}(AC)\mathrm{tr}(BD)$ yields

$$\mathcal{G}_{\sigma\sigma'} = \sum_{\{\mu_i\},\{\nu_i\}} \left(\beta^\sigma_{\{\nu_i\}} \alpha^{\sigma'}_{\{\mu_i\}} \prod_{i=1}^{N} \mathrm{tr}(\nu_i \mathcal{N}^{(1)}[\tfrac{1}{2}\mu_i]) \right). \tag{24}$$

From the orthogonality of Pauli matrices, the matrix $\frac{1}{2}\mu_i$, when written as a vector of expectation values, has a 1 in the μ_i component and zeros elsewhere. Further, $\mathrm{tr}(\nu_i \rho)$ is simply the ν_i component of $\vec{\rho}$. Thus $\mathrm{tr}(\nu_i \mathcal{N}^{(1)}[\frac{1}{2}\mu_i]) = \mathcal{N}^{(1)}_{\nu_i \mu_i}$, and we have

$$\mathcal{G}_{\sigma\sigma'} = \sum_{\{\mu_i\},\{\nu_i\}} \left(\beta^\sigma_{\{\nu_i\}} \alpha^{\sigma'}_{\{\mu_i\}} \prod_{i=1}^{N} \mathcal{N}^{(1)}_{\nu_i \mu_i} \right). \tag{25}$$

Thus the matrix elements of $\mathcal{G}$ can be expressed as polynomials of the matrix elements of $\mathcal{N}^{(1)}$, with the polynomial coefficients depending only on the $E_{\sigma'}$ and D_σ of the code. These polynomials specify Ω^C. By computing these polynomials for a code C, one can easily calculate the effective channel for the code C due to any error model with identical, uncorrelated noise acting on each physical qubit. [If a different noise model acts on each physical qubit, i.e., $\mathcal{N} = \mathcal{N}^{(1)} \otimes \cdots \otimes \mathcal{N}^{(N)}$, simply replace $\mathcal{N}^{(1)}_{\nu_i \mu_i}$ with $\mathcal{N}^{(i)}_{\nu_i \mu_i}$ in Eq. (25).]

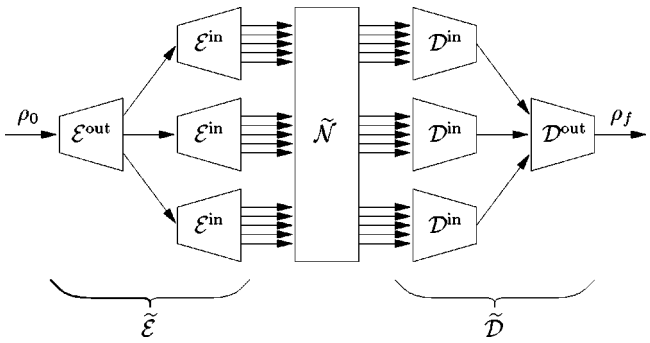

FIG. 2. The error-correction process for the concatenated code $C^{\mathrm{out}}(C^{\mathrm{in}}) = (\tilde{\mathcal{E}}, \tilde{\mathcal{D}})$; here $C^{\mathrm{out}} = (\mathcal{E}^{\mathrm{out}}, \mathcal{D}^{\mathrm{out}})$ is a three-qubit code and $C^{\mathrm{in}} = (\mathcal{E}^{\mathrm{in}}, \mathcal{D}^{\mathrm{in}})$ is a five-qubit code. The noise process $\tilde{\mathcal{N}}$ acts on the entire 15-qubit register.

IV. CONCATENATED CODES

We now consider concatenated codes [3,5]. We first describe the procedure for constructing such codes, and then show how the coding maps Ω^C make the calculation of the effective channels for such codes straightforward.

A. Constructing concatenated codes

We now describe how two codes may be concatenated to form a larger code; the procedure is depicted in Fig. 2. Let the two codes be an M-qubit code $C^{\mathrm{out}} = (\mathcal{E}^{\mathrm{out}}, \mathcal{D}^{\mathrm{out}})$, called the outer code, and an N-qubit code $C^{\mathrm{in}} = (\mathcal{E}^{\mathrm{in}}, \mathcal{D}^{\mathrm{in}})$, called the inner code. A logical qubit ρ_0 is encoded first using the outer code C^{out}, yielding the M-qubit state $\mathcal{E}^{\mathrm{out}}[\rho_0]$. Each of these qubits is then encoded by the inner code; i.e., the map $\mathcal{E}^{\mathrm{in}} \otimes \cdots \otimes \mathcal{E}^{\mathrm{in}} = (\mathcal{E}^{\mathrm{in}})^{\otimes M}$ acts on $\mathcal{E}^{\mathrm{out}}[\rho_0]$. The composition of these encodings forms the encoding map for the concatenated code:

$$\tilde{\mathcal{E}} = (\mathcal{E}^{\mathrm{in}})^{\otimes M} \circ \mathcal{E}^{\mathrm{out}}. \tag{26}$$

The M sections of the register encoding each of the M qubits in $\mathcal{E}^{\mathrm{out}}[\rho_0]$ are called blocks; each block contains N qubits. After the encoding, a noise process $\tilde{\mathcal{N}}$ acts on the entire MN-qubit register.

A simple error-correction scheme (and one that seems reasonable for use in a scalable architecture) coherently corrects each of the code blocks based on the inner code, and then corrects the entire register based on the outer code. That is, the decoding map for the concatenated code is given by

$$\tilde{\mathcal{D}} = \mathcal{D}^{\mathrm{out}} \circ \mathcal{D}^{\mathrm{in} \otimes M}. \tag{27}$$

We denote the concatenated code (with this correction scheme) by $C^{\mathrm{out}}(C^{\mathrm{in}}) = (\tilde{\mathcal{E}}, \tilde{\mathcal{D}})$; note that $C^{\mathrm{out}}(C^{\mathrm{in}})$ is an MN-qubit code.

B. Effective channels for concatenated codes

Suppose that we have computed the effective channel $\mathcal{G}$ due to a code $C^{\text{in}}=(\mathcal{E}^{\text{in}},\mathcal{D}^{\text{in}})$ with some noise dynamics $\mathcal{N}$, and wish to consider the effective channel $\tilde{\mathcal{G}}$ resulting from the concatenated code $C^{\text{out}}(C^{\text{in}})$. We assume that each N-bit block in the register evolves according to the noise dynamics $\mathcal{N}$ and no cross-block correlations are introduced, i.e., that the evolution operator on the MN-bit register is

$$\tilde{\mathcal{N}}=\mathcal{N}\otimes\mathcal{N}\otimes\cdots\otimes\mathcal{N}=\mathcal{N}^{\otimes M}. \tag{28}$$

By definition, we have $\tilde{\mathcal{G}}=\tilde{\mathcal{D}}\circ\tilde{\mathcal{N}}\circ\tilde{\mathcal{E}}$. Substituting Eqs. (26), (27), and (28) into this expression yields

$$\begin{aligned}\tilde{\mathcal{G}}&=\mathcal{D}^{\text{out}}\circ\mathcal{D}^{\text{in}\otimes M}\circ\mathcal{N}^{\otimes M}\circ\mathcal{E}^{\text{in}\otimes M}\circ\mathcal{E}^{\text{out}}\\&=\mathcal{D}^{\text{out}}\circ(\mathcal{D}^{\text{in}}\circ\mathcal{N}\circ\mathcal{E}^{\text{in}})^{\otimes M}\circ\mathcal{E}^{\text{out}}\\&=\mathcal{D}^{\text{out}}\circ\mathcal{G}^{\otimes M}\circ\mathcal{E}^{\text{out}},\end{aligned} \tag{29}$$

where we have used $\mathcal{G}=\mathcal{D}^{\text{in}}\circ\mathcal{N}\circ\mathcal{E}^{\text{in}}$. This result makes sense: each of the M blocks of N bits represents a single logical qubit encoded in C^{in}, and as the block has dynamics $\mathcal{N}$, this logical qubit's evolution will be described by $\mathcal{G}$. Comparing with the definition of the coding map (19), we then have

$$\tilde{\mathcal{G}}=\Omega^{C^{\text{out}}}(\mathcal{G}). \tag{30}$$

Thus given the effective channel for a code C^{in} and an error model, the coding map $\Omega^{C^{\text{out}}}$ makes it straightforward to compute the effective channel due to the concatenated code $C^{\text{out}}(C^{\text{in}})$.

Further, suppose that the original noise model $\mathcal{N}$ had the form of uncorrelated noise on single physical qubits, as given by Eq. (18). Then $\mathcal{G}=\Omega^{C^{\text{in}}}(\mathcal{N}^{(1)})$, and so $\tilde{\mathcal{G}}=\Omega^{C^{\text{out}}}(\Omega^{C^{\text{in}}}(\mathcal{N}^{(1)}))$. We may therefore conclude that composing coding maps gives the coding map for the concatenated code, i.e.,

$$\Omega^{C^{\text{out}}(C^{\text{in}})}=\Omega^{C^{\text{out}}}\circ\Omega^{C^{\text{in}}}. \tag{31}$$

More generally, we may characterize both the finite and asymptotic behavior of any concatenation scheme involving the codes $\{C_k\}$ by computing the maps Ω^{C_k}. Then the finite concatenation scheme $C_1(C_2(\ldots C_n\ldots))$ is characterized by $\Omega^{C_1(C_2(\ldots C_n\ldots))}=\Omega^{C_1}\circ\Omega^{C_2}\circ\cdots\circ\Omega^{C_n}$. We expect the typical Ω^C to be sufficiently well behaved that standard dynamical systems methods [10] will yield the $\ell\to\infty$ limit of $(\Omega^C)^\ell$; one need not compose the $(\Omega^C)^\ell$ explicitly. In Sec. VII, we will consider such asymptotic limits in more detail.

V. DIAGONAL CHANNELS

As an application of the methods presented above, we will consider the commonly-considered error model in which each physical register qubit is subjected to the symmetric depolarizing channel [3]. These single-qubit noise dynamics are given by the master equation

$$\frac{d\rho}{dt}=\frac{\gamma}{4}\mathcal{L}_X[\rho]+\frac{\gamma}{4}\mathcal{L}_Y[\rho]+\frac{\gamma}{4}\mathcal{L}_Z[\rho], \tag{32}$$

where for any linear qubit operator c the Lindblad decoherence operator $\mathcal{L}_c$ is given by

$$\mathcal{L}_c[\rho]=c\rho c^\dagger-\frac{1}{2}c^\dagger c\rho-\frac{1}{2}\rho c^\dagger c \tag{33}$$

and γ is a measure of the noise strength. This master equation is easily solved, yielding a qubit channel with matrix representation

$$\mathcal{N}_t^{\text{dep}}=\begin{pmatrix}1&0&0&0\\0&e^{-\gamma t}&0&0\\0&0&e^{-\gamma t}&0\\0&0&0&e^{-\gamma t}\end{pmatrix}. \tag{34}$$

Before calculating effective channels due to this error model, it will be useful to discuss the more general set of channels whose matrix representation is diagonal. As we will see, these channels correspond to single-bit Pauli channels, and will allow us to demonstrate the power of the techniques developed above.

Consider a qubit channel given by a diagonal matrix $\mathcal{N}^{(1)}$. From trace preservation $\mathcal{N}^{(1)}_{II}=1$, so let the channel with $\mathcal{N}^{(1)}_{XX}=x$, $\mathcal{N}^{(1)}_{YY}=y$, and $\mathcal{N}^{(1)}_{ZZ}=z$ be denoted $[x,y,z]$ for compactness. (Thus the depolarizing channel (34) is given by $[e^{-\gamma t},e^{-\gamma t},e^{-\gamma t}]$.) In Ref. [11] it is shown that complete positivity of such a channel requires

$$\begin{aligned}-x+y+z&\leq 1,\\x-y+z&\leq 1,\\x+y-z&\leq 1,\\-x-y-z&\leq 1.\end{aligned} \tag{35}$$

Now consider the single-bit Pauli channel in which the transmitted state is subjected to the Pauli operators X, Y, and Z with exclusive probabilities p_X, p_Y, and p_Z, i.e.,

$$\rho\to(1-p_X-p_Y-p_Z)\rho+p_XX\rho X+p_YY\rho Y+p_ZZ\rho Z. \tag{36}$$

It is easy to show that this channel has the diagonal matrix representation

$$[1-2(p_Y+p_Z),1-2(p_X+p_Z),1-2(p_X+p_Y)], \tag{37}$$

and so any Pauli channel is a diagonal channel. The converse is also true: choosing $p_x=(1+x-y-z)/4$, $p_y=(1-x+y-z)/4$, and $p_z=(1-x-y+z)/4$ yields the channel $[x,y,z]$, and the complete positivity constraints (35) yield the standard probability rules $p_X,p_Y,p_Z\geq 0$ and $p_X+p_Y+p_Z\leq 1$. Thus any diagonal channel may be realized as a Pauli channel. Pauli channels are among the most commonly considered error models in the literature, and we will restrict our attention to diagonal channels for the remainder of this work.

The effect of a diagonal channel on a qubit is simple to interpret: we have $\langle X\rangle_f = x\langle X\rangle_0$, $\langle Y\rangle_f = y\langle Y\rangle_0$, and $\langle Z\rangle_f = z\langle Z\rangle_0$. Thus the X, Y, and Z components of $\vec{\rho}_0$ decay independently, and we may therefore speak of the decoherence of $\langle X\rangle$, $\langle Y\rangle$, and $\langle Z\rangle$. Recalling from Sec. II B that the fidelity of a pure state ρ through a qubit channel $\mathcal{G}$ is given by $\frac{1}{2}\vec{\rho}^{\mathrm{T}}\mathcal{G}\vec{\rho}$, the respective fidelities of X, Y, and Z eigenstates through the channel are $\frac{1}{2}(1+x)$, $\frac{1}{2}(1+y)$, and $\frac{1}{2}(1+z)$. More generally, the fidelity of a pure state [requiring $\langle X\rangle^2+\langle Y\rangle^2+\langle Z\rangle^2=1$] is given by $\frac{1}{2}(1+x\langle X\rangle^2+y\langle Y\rangle^2+z\langle Z\rangle^2)$. A common figure of merit for a channel is the worst-case fidelity of a pure state, which for a diagonal channel is $\frac{1}{2}[1+\min(x,y,z)]$. Thus if for a given error model a code C yields an effective channel $[x,y,z]$ and a code C' yields an effective channel $[x',y',z']$, we say that C outperforms C' if $\min(x,y,z)>\min(x',y',z')$.

Many commonly considered codes are *stabilizer codes* [3,12], which are designed to detect and correct Pauli errors; it would therefore not be so surprising if the coding maps for such codes were particularly well behaved when acting on a Pauli channel. In fact, as proved in Appendix A, if C is a stabilizer code and $\mathcal{N}^{(1)}$ is diagonal, then $\Omega^C(\mathcal{N}^{(1)})$ is also diagonal. Thus just as arbitrary codes act as maps on the space of qubit channels, stabilizer codes act as maps on the space of diagonal qubit channels.

VI. EXACT PERFORMANCE FOR SEVERAL CODES OF INTEREST

We will now present the effective channels for several codes of interest under diagonal error models. The codes considered here may all be formulated as stabilizer codes; thus, as described in the preceding section, the effective channels will also be diagonal. The diagonal elements of the effective channel $\mathcal{G}=\Omega^C([x,y,z])$ may be calculated either using the coding map methods presented in Sec. III, or using the stabilizer formalism as shown in Appendix A, which may be computationally advantageous. For each code, we will compute the effective channel for a general diagonal error model $[x,y,z]$, and then interpret the results for the symmetric depolarizing channel $\mathcal{N}_t^{\mathrm{dep}}=[e^{-\gamma t},e^{-\gamma t},e^{-\gamma t}]$.

The bit-flip code, first mentioned in Sec. II A, is a stabilizer code; letting Ω^{bf} denote the corresponding coding map, we find

$$\Omega^{\mathrm{bf}}([x,y,z])=[x^3,\tfrac{3}{2}x^2y-\tfrac{1}{2}y^3,\tfrac{3}{2}z-\tfrac{1}{2}z^3]. \qquad (38)$$

As the bit-flip code is only a three-qubit code, it is not unreasonable to check this result with more conventional methods, e.g., by counting bit-flip and phase-flip errors, or by working in the Heisenberg picture to compute the evolution of the relevant expectation values. However, for larger codes such computations will rapidly become unmanageable.

To examine the bit-flip code acting under the symmetric depolarizing channel, define $[x^{\mathrm{bf}}(t),y^{\mathrm{bf}}(t),z^{\mathrm{bf}}(t)]=\Omega^{\mathrm{bf}}(\mathcal{N}_t^{\mathrm{dep}})$; the functions x^{bf}, y^{bf}, and z^{bf} are plotted in Fig. 3 along with $e^{-\gamma t}$ (describing the decoherence of the physical qubits) for comparison. We see that $z^{\mathrm{bf}}(t)>e^{-\gamma t}$,

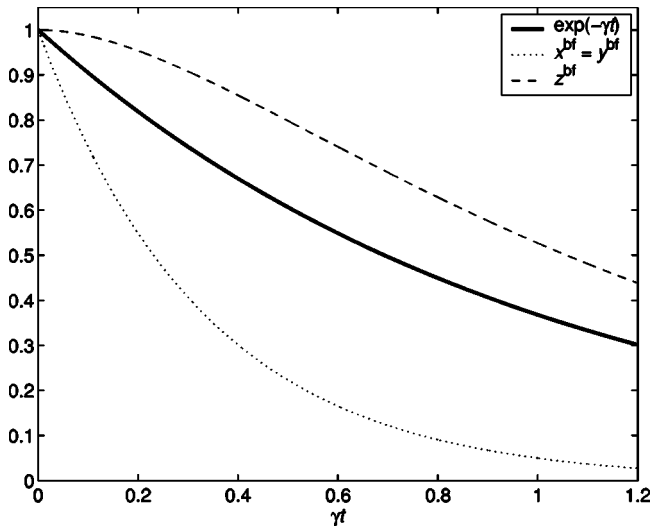

FIG. 3. The effective channel $[x^{\mathrm{bf}}(t),y^{\mathrm{bf}}(t),z^{\mathrm{bf}}(t)]$ due to the bit-flip code under the symmetric depolarizing channel. The respective fidelities of X, Y, and Z eigenstates for correction performed at time t are given by $\frac{1}{2}[1+x^{\mathrm{bf}}(t)]$, $\frac{1}{2}[1+y^{\mathrm{bf}}(t)]$, and $\frac{1}{2}[1+z^{\mathrm{bf}}(t)]$.

and thus the decoherence of $\langle Z\rangle$ is suppressed by the bit-flip code. However, $x^{\mathrm{bf}}(t)=y^{\mathrm{bf}}(t)<e^{-\gamma t}$, and thus the decoherences of $\langle X\rangle$ and $\langle Y\rangle$ are increased by the bit-flip code.

More generally, for any $0<x,z<1$ we have $\frac{3}{2}z-\frac{1}{2}z^3>z$ and $x^3<x$, so for any physical channel in this regime the bit-flip code always suppresses decoherence of $\langle Z\rangle$ and increases decoherence of $\langle X\rangle$. Decoherence of $\langle Y\rangle$ is suppressed when $x>\sqrt{2/3}$ and $0<y<\sqrt{3x^2-2}$, and increased for all other positive values of x and y. We may therefore conclude that under a general Pauli channel the bit-flip code increases the fidelity of some transmitted states at the expense of others, and thus the bit-flip code is outperformed by storing the logical qubit in a single physical bit.

However, as the bit-flip code is designed to only protect against physical bit-flip (X) errors, it should not be expected to perform well in the presence of arbitrary Pauli errors. If we consider physical channels with only X errors, we find that the bit-flip code suppresses decoherence of all encoded states. More precisely, suppose that the physical qubits are evolving via a Pauli channel (36) with only X errors, i.e., $p_Y=p_Z=0$. Then $[x,y,z]=[1,1-2p_X,1-2p_X]$, and $\Omega^{\mathrm{bf}}([x,y,z])=[1,1-\frac{3}{2}p_X^2+\frac{1}{2}p_X^3,1-\frac{3}{2}p_X^2+\frac{1}{2}p_X^3]$. Thus we have reproduced the usual result of a leading-order analysis: the bit-flip code suppresses decoherence due to X errors to order p_X^2.

Now consider the three-qubit phase-flip code [3], with encoding $|\pm\rangle\mapsto|\pm\pm\pm\rangle$ for $|\pm\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)$. This code is completely analogous to the bit-flip code, detecting and correcting single phase-flip (Z) errors instead of single bit-flip (X) errors. The phase-flip code's coding map Ω^{pf} is exactly the same as that of the bit-flip code, with the role of X and Z interchanged,

$$\Omega^{\mathrm{pf}}([x,y,z])=[\tfrac{3}{2}x-\tfrac{1}{2}x^3,\tfrac{3}{2}z^2y-\tfrac{1}{2}y^3,z^3]. \qquad (39)$$

The concatenation phase-flip(bit-flip) yields the Shor nine-bit

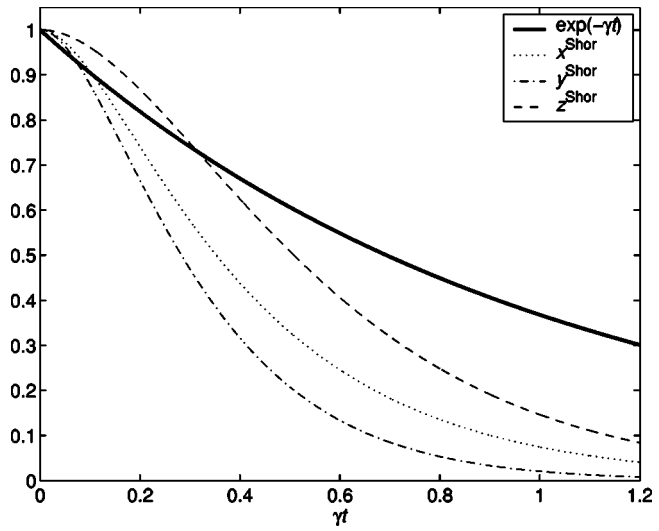

FIG. 4. The effective channel $[x^{\mathrm{Shor}}(t),y^{\mathrm{Shor}}(t),z^{\mathrm{Shor}}(t)]$ due to the Shor code under the symmetric depolarizing channel.

code [1,3] with encoding $|\pm\rangle\mapsto 1/\sqrt{8}(|000\rangle\pm|111\rangle)^{\otimes 3}$. Thus $\Omega^{\mathrm{Shor}}=\Omega^{\mathrm{pf}}\circ\Omega^{\mathrm{bf}}$. Evaluating this composition by using the coding maps (38) and (39),

$$\Omega^{\mathrm{Shor}}([x,y,z])=\Omega^{\mathrm{pf}}(\Omega^{\mathrm{bf}}([x,y,z])) =[P(x),Q(x,y,z),R(z)], \tag{40}$$

where

$$P(x)=\tfrac{3}{2}x^3-\tfrac{1}{2}x^9,$$

$$Q(x,y,z)=\tfrac{3}{2}(\tfrac{3}{2}z-\tfrac{1}{2}z^3)^2(\tfrac{3}{2}x^2y-\tfrac{1}{2}y^3)-\tfrac{1}{2}(\tfrac{3}{2}x^2y-\tfrac{1}{2}y^3)^3,$$

$$R(z)=(\tfrac{3}{2}z-\tfrac{1}{2}z^3)^3. \tag{41}$$

(The combinatoric analysis required to reproduce this result by counting bit-flip and phase-flip errors would be quite tedious.)

To examine the Shor code acting on the symmetric depolarizing channel, let $[x^{\mathrm{Shor}}(t),y^{\mathrm{Shor}}(t),z^{\mathrm{Shor}}(t)] =\Omega^{\mathrm{Shor}}(\mathcal{N}_t^{\mathrm{dep}})$; the functions x^{Shor}, y^{Shor}, and z^{Shor} are plotted in Fig. 4. We see that for short times (or equivalently, weak noise-strength γ), the Shor code suppresses decoherence of $\langle X\rangle$, $\langle Y\rangle$, and $\langle Z\rangle$. For long times, however, the code increases the decoherence of all three expectation values, and as $z^{\mathrm{Shor}}(t)>x^{\mathrm{Shor}}(t)>y^{\mathrm{Shor}}(t)$, in an intermediate regime the code suppresses the decoherence of some of the expectation values while increasing that of others. Thus to suppress the decoherence of an arbitrary logical state, correction needs to be performed at a time t when $y^{\mathrm{Shor}}(t)>e^{-\gamma t}$.

Above we defined the phase-flip code by the encoding $|\pm\rangle\mapsto|\pm\pm\pm\rangle$; we could have also used the encoding given by $|0\rangle\mapsto|+++\rangle$, $|1\rangle\mapsto|---\rangle$. Call the code with this encoding phase-flip II, with coding map Ω^{pfII}. As this modification of the phase-flip code simply interchanges the encoded X and Z eigenstates, the new effective channel is simply that of the original phase-flip code with the effects of the channel on the X and Z components of $\vec{\rho}_0$ interchanged: $\Omega^{\mathrm{pfII}}([x,y,z])=[z^3,\frac{3}{2}z^2y-\frac{1}{2}y^3,\frac{3}{2}x-\frac{1}{2}x^3]$ [compare to Eq. (39)]. We could then use this version of the phase-flip code to define an alternative version of the Shor code with the encoding $|0\rangle\mapsto 1/\sqrt{8}(|000\rangle+|111\rangle)^{\otimes 3}$, $|1\rangle\mapsto 1/\sqrt{8}(|000\rangle -|111\rangle)^{\otimes 3}$. Call this code Shor II, with corresponding coding map $\Omega^{\mathrm{Shor\,II}}=\Omega^{\mathrm{pfII}}\circ\Omega^{\mathrm{bf}}$. We find

$$\Omega^{\mathrm{Shor\,II}}([x,y,z])=[R(z),Q(x,y,z),P(x)], \tag{42}$$

with the polynomials P, Q, and R defined by Eq. (41). Comparing to Eq. (40), we see that again this modification of the Shor code simply interchanges the effect of the channel on X and Z components of $\vec{\rho}_0$. Assuming that the encoded logical states are randomly distributed (as opposed to always sending Z eigenstates, for example), the choice of using the Shor code or the Shor II code is simply one of aesthetics: the effective channels are identical up to the interchange of the decoherence of $\langle X\rangle$ and $\langle Z\rangle$. However, as we will see in the next section, this choice does have an impact when these codes are concatenated.

For comparison, we consider two other stabilizer codes of interest. The Steane code [2,3] is a seven-bit code designed to correct errors consisting either of a Pauli error (X, Y, or Z) on a single qubit of the codeword, or of an X and a Z error on separate qubits. We find

$$\Omega^{\mathrm{Steane}}([x,y,z])=[S(x),T(x,y,z),S(z)] \tag{43}$$

with

$$S(x)=\tfrac{7}{4}x^3-\tfrac{3}{4}x^7,$$

$$T(x,y,z)=\tfrac{7}{16}y^3+\tfrac{9}{16}y^7-\tfrac{21}{16}(x^4+z^4)y^3+\tfrac{21}{8}x^2yz^2. \tag{44}$$

Let $[x^{\mathrm{Steane}}(t),y^{\mathrm{Steane}}(t),z^{\mathrm{Steane}}(t)]=\Omega^{\mathrm{Steane}}(\mathcal{N}_t^{\mathrm{dep}})$; we find that the functions x^{Steane}, y^{Steane}, and z^{Steane} are qualitatively similar to the analogous functions of the Shor code. If they were plotted in Fig. 4, these functions would be interspersed between the plotted curves: for all values of $t>0$, we have $z^{\mathrm{Shor}}>z^{\mathrm{Steane}}=x^{\mathrm{Steane}}>x^{\mathrm{Shor}}>y^{\mathrm{Steane}}>y^{\mathrm{Shor}}$. Though the Shor code more effectively suppresses decoherence for logical Z eigenstates, the Steane code performs better in the worst case (Y eigenstates), and thus outperforms the Shor code.

The five-bit code [3,13,14] corrects Pauli errors on a single qubit of the codeword. We find

$$\Omega^{\mathrm{Five}}([x,y,z])=[U(x,y,z),U(y,z,x),U(z,x,y)] \tag{45}$$

with

$$U(x,y,z)=\tfrac{5}{4}x(y^2+z^2)-\tfrac{5}{4}xy^2z^2-\tfrac{1}{4}x^5. \tag{46}$$

Letting $[x^{\mathrm{Five}}(t),y^{\mathrm{Five}}(t),z^{\mathrm{Five}}(t)]=\Omega^{\mathrm{Five}}(\mathcal{N}_t^{\mathrm{dep}})$ yields $x^{\mathrm{Five}} =y^{\mathrm{Five}}=z^{\mathrm{Five}}$, as expected from the symmetries of the code and of the map Ω^{Five}. Thus the fidelity of a state through this channel is independent of the state. These functions also have behavior qualitatively similar to those plotted in Fig. 4, and for $t>0$ we have $z^{\mathrm{Shor}}>z^{\mathrm{Five}}>z^{\mathrm{Steane}}>x^{\mathrm{Shor}}$. Thus the five-bit code outperforms both the Shor and Steane codes.

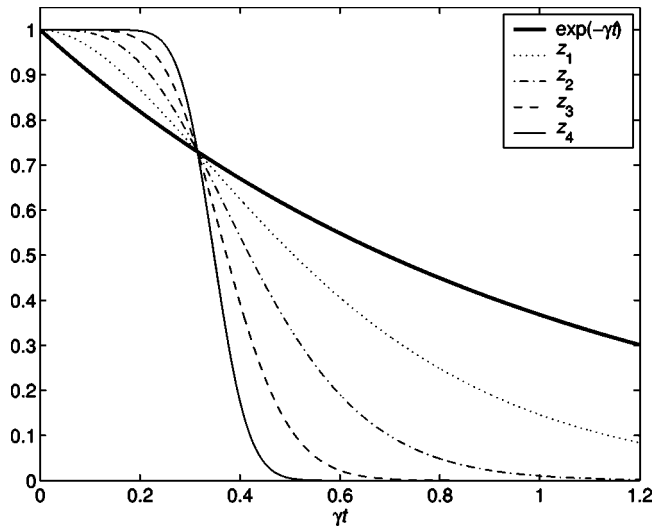

FIG. 5. The functions z_ℓ, where $[x_\ell(t),y_\ell(t),z_\ell(t)]$ is the effective channel for ℓ concatenations of the Shor code under the symmetric depolarizing channel.

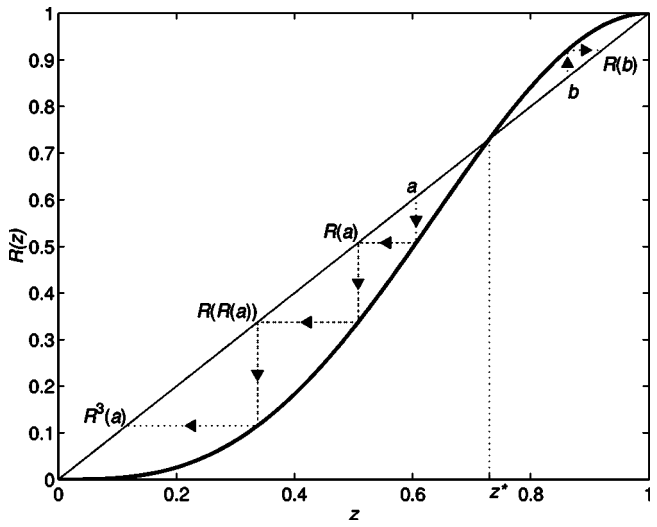

FIG. 6. The function $R(z)$ (plotted as the thick curve). Observe that the map $z \mapsto R(z)$ has fixed points at 0, 1, and $z^\star$. The arrows depict the iteration of this map pushing points in the interval $(0,z^\star)$ toward 0 and points in the interval $(z^\star,1)$ toward 1.

VII. EXACT PERFORMANCE AND THRESHOLDS FOR CERTAIN CONCATENATION SCHEMES

We now consider the effective channel due to families of concatenated codes under the symmetric depolarizing channel. First, consider the Shor code concatenated with itself ℓ times, denoted by Shor$-\ell$. From Sec. IV, we know that the coding map for this code is given by $\Omega^{(\mathrm{Shor}-\ell)} = \Omega^{\mathrm{Shor}} \circ \cdots \circ \Omega^{\mathrm{Shor}} = (\Omega^{\mathrm{Shor}})^\ell$. As Ω^{Shor} takes diagonal channels to diagonal channels, the effective channel due to Shor $-\ell$ is also diagonal. Let

$$[x_\ell(t),y_\ell(t),z_\ell(t)] = (\Omega^{\mathrm{Shor}})^\ell(\mathcal{N}_t^{\mathrm{dep}}), \tag{47}$$

which may be calculated using the polynomials of Ω^{Shor} given in Eq. (41).

The functions $z_\ell(t)$ for $0 \leqslant \ell \leqslant 4$ are plotted in Fig. 5. We immediately observe that as $\ell \to \infty$ the functions $z_\ell(t)$ approach a step function. Denoting the step function's time of discontinuity by $t_Z^\star$, we have $z_\ell(t) \to \theta(t_Z^\star - t)$ where

$$\theta(x) = \begin{cases} 0 & x<0 \\ 1 & x>0. \end{cases} \tag{48}$$

For $t<t_Z^\star$, each layer of concatenation decreases the $\langle Z \rangle$ decoherence, yielding perfect preservation of the encoded $\langle Z \rangle$ information in the infinite concatenation limit. However, for $t>t_Z^\star$, the $\langle Z \rangle$ decoherence increases. Thus in the infinite concatenation limit, the code will perfectly protect $\langle Z \rangle$ of the logical qubit if correction is performed prior to $t_Z^\star$; if correction is performed after this time, all $\langle Z \rangle$ information is lost.

Similarly, the functions $x_\ell(t)$ and $y_\ell(t)$ approach step function limits as $\ell \to \infty$; call the discontinuous times of these step functions $t_X^\star$ and $t_Y^\star$. To perfectly protect an arbitrary state in the infinite concatenation limit, correction must be performed prior to $t_{\mathrm{th}} = \min(t_X^\star, t_Y^\star, t_Z^\star)$. We call t_{th} the *storage threshold*. (We use the term "storage threshold" to indicate that the threshold takes into account only noise in the register, rather than gate or measurement errors which are also considered in fault-tolerant settings.) We now show how the coding map Ω^{Shor} may be used to find this threshold.

Observe in Fig. 5 that all the plots of $z_\ell(t)$ intersect at a point $(\gamma t_Z^\star, z^\star)$. Writing Ω^{Shor} in the form (40), we have $z_{\ell+1}(t) = R(z_\ell(t))$. The function $R(z)$ is plotted in Fig. 6. We see that the map $z \mapsto R(z)$ has fixed points at 0, 1, and a point $z^\star \approx 0.7297$. [We find $z^\star$ by numerically solving $z = R(z)$ on the interval $(0,1)$.] Iterating the map pushes points in the interval $(0,z^\star)$ toward 0, and pushes points in the interval $(z^\star,1)$ toward 1. In the language of dynamical systems [10], 0 and 1 are attracting fixed points, and $z^\star$ is a repelling fixed point. This behavior leads to the shape of the plots in Fig. 5. We then invert $e^{-\gamma t_Z^\star} = z^\star$ to find $\gamma t_Z^\star = 0.3151$. The function $P(x)$ has the same qualitative behavior on $(0,1)$ as $R(z)$, so we may similarly find $x^\star \approx 0.9003$ and $\gamma t_X^\star \approx 0.1050$.

We cannot use the same method to find $t_Y^\star$, as $y_{\ell+1}(t)$ is a function of $x_\ell(t)$, $y_\ell(t)$, and $z_\ell(t)$, not of $y_\ell(t)$ alone. [This problem is evident from plots of the functions $y_\ell(t)$: though these functions approach a step function in the $\ell \to \infty$ limit, they do not all intersect at a point as the plots of $z_\ell(t)$ do.] However, we now argue that finding $t_X^\star$ and $t_Z^\star$ is sufficient to find $t_Y^\star$. For $t<t_X^\star$, $x_\ell(t) \to 1$ and $z_\ell(t) \to 1$. Using the complete positivity constraints (35), we find that if $[x,y,z]$ is a channel, $x=z=1$ implies $y=1$. Since the space of channels $[x,y,z]$ is closed and bounded (it consists of the boundary and interior of a tetrahedron in $\mathbb{R}^3$), $x_\ell(t) \to 1$ and $z_\ell(t) \to 1$ implies $y_\ell(t) \to 1$. Now for $t_X^\star < t < t_Z^\star$, $x_\ell(t) \to 0$, and $z_\ell(t) \to 1$. Using the complete positivity constraints (35), we find that if $[x,y,z]$ is a channel, $x=0$ and $z=1$ implies $y=0$. Thus we may conclude that for these values of t, $y_\ell(t) \to 0$. We now have $y_\ell(t) \to 1$ for $t<t_X^\star$, and $y_\ell(t) \to 0$ for $t>t_X^\star$, thus we conclude $t_Y^\star = t_X^\star$. More

TABLE I. Code storage threshold results (see text for discussion.)

Code	Shor		Shor II		Steane	Five-bit
σ	X,Y	Z	X,Y	Z	X,Y,Z	X,Y,Z
$\gamma t^\star_\sigma$	0.1050	0.3151	0.1618	0.2150	0.1383	0.2027
p_{th}	0.0748		0.1121		0.0969	0.1376

generally, if we know $t^\star_X$ and $t^\star_Z$, then $t^\star_Y$ is given by $\min(t^\star_X,t^\star_Z)$. We may therefore conclude that $\gamma t^\star_Y \approx 0.1050$, and so $\gamma t_{\text{th}} \approx 0.1050$. (The value of $t^\star_Y$ could also be obtained from the dynamics of the polynomial maps P, Q, and R without making reference to the complete positivity constraint, but the method presented here requires less argumentation.)

We may also phrase these thresholds in the language of finitely probable errors. Consider the symmetric Pauli channel given by Eq. (36) with $p_X=p_Y=p_Z=p/3$. This channel subjects a qubit to a random Pauli error with probability p, and is described by $\mathcal{N}^{\text{Pauli}}(p)=[1-\frac{4}{3}p,1-\frac{4}{3}p,1-\frac{4}{3}p]$. Observe that the symmetric Pauli channel and the symmetric depolarizing channel are related by $\mathcal{N}^{\text{Pauli}}(\frac{3}{4}(1-e^{-\gamma t}))=\mathcal{N}^{\text{dep}}_t$. Thus in the infinite concatenation limit with $\mathcal{N}^{\text{Pauli}}(p)$ acting on each register qubit, the $\langle\sigma\rangle$ of the logical qubit will be perfectly protected if $p<p^\star_\sigma=\frac{3}{4}(1-e^{-\gamma t^\star_\sigma})$. Define the threshold probability $p_{\text{th}}=\min\{p^\star_X,p^\star_Y,p^\star_Z\}$; for $p<p_{\text{th}}$, all encoded qubits are perfectly protected in the infinite concatenation limit. Values for $\gamma t^\star_\sigma$ and p_{th} appear in Table I.

We now use similar methods to derive thresholds for the Shor II, Steane, and five-bit codes presented in the preceding section. First, consider the Shor II code. Let $[x'_\ell(t),y'_\ell(t),z'_\ell(t)]=(\Omega^{\text{Shor II}})^\ell(\mathcal{N}^{\text{dep}}_t)$. The $y'_\ell(t)$ approach a step function as $\ell\to\infty$, but $x'_\ell(t)$ and $z'_\ell(t)$ approach a limit cycle of period 2: we find that $x'_{2\ell}$ and $z'_{2\ell+1}$ both approach $\theta(t^\star_1-t)$ for some value of $t^\star_1$, while $x'_{2\ell+1}$ and $z'_{2\ell}$ approach $\theta(t^\star_2-t)$ for some distinct value of $t^\star_2$. From the form of $\Omega^{\text{Shor II}'}$ given in Eq. (42), we see that $x'_{\ell+1}(t)$ is a function of $z'_\ell(t)$, and $z'_{\ell+1}(t)$ a function of $x'_\ell(t)$, so it is not so surprising that the sequence $z'_0,x'_1,z'_2,x'_3,\ldots$ converges and the sequence $x'_0,z'_1,x'_2,z'_3,\ldots$ converges. To find the threshold, we simply consider the sequence of channels $[x'_{2\ell},y'_{2\ell},z'_{2\ell}]$, generated by the map $(\Omega^{\text{Shor II}})^2$. From Eq. (42) we see that $x'_{2(\ell+1)}=R(P(x'_{2\ell}))$ and $z'_{2(\ell+1)}=P(R(z'_{2\ell}))$. Thus to find the values $t^\star_X$, $t^\star_Y$, and $t^\star_Z$, we find the fixed points of the maps $x\mapsto R(P(x))$ and $z\mapsto P(R(z))$, and proceed as with the Shor code. As shown in Table I, we find that, compared to the Shor code, the Shor II code has greater values for $t^\star_X$ and $t^\star_Y$, and a lesser value for $t^\star_Z$. As the threshold t_{th} is given by the minimum of these three values, the Shor II code outperforms the Shor code in the infinite concatenation limit.

The map Ω^{Steane}, given by Eq. (43), has the same form as the Shor code map (40), and therefore we can use the same methods to find the Steane code thresholds. The map Ω^{Five}, given by Eq. (45), has a different form. However, as $\mathcal{N}^{\text{dep}}_t$ has the symmetric form $[x,x,x]$ and Ω^{Five} preserves this symmetry by taking $[x,x,x]$ to $[U(x,x,x),U(x,x,x),U(x,x,x)]$, we may find $t^\star_X=t^\star_Y=t^\star_Z$ simply by finding the fixed point of $x\mapsto U(x,x,x)$. Results are summarized in Table I. We find that the five-bit code has the largest threshold, and therefore the best performance in the infinite concatenation limit. It is interesting to note that the Shor II code outperforms the Steane code in the infinite concatenation limit, even though the opposite is true for only one layer of each code.

We conclude our discussion of the thresholds by comparing the exact values of p_{th} to those calculated with traditional leading-order techniques (e.g., in Ref. [3]). First consider the five-bit code. Under the symmetric Pauli channel $\mathcal{N}^{\text{Pauli}}(p)$, a physical qubit is unmodified with probability $1-p$. The five-bit code perfectly protects its encoded information if no more than one of the five physical qubits are subjected to a Pauli error. Under $\mathcal{N}^{\text{Pauli}}(p)$, the probability of no errors on any physical qubit is $(1-p)^5$, and the probability of exactly one error is $5p(1-p)^4$. We then assume that all greater-weight errors are uncorrectable, and find that the probability of a correctable error is $(1-p)^5+5p(1-p)^4=1-10p^2+O(p^3)$. The threshold value p_{th} is the value of p at which the single physical qubit and the encoded information have the same probability of error. Thus to estimate the threshold we solve $1-10p^2=1-p$, yielding $p_{\text{th}}=\frac{1}{10}$. Thus the leading-order calculation underestimates the actual threshold (0.1376) by 27%. (The assumption that all errors of greater weight are uncorrectable assures that the approximation underestimates, rather than overestimates, the threshold.) The Steane code corrects all weight-one errors, and weight-two errors consisting of an X on one bit and a Z on another bit. A similar calculation finds the probability of a correctable error to be $1-\frac{49}{3}p^2+O(p^3)$, yielding $p_{\text{th}}\approx 0.0612$, a 37% underestimate. The Shor code corrects all weight-one errors, and weight-two errors such that any X and Y operators occur in different blocks, and any Y and Z errors occur in the same block. The probability of a correctable error is found to be $1-16p^2+O(p^3)$, yielding $p_{\text{th}}=0.0625$, a 16% underestimate. The analysis is exactly the same for the Shor II code, yet the Shor II code has a very different threshold; in this case, the leading-order result underestimates the threshold by 44%.

VIII. CONCLUSION

We have shown how a code's performance for a given error model can be described by the effective channel for the encoded information. The methods presented for calculating the effective channel have allowed us to find the performance of several codes of interest under single-bit Pauli channels, and further have allowed us to find thresholds describing these codes' asymptotic limits of concatenation under the symmetric depolarizing channel. Though we chose to restrict our attention to diagonal channels, these methods can be applied to any uncorrelated error model (e.g., the amplitude-damping channel [3], which is nondiagonal), and will substantially simplify the exact analysis of code performance in these more general settings.

We believe that this effective channel description of code performance may be useful in other contexts as well. For example, this work could be extended to take account of encoding and decoding circuit errors, thereby providing a method for calculating exact fault-tolerant thresholds. Also, by providing a comprehensive method for describing the performance of a quantum code without reference to a particular error model (e.g., bit-flip and phase-flip errors) perhaps these methods will allow us to address open questions such as the optimal code for a given error model, and the quantum channel capacity.

ACKNOWLEDGMENTS

This work was partially supported by the Caltech MURI Center for Quantum Networks and the NSF Institute for Quantum Information. B.R. acknowledges the support of the NSF and thanks J. Preskill and P. Parrilo for insightful discussions.

APPENDIX A: STABILIZER CODES AND DIAGONAL CHANNELS

In this appendix we consider the effective channel $\mathcal{G}=\Omega^C(\mathcal{N}^{(1)})$ when $\mathcal{N}^{(1)}$ is diagonal and C is a stabilizer code. We show that $\mathcal{G}$ is also diagonal, and show how the stabilizer formalism facilitates its calculation. The reader unfamiliar with stabilizer codes is directed to Ref. [3] for an introduction, and to Ref. [12] for a more complete discussion.

Since $\mathcal{N}^{(1)}$ is diagonal, the terms $N^{(1)}_{\nu_i\mu_i}$ in the expression for the effective channel (25) vanish for $\nu_i\neq\mu_i$. Thus we have

$$\mathcal{G}_{\sigma\sigma'}=\sum_{\{\mu_i\}}\left(\beta^{\sigma}_{\{\mu_i\}}\alpha^{\sigma'}_{\{\mu_i\}}\prod_{i=1}^{N}\mathcal{N}^{(1)}_{\mu_i\mu_i}\right), \tag{A1}$$

dramatically simplifying the calculation of $\mathcal{G}$. The coefficients $\alpha^{\sigma'}_{\{\mu_i\}}$ and $\beta^{\sigma}_{\{\mu_i\}}$ are defined in terms of the $E_{\sigma'}$ and D_σ operators in Eqs. (20) and (21); to calculate these operators we now consider the code C in more detail.

Let C be a stabilizer code given by stabilizer $S=\{S_k\}\subset\pm\{I,X,Y,Z\}^{\otimes N}$, storing one qubit in an N-qubit register. The stabilizer S defines the codespace, and the logical operators $\overline{I},\overline{X},\overline{Y},\overline{Z}\subset\pm\{I,X,Y,Z\}^{\otimes N}$ determine the particular basis of codewords $|\overline{0}\rangle$, $|\overline{1}\rangle$. Recall that the $E_{\sigma'}$ operators act as $\frac{1}{2}\sigma'$ on the codespace and vanish elsewhere. It can be shown that $P_C=(1/|S|)\Sigma_k S_k$ acts as a projector onto the codespace, and by definition the logical operators $\overline{\sigma'}$ act as σ' on the codespace. Thus

$$E_{\sigma'}=\tfrac{1}{2}P_C\overline{\sigma'}=\frac{1}{2|S|}\sum_k S_k\overline{\sigma'} \tag{A2}$$

will act as $\frac{1}{2}\sigma'$ on the codespace and vanish elsewhere.

As an example, consider the bit-flip code introduced in Sec. II A. The bit-flip code may be specified as a stabilizer code, with $S=\{III,ZZI,IZZ,ZIZ\}$, $\overline{I}=III$, $\overline{X}=XXX$, $\overline{Y}=-YYY$, $\overline{Z}=ZZZ$. The above expression reproduces the expressions for the $E_{\sigma'}$ presented in Eq. (22). Without the stabilizer formalism, deriving Eq. (22) is an exercise in expanding projectors in a basis of Pauli operators; with this method the computation is very simple.

We now construct the D_σ operators for the stabilizer code. As in Sec. II A, let $\{P_j\}$ be the projectors describing the syndrome measurement. For a stabilizer code, the recovery operators R_j are each chosen to be a Pauli operator taking the space projected by P_j back to the codespace. Consider the expression for D_σ given by Eq. (16); substituting in the expression (A2) for E_σ, we have

$$D_\sigma=\frac{1}{|S|}\sum_{k,j}R_j^\dagger S_k\overline{\sigma}R_j. \tag{A3}$$

Now because R_j, S_k, and $\overline{\sigma}$ are all Pauli operators, they either commute or anticommute. For two Pauli operators V and W, let $\eta(V,W)=\pm1$ for $VW=\pm WV$. Commuting the R_j to the left in the above expression and noting that $R_j^\dagger R_j=1$,

$$\begin{aligned}D_\sigma&=\frac{1}{|S|}\sum_{k,j}\eta(S_k,R_j)\,\eta(R_j,\overline{\sigma})S_k\overline{\sigma}\\&=\frac{1}{|S|}\sum_k f_{k\sigma}S_k\overline{\sigma}\end{aligned} \tag{A4}$$

with $f_{k\sigma}=\Sigma_j\eta(S_k,R_j)\,\eta(R_j,\overline{\sigma})$. Again, as an example, consider the stabilizer definition of the bit-flip code. The recovery operators are III, XII, IXI, and IXI. Evaluating the above expression for D_σ yields the previous result of Eq. (23).

Using the expressions (A2) and (A4) for the $E_{\sigma'}$ and D_σ operators in the stabilizer formalism, we will now find the coefficients $\alpha^{\sigma'}_{\{\mu_i\}}$ and $\beta^{\sigma}_{\{\nu_i\}}$ as defined in Eqs. (20) and (21). Since $S_k\overline{\sigma}$ is a Pauli operator, the sums (A2) and (A4) are expansions of these operators $E_{\sigma'}$ and D_σ in the Pauli basis; if we were to write down these sums explicitly for a given stabilizer code, the coefficients α and β could be read off immediately, e.g., from Eqs. (22) and (23).

This approach may be formalized as follows. First, note that S_k and $\overline{\sigma}$ are both Hermitian Pauli operators, and they commute; therefore their product is also a Hermitian Pauli operator, i.e., $S_k\overline{\sigma}\in\pm\{I,X,Y,Z\}^{\otimes N}$. For any operator $V=\pm\mu_1\otimes\cdots\otimes\mu_N$ with $\mu_i\in\{I,X,Y,Z\}$, let $\phi(V)=\mu_1\otimes\cdots\otimes\mu_N$, and let $a(V)\in\{0,1\}$ such that $V=(-1)^{a(V)}\phi(V)$. Then, using $|S|=2^{N-1}$, we may rewrite Eqs. (A2) and (A4) as

$$E_{\sigma'}=\sum_k(-1)^{a(S_k\overline{\sigma'})}\frac{1}{2^N}\phi(S_k\overline{\sigma'}), \tag{A5}$$

$$D_\sigma=\sum_k(-1)^{a(S_k\overline{\sigma})}\frac{1}{|S|}f_{k\sigma}\phi(S_k\overline{\sigma}). \tag{A6}$$

Comparing Eq. (A5) with the definition of $\alpha^{\sigma'}_{\{\mu_i\}}$ in Eq. (20), we see that each term of the sum over k contributes to a single coefficient $\alpha^{\sigma'}_{\phi(S_k\overline{\sigma'})}$, as $(1/2^N)\phi(S_k\overline{\sigma'})$ is of the form $(\frac{1}{2}\mu_1\otimes\cdots\otimes\frac{1}{2}\mu_N)$. Similarly, each term in Eq. (A6) contributes to a single coefficient $\beta^{\sigma}_{\phi(S_k\overline{\sigma})}$. Lemma 2 of Appendix B shows that $\phi(S_k\overline{\sigma})\neq\phi(S_{k'}\overline{\sigma})$ unless $k=k'$ and $\sigma=\sigma'$. Thus each term in Eq. (A5) contributes to a *distinct* coefficient $\alpha^{\sigma'}_{\phi(S_k\overline{\sigma'})}$, and each term in (A6) contributes to a *distinct* coefficient $\beta^{\sigma}_{\phi(S_k\overline{\sigma})}$. We may therefore simply read off the coefficients from Eqs. (A5) and (A6), yielding

$$\alpha^{\sigma'}_{\phi(S_k\overline{\sigma'})}=(-1)^{a(S_k\overline{\sigma'})}, \tag{A7}$$

$$\beta^{\sigma}_{\phi(S_k\overline{\sigma})}=(-1)^{a(S_k\overline{\sigma})}\frac{1}{|S|}f_{k\sigma}, \tag{A8}$$

and all other $\alpha^{\sigma'}_{\{\mu_i\}}$ and $\beta^{\sigma}_{\{\mu_i\}}$ vanishing.

We now evaluate $\mathcal{G}=\Omega^C(\mathcal{N}^{(1)})$ where $\mathcal{N}^{(1)}=[x,y,z]$ using Eq. (A1). The only nonvanishing terms $\beta^{\sigma}_{\{\mu_i\}}$ occur when $\mu_1\otimes\cdots\otimes\mu_N=\phi(S_k\overline{\sigma})$ for some k and σ, and the only nonvanishing terms $\alpha^{\sigma'}_{\{\mu_i\}}$ occur when $\mu_1\otimes\ldots\otimes\mu_N=\phi(S_k\overline{\sigma'})$ for some k and σ'. Thus the coefficients $\beta^{\sigma}_{\{\mu_i\}}\alpha^{\sigma'}_{\{\mu_i\}}$ of Eq. (A1) will vanish unless $\mu_1\otimes\cdots\otimes\mu_N=\phi(S_k\overline{\sigma})=\phi(S_{k'}\overline{\sigma'})$ for some k and k'. As proved in Lemma 2 of Appendix B, this cannot happen when $\sigma\neq\sigma'$. Thus all the matrix elements $\mathcal{G}_{\sigma\sigma'}$ vanish when $\sigma\neq\sigma'$, i.e., $\mathcal{G}$ is diagonal.

Having demonstrated that the coding map Ω^C of a stabilizer code C takes diagonal channels to diagonal channels, and because $\mathcal{G}_{II}=1$ from trace preservation, we need to only compute $\mathcal{G}_{XX}$, $\mathcal{G}_{YY}$, and $\mathcal{G}_{ZZ}$ by using Eq. (A1) to find $\mathcal{G}=\Omega^C([x,y,z])$. These computations can be performed using the methods of Sec. III, but we conclude this section by expressing these elements by using the stabilizer formalism, which may be computationally advantageous.

Consider the diagonal terms $\mathcal{G}_{\sigma\sigma}$ given by Eq. (A1). We need to only sum over the nonvanishing coefficients α and β, which are given by Eqs. (A7) and (A8). Substituting in these expressions yields

$$\mathcal{G}_{\sigma\sigma}=\sum_k\left(\frac{1}{|S|}f_{k\sigma}\prod_{i=1}^{N}\mathcal{N}^{(1)}_{\phi_i(S_k\overline{\sigma})\phi_i(S_k\overline{\sigma})}\right), \tag{A9}$$

where $\phi_i(V)$ denotes μ_i for $\phi(V)=\mu_1\otimes\cdots\otimes\mu_N$. Now as $\mathcal{N}^{(1)}=[x,y,z]$, the product of the matrix elements of $\mathcal{N}^{(1)}$ in the previous expression is simply a product of x's, y's, and z's; each factor appears as many times as (respectively) X, Y, and Z appear in $\phi(S_k\overline{\sigma})$. Letting $w_\sigma(p)$ denote the σ weight of a Pauli operator p, e.g., $w_X(XYX)=2$, we have

$$\mathcal{G}_{\sigma\sigma'}=\delta_{\sigma\sigma'}\frac{1}{|S|}\sum_k f_{k\sigma}x^{w_X(S_k\overline{\sigma})}y^{w_Y(S_k\overline{\sigma})}z^{w_Z(S_k\overline{\sigma})}. \tag{A10}$$

APPENDIX B

This appendix contains lemmas deferred from previous sections.

Lemma 1. The decoding operation $\mathcal{D}$ given by Eq. (4) is a quantum operation.

Proof. From Eq. (4) we have

$$\mathcal{D}[\rho]=\sum_j B^\dagger A_j\rho A_j^\dagger B. \tag{B1}$$

To prove that $\mathcal{D}$ is a quantum operation, we must show that

$$\sum_j (A_j^\dagger B)(B^\dagger A_j)=\mathbf{1}, \tag{B2}$$

where $\mathbf{1}$ is the identity on the register space. As we assumed that $\mathcal{R}$ maps all states into the codespace, we can choose the operators A_j to only have range on the codespace. With such a choice, $A_j^\dagger A_j=A_j^\dagger(|\overline{0}\rangle\langle\overline{0}|+|\overline{1}\rangle\langle\overline{1}|)A_j=A_j^\dagger BB^\dagger A_j$. We therefore have

$$\sum_j (A_j^\dagger B)(B^\dagger A_j)=\sum_j A_j^\dagger A_j. \tag{B3}$$

From Eq. (3) we have $\Sigma_j A_j^\dagger A_j=\mathbf{1}$, and so $\mathcal{D}$ is a quantum operation. ■

Lemma 2. For a stabilizer code with stabilizer $\{S_k\}$ and logical operators $\{\overline{\sigma}\}$, and ϕ defined in Appendix A, $\phi(S_k\overline{\sigma})\neq\phi(S_{k'}\overline{\sigma'})$ unless $k=k'$ and $\sigma=\sigma'$.

Proof. Suppose we have $\phi(S_k\overline{\sigma})=\phi(S_{k'}\overline{\sigma'})$; then $S_k\overline{\sigma}=\pm S_{k'}\overline{\sigma'}$. As the stabilizers S_k and $S_{k'}$ act trivially on the codespace, $S_k\overline{\sigma}$ and $\pm S_{k'}\overline{\sigma'}$ act respectively as σ and $\pm\sigma'$ on the codespace. Thus we must have $\sigma=\pm\sigma'$, which requires $\sigma=\sigma'$ and the $\pm$ sign be positive. We now have $S_k\overline{\sigma}=S_{k'}\overline{\sigma}$; right-multiplying by $\overline{\sigma}$ yields $S_k=S_{k'}$, and thus $k=k'$. ■

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

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

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000), and references therein; J. Preskill, http://theory.caltech.edu/~preskill/ph219.

[4] J. Preskill, e-print quant-ph/9712048, 1997, and references therein.

[5] E. Knill and R. Laflamme, e-print quant-ph/9698012, 1996.

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

[7] K. Kraus, *States, Effect, and Operations* (Springer-Verlag, Berlin, 1983).

[8] M. B. Ruskai *et al.*, e-print quant-ph/0101003, 2001.

[9] D. A. Lidar *et al.*, Phys. Rev. A **63**, 022306 (2001).

[10] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems* (Addison-Wesley, London, 1989).
[11] C. King and M. B. Ruskai, IEEE Trans. Inf. Theory **47**, 192 (2001); e-print quant-ph/9911079.
[12] D. Gottesman, Ph.D. thesis, Caltech, California, 1997; e-print quant-ph/9705052.
[13] R. Laflamme *et al.*, Phys. Rev. Lett. **77**, 198 (1996).
[14] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).