Quantum error correction with degenerate codes for correlated noise

Giulio Chiribella,[1] Michele Dall'Arno,[2,3] Giacomo Mauro D'Ariano,[2,3] Chiara Macchiavello,[2,3] and Paolo Perinotti[2,3]
[1]*Perimeter Institute for Theoretical Physics, 31 Caroline St. North, Waterloo, Ontario N2L 2Y5, Canada*
[2]*Quit group, Dipartimento di Fisica "A. Volta," via Bassi 6, I-27100 Pavia, Italy*
[3]*INFN Sezione di Pavia, via Bassi 6, I-27100 Pavia, Italy*

(Received 21 July 2010; revised manuscript received 13 October 2010; published 9 May 2011)

We introduce a quantum packing bound on the minimal resources required by nondegenerate error-correction codes for any kind of noise. We prove that degenerate codes can outperform nondegenerate ones in the presence of correlated noise, by exhibiting examples where the quantum packing bound is violated.

DOI: 10.1103/PhysRevA.83.052305 PACS number(s): 03.67.Pp

I. INTRODUCTION

Since its early development in 1995 [1–7], the theory of quantum error correction has played a major role in design strategies for protecting quantum information in the presence of noise. This task is particularly relevant in several contexts, such as the communication of quantum information over quantum channels [8] and fault tolerant quantum computation [9]. In view of the massive experimental effort in investigating suitable quantum computational systems and of future implementations, it is of great importance to establish what are the minimum resources needed to have successful quantum error correction.

A useful bound that allows us to quantify them is the quantum Hamming bound [10] for nondegenerate codes, namely, codes for which each error is individually identifiable. This bound holds when the dominant terms in the noise process correspond to all the error operators that involve at most a fixed number of subsystems. This is the case, for example, when the noise affects independently every single subsystem (uncorrelated noise). Intuitively, the quantum Hamming bound can be explained from the fact that if each error is individually identifiable, then it must send the encoded information into orthogonal subspaces, thus setting a lower bound on the dimension of the system. Actually, so far no degenerate code has been proved to violate the quantum Hamming bound [11], and for some classes of degenerate codes, the impossibility of violating the bound has been demonstrated [12].

Here, we derive a general bound that we call a quantum packing bound, constraining the resource requirements for the correction of any kind of noise process. In particular, the quantum Hamming bound is an instance of the quantum packing bound for the case of an arbitrary noise process affecting at most a fixed number of systems.

The assumption of uncorrelated noise may not hold in many physical implementations of fault tolerant quantum computers, such as ion traps [13], quantum dots [14], or solid-state systems [15]. In this work, we study the resource requirements of error correction codes in the presence of correlated noise, namely, noise processes where perfect correlations among the encoding subsystems dominate, and, therefore, not all the strings of single-particle noisy processes are relevant. We show that degenerate codes can outperform nondegenerate ones in the presence of correlated noise. The resource requirements of quantum error-correction codes for a particular class of correlated errors, namely, spatially correlated (or burst) errors, have been studied in [16].

The paper is organized as follows. In Sec. II, we provide the quantum packing bound on the minimal resources required by a nondegenerate code in the presence of any kind of noise. We refer to such a bound as a quantum packing bound. We prove that the quantum Hamming bound can be recovered as a particular case. In Sec. III, we show that in the presence of correlated noise, the quantum packing bound can be violated by degenerate codes, which lead to a much more compact transmission of information, unveiling the fact that, for some noise channels, degenerate codes can work better than nondegenerate codes in terms of the resources required. Finally, we summarize our results in Sec. IV.

II. QUANTUM PACKING BOUND

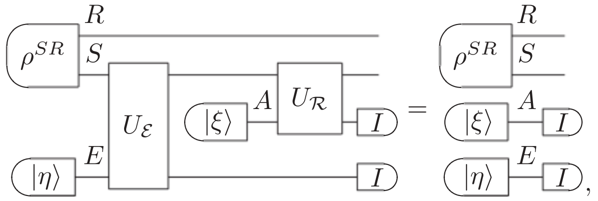
An $[[n,k,d]]_q$ quantum error-correction code is given by a q^k-dimensional subspace of the state space $\mathscr{H} = (\mathbb{C}^q)^{\otimes n}$ of n quantum systems with q levels where it is possible to correct all errors affecting at most $(d-1)/2$ quantum systems. We denote by P_Q the projector onto the quantum code Q. Let S_E denote a subspace of linear operators on $\mathscr{H}$. The quantum code Q is able to correct all errors in S_E if and only if there exists a Hermitian matrix M such that for any pair of error operators L_i, L_j which belong to a basis on S_E [17],

$$P_Q L_i^\dagger L_j P_Q = M_{ij} P_Q. \tag{1}$$

In the above expression, known as the Knill-Laflamme correctability condition, M_{ij} are the entries of the Hermitian matrix M, that depends on the choice of the L_i's. The pair (Q,S_E), consisting of a quantum code Q and a vector space of errors S_E, is called *degenerate* if and only if the Hermitian matrix M in Eq. (1) is singular; otherwise, (Q,S_E) is called *nondegenerate*. In other words, in the case of nondegenerate codes and with a suitable choice of error operators, the quantum code is transformed into a set of distinct orthogonal subspaces by applying the error operators, while for degenerate codes it may happen that distinct error operators transform the code into the same subspace.

We derive now a bound for nondegenerate codes, which does not depend on the form of the noise acting on the encoding system, and which can be reduced to the well-known quantum Hamming bound [10] as a particular case. To this purpose, we first give a brief overview on a few results about error correction. Let us denote the *system* by S and the *encoding subspace* by $Q \subseteq S$. Given a state ρ^S, we say that a channel $\mathcal{E}$ is *correctable upon input of* ρ^S if and only if there exists a channel $\mathcal{R}$ such that $\mathcal{R}\mathcal{E}(\sigma) = \sigma$ for every σ with $\mathrm{supp}(\sigma) \subseteq \mathrm{supp}(\rho^S)$. Clearly, if $\mathrm{supp}(\rho^S) = Q$, this is equivalent to saying that Q is a good quantum code.

Let us introduce a purification ρ^{SR} of ρ^S, R being the *reference*. It is easy to see that for arbitrary channels $\mathcal{C}$ and $\mathcal{D}$, we have $\mathcal{I}_R \otimes \mathcal{C}(\rho^{SR}) = \mathcal{I}_R \otimes \mathcal{D}(\rho^{SR})$ if and only if $\mathcal{C}(\sigma) = \mathcal{D}(\sigma)$ for any σ with $\mathrm{supp}(\sigma) \subseteq \mathrm{supp}(\rho^S)$. This fact implies that $\mathcal{E}$ is correctable upon input of ρ if and only if we have $\mathcal{I}_R \otimes \mathcal{R}\mathcal{E}(\rho^{SR}) = \rho^{SR}$. Taking a unitary dilation $(U_{\mathcal{E}}, |\eta\rangle)$ $[(U_{\mathcal{R}}, |\xi\rangle)]$ of channel $\mathcal{E}$ $(\mathcal{R})$ with *environment* E (A), this is equivalent to the following equation:



(2)

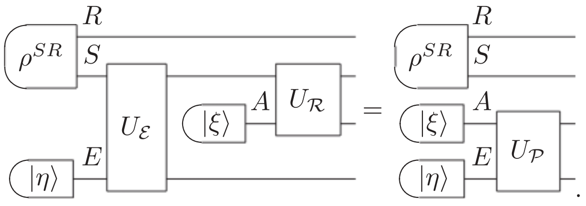
where represents the partial trace. Consider the circuit on the left-hand side. Denote by $\rho^{S'R'E'}$, the state of S, R, and E after the action of $U_{\mathcal{E}}$, and by $\rho^{S'R'}$ $(\rho^{R'E'})$, its marginal on SR (RE). Since $\rho^{S'R'E'}$ is a purification for $\rho^{R'E'}$, we have

$$\dim(S) \geqslant \mathrm{rank}(\rho^{R'E'}). \tag{3}$$

We now give two other necessary and sufficient conditions for correctability, which imply the quantum packing bound.

Proposition 1. A channel $\mathcal{E}$ is correctable upon input of ρ^S if and only if the reference R and the environment E are uncorrelated after the interaction, i.e., $\rho^{R'E'} = \rho^{R'} \otimes \rho^{E'}$ (see, e.g., [18,19]).

Proof. We repeat here only the proof of necessity, since it is the only part needed. Calling $\rho^{S''R''E''A''}$ the state of $SREA$ after the action of $U_{\mathcal{E}}$ and $U_{\mathcal{R}}$, Eq. (2) is nothing but the statement that $\rho^{S''R''E''A''}$ and $\rho^{SR} \otimes \eta^E \otimes \xi^F$ are both purifications of ρ^{RS}. Therefore, there exists a unitary $U_{\mathcal{P}}$ such that



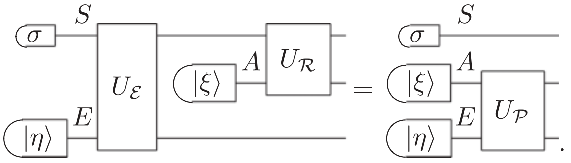
(4)

Discarding systems S and A on both sides, one then obtains $\rho^{R'E'} = \rho^{R'} \otimes \rho^{E'}$. ■

The second necessary and sufficient condition is

Proposition 2. A channel $\mathcal{E}$ is correctable upon input of ρ^S if and only if its complementary channel $\tilde{\mathcal{E}}$—namely the channel from S to E' obtained by tracing S' instead of E'—is a deletion channel upon input of ρ^S, i.e., $\tilde{\mathcal{E}}(\sigma) = \rho^{E'}$ for every σ with $\mathrm{supp}(\sigma) \subseteq \mathrm{supp}(\rho^S)$ [20] (see also [18] for a graphical proof).

Proof. We reproduce here only the proof of necessity, because it is the only part needed for our considerations. Equation (4) implies that for every σ with $\mathrm{supp}(\sigma) \subseteq \mathrm{supp}(\rho^S)$, we have



(5)

Taking the partial trace over S and A on both sides, we then obtain $\tilde{\mathcal{E}}(\sigma) = \rho^{E'}$, thus proving that $\tilde{\mathcal{E}}$ is a deletion channel. ■

The proofs of Propositions 1 and 2 rely only upon the very general requirement that any mixed state admits a unique purification up to reversible transformations, thus holding for any probabilistic theory with a purification [18].

Restricting now Propositions 1 and 2 to the quantum case, we derive the following bounds. Using Proposition (1), Eq. (3) becomes

$$\dim(S) \geqslant \mathrm{rank}(\rho^{R'})\mathrm{rank}(\rho^{E'}) = \mathrm{rank}(\rho^S)\mathrm{rank}(\rho^{E'}), \tag{6}$$

where the last equality holds since $\mathcal{E}$ does not act on R, and R purifies ρ^S, so $\mathrm{rank}(\rho^{R'}) = \mathrm{rank}(\rho^R) = \mathrm{rank}(\rho^S)$. Proposition 2 allows us to identify the matrix M in the Knill-Laflamme condition [Eq. (1)] with (the transpose of) $\rho^{E'}$. Indeed, for every (unnormalized) state of the form $P_Q\rho P_Q$, the complementary channel $\tilde{\mathcal{E}}$ acts as

$$\begin{aligned}\tilde{\mathcal{E}}(P_Q\rho P_Q) &= \mathrm{Tr}_S[U_{\mathcal{E}}(P_Q\rho P_Q \otimes |\eta\rangle\langle\eta|)U_{\mathcal{E}}^\dagger]\\ &= \mathrm{Tr}[P_Q\rho P_Q]\rho^{E'}.\end{aligned} \tag{7}$$

If $\mathcal{E}$ has the Kraus decomposition $\mathcal{E}(\rho) = \sum_i L_i\rho L_i^\dagger$ and $U_{\mathcal{E}}|\eta\rangle = \sum_i L_i \otimes |e_i\rangle$, where $|e_i\rangle$ is an orthonormal set in E, then Eq. (7) becomes

$$\mathrm{Tr}_S[L_iP_Q\rho P_Q L_j^\dagger] = \mathrm{Tr}[P_Q\rho P_Q]\rho_{ij}^{E'}. \tag{8}$$

Taking $\rho = |\psi\rangle\langle\psi|$ with an arbitrary $|\psi\rangle \in \mathscr{H}$, Eq. (8) becomes

$$\langle\psi|\, P_Q L_j^\dagger L_i P_Q\,|\psi\rangle = \langle\psi|\, P_Q\,|\psi\rangle\, \rho_{ij}^{E'}, \tag{9}$$

which is equivalent to the Knill-Laflamme condition [Eq. (1)] with $\rho^{E'} = M^T$. Summarizing, we proved the following result,

$$\dim(S) \geqslant \mathrm{rank}(\rho^S)\mathrm{rank}(M), \tag{10}$$

or, equivalently,

$$\dim(S) \geqslant \dim(Q)\mathrm{rank}(M). \tag{11}$$

Notice that $\mathrm{rank}(M)$ does not depend on the choice of Kraus operators $\{L_i\}$. In particular, to compute $\mathrm{rank}(M)$, we can use a minimal Kraus decomposition $\mathcal{E}(\rho) = \sum_{i=1}^{\mathrm{rank}(R_{\mathcal{E}})} K_i\rho K_i^\dagger$, whose cardinality is equal to the rank of the Choi-Jamiołkowski operator $R_{\mathcal{E}} = (\mathcal{E} \otimes \mathcal{I})(|I\rangle\rangle\langle\langle I|)$, obtained by applying the channel $\mathcal{E}$ on one side of the maximally entangled vector $|I\rangle\rangle = \sum_{n=1}^d |n\rangle|n\rangle$.

We now consider the case of nondegenerate codes, i.e., codes for which the matrix M is nonsingular. In this case, $\mathrm{rank}(M)$ equals $\mathrm{rank}(R_{\mathcal{E}})$, namely, the cardinality of the minimal Kraus $\{K_i\}$.

Proposition 3 (Quantum Packing Bound). Given a quantum channel $\mathcal{E}$ with the Choi-Jamiołkowski operator $R_{\mathcal{E}}$, any nondegenerate code Q subspace of the system S must satisfy

$$\dim(S) \geqslant \dim(Q)\text{rank}(R_{\mathcal{E}}). \tag{12}$$

We refer to Eq. (12) as a quantum packing bound.

Proof. The thesis follows immediately from Propositions 1 and 2, along with the considerations above.

Here, we provide an alternative short proof that makes use of more technicalities. Diagonalize the matrix M in Eq. (1) to obtain a diagonal matrix D and a new error basis J_i. The correctability condition in Eq. (1) then becomes

$$P_Q J_i^\dagger J_j P_Q = D_{ij} P_Q. \tag{13}$$

Make use of the polar decomposition and of the correctability condition in Eq. (13) to obtain

$$J_i P_Q = U_i \sqrt{P J_i^\dagger J_i P_q} = \sqrt{D_{ii}} U_i P_Q, \tag{14}$$

where U is some unitary matrix. Thus, the action of the error J_i is to rotate Q into the subspace defined by the projector$P_i := U_i P U_i^\dagger = J_i P U_i^\dagger / \sqrt{D_{ii}}$. Since such subspaces are orthogonal by Eq. (13) and are in number of $\text{rank}(D) = \text{rank}(M)$, Eq. (11) follows. Finally, using the nondegeneracy hypothesis, $\text{rank}(M) = \text{rank}(R_{\mathcal{E}})$, the statement follows. ■

Notice that in Eq. (12), only the rank of the Choi-Jamiołkowski operator describing the noise is involved, but no assumption on the form of the noise process affecting the encoding system has been formulated. The quantum Hamming bound [10], which holds for noise acting independently on the encoding systems, can be derived from Eq. (12) as a particular case. Actually, if we look at the case of qubits and wish to correct noise affecting at most t qubits, we consider a basis of error operators given by products of Pauli matrices involving up to t qubits. Then, correcting all errors is equivalent to correcting the random-unitary channel $\mathcal{E}$ whose Kraus operators are proportional to the possible products of $i \leqslant t$ Pauli matrices [21]. Since Pauli matrices are orthogonal, this Kraus representation is already minimal, whence $\text{rank}(R_{\mathcal{E}})$ can be straightforwardly derived counting the number of independent Kraus operators [the ones affecting i qubits are $3^i \binom{n}{i}$], and this leads to

$$2^n \geqslant 2^k \sum_{i=0}^{t} 3^i \binom{n}{i}. \tag{15}$$

The above formula can be straightforwardly generalized to q-dimensional systems by replacing powers of 2 with powers of q, and 3 with $q^2 - 1$.

III. DEGENERATE CODES FOR CORRELATED NOISE

We will now consider the case where noise is correlated, i.e., it does not act independently on the encoding systems and cannot be expressed as $\mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \cdots \otimes \mathcal{E}_n$, where $\mathcal{E}_i$ represent the noise process acting on the ith system in the encoding space. We will consider in the following the case of qubits with Pauli correlated noise, i.e., correlated channels in which each Kraus operator is the product of Pauli matrices [22].

As a first example, consider the following completely positive (CP) map

$$\mathcal{E}(\rho) = p\rho + \sum_{i=1\ldots n, j>i} (p_{X,ij} X_i X_j \rho X_j X_i + p_{Y,ij} Y_i Y_j \rho Y_j Y_i + p_{Z,ij} Z_i Z_j \rho Z_j Z_i), \tag{16}$$

where with probability $p = 1 - \sum_{i=1\ldots n, j>i} p_{X,ij} + p_{Y,ij} + p_{Z,ij}$, the input state is left unchanged, while with probabilities $p_{X,ij}$, $p_{Y,ij}$, and $p_{Z,ij}$, pairwise Pauli operators X, Y, and Z are applied to qubits i and j, respectively. By evaluating the rank of the above CP map, the quantum packing bound (12) in this case takes the simple form

$$2^n \geqslant 2^k \left[1 + 3\binom{n}{2}\right]. \tag{17}$$

Let us consider the simple case $k = 1$: the smallest integer that satisfies the above bound is $n = 7$. Nevertheless, we can easily construct error-correction codes with lower values for n. Consider the quantum code spanned by

$$|\bar{0}\rangle = |000\rangle \quad |\bar{1}\rangle = |111\rangle\,. \tag{18}$$

Notice that the above states are also the code words that saturate the Hamming bound for the classical error on at most one qubit ($t = 1$) [10]. Our error correcting strategy works as follows: we encode logical $|0\rangle$ into $|\bar{0}\rangle$ and logical $|1\rangle$ into $|\bar{1}\rangle$. As mentioned above, this kind of noise either leaves the qubits unchanged, or acts on two of them with the same Pauli operator. Notice that the two code words are not changed by the application of the Z matrix on any pair of qubits. As a consequence of this, the application of pairwise Y operators gives the same result as the application of pairwise X operators, namely, the code is thus degenerate. Therefore, we have only to correct errors due to the action of the X operators. To achieve this, we perform a projective measurement on the bidimensional subspaces $S_{00} = \text{span}\{|000\rangle, |111\rangle\}$, $S_{01} = \text{span}\{|100\rangle, |011\rangle\}$, $S_{10} = \text{span}\{|010\rangle, |101\rangle\}$, and $S_{11} = \text{span}\{|001\rangle, |110\rangle\}$. If the outcome of the measurement is 00, noise has not affected any qubit; if the result is 01, noise has affected qubits 2 and 3; if the result is 10, noise has affected qubits 1 and 3; and if the result is 11, noise has affected qubits 1 and 2. In these last three situations, acting with X on the corresponding pair of qubits gives the original qubits. As we can see, this code exploits the invariance of the coding subspace under the action of two Z operators to allow for perfect error correction while strongly violating the quantum packing bound.

The above error correcting strategy can be also successfully applied to a generalization of the correlated noise [Eq. (16)], where we can add additional terms involving products of an even number of Pauli operators along the same direction. For example, it is possible to correct in the same way errors acting also on four qubits. In this case, the choice of the code words is

$$|\bar{0}\rangle = |00000\rangle \quad |\bar{1}\rangle = |11111\rangle\,, \tag{19}$$

and the error correction is performed in a way similar to the previous one. As before, this code is highly degenerate because it is invariant under the application of the product of an even number of Z Pauli operators. The error syndrome is discovered by performing a projective measurement on the subspaces span$\{|00000\rangle, |11111\rangle\}$ corresponding to no errors, span$\{|11000\rangle, |00111\rangle\}$ and all possible permutations corresponding to two qubits error, and span$\{|11110\rangle, |00001\rangle\}$ and all possible permutations corresponding to four qubits error. Then, an error correction is performed in a similar way to the case discussed before.

In this way we have constructed a degenerate quantum code which violates the corresponding quantum packing bound for nondegenerate codes

$$2^n \geqslant 2^k \left[1 + 3\binom{n}{2} + 3\binom{n}{4}\right], \tag{20}$$

which would require for $k = 1$, a minimum $n = 14$. By generalizing this procedure, we can efficiently correct noise acting on every even number of qubits. In fact, the strategy we have provided allows one to correct correlated errors acting on $2,4,6,\ldots,2m$ qubits coding on $n = 2m + 1$ qubits. The two coding states are then given by

$$|\bar{0}\rangle = |0\rangle^{\otimes 2m+1} \qquad |\bar{1}\rangle = |1\rangle^{\otimes 2m+1}. \tag{21}$$

In this case, the quantum packing bound becomes

$$2^n \geqslant 2^k \sum_{i=0}^{m} 3\binom{n}{2i}. \tag{22}$$

We emphasize that the possibility of achieving such compact quantum codes for correlated noise of the form studied here is related to the fact that we consider error operators acting on an even number of qubits. We now consider the problem of correcting correlated noise on three qubits. The noisy channel is then of the form

$$\mathcal{E}(\rho) = p\rho + \sum_{i=1\ldots n, j>i, k>j} p_{X,ijk} X_i X_j X_k \rho X_k X_j X_i + p_{Y,ijk} Y_i Y_j Y_k \rho Y_k Y_j Y_i + p_{Z,ijk} Z_i Z_j Z_k \rho Z_k Z_j Z_i. \tag{23}$$

The smallest number of physical qubits we can employ for such a channel is $n = 3$, which corresponds to a nondegenerate code which saturates the corresponding quantum packing bound $2^n \geqslant 2^k[1 + 3\binom{n}{3}]$. Actually, it is possible to encode one logical qubit on $n = 3$ physical ones by employing the additional two qubits as an ancilla initially fixed in the state $|a\rangle\rangle = |0\rangle|+\rangle$, where $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$. After the action of noise, the two ancilla qubits are measured in the computational basis and in the $|+\rangle$, $|-\rangle$ basis, respectively. From the result of this measurement, we learn exactly which of the four Kraus operators has acted on the qubits because the operators XX, YY, and ZZ applied to the above state $|a\rangle\rangle = |0\rangle|+\rangle$ transform it to the mutually orthogonal states $|1\rangle|+\rangle$, $|1\rangle|-\rangle$, and $|0\rangle|-\rangle$, respectively. In order to correct the errors, after learning the result of the measurement, we either do nothing, or we apply one of the three Pauli operators on the first qubit to recover the noiseless state. This strategy, in contrast to what happens in quantum codes for independent noise, does not involve multipartite entanglement in the encoding systems as the three qubits in the encoded state are always factorized. In this case, there seems to be an intriguing balance between the correlations of the noise and the entanglement in the encoding system: if the noise is fully correlated on the three qubits, then no entanglement is needed for encoding, while if the noise is independent, then encoding is performed on multipartite entangled states.

The above procedure can be employed to correct correlated noise of the form [Eq. (23)] acting on an arbitrary number n of qubits by encoding $k = n - 2$ qubits. As before, the k-qubit state to be protected is encoded, appending to it the two ancilla qubits in state $|0\rangle|+\rangle$. After the receipt of the encoded state, the previously described measurement of the ancilla will give the syndrome and the necessary operations to be performed on the rest of the qubits to rescue the original state. In this case, we again construct nondegenerate codes that saturate the corresponding quantum packing bound.

IV. CONCLUSION

In this paper, we provided a quantum packing bound for nondegenerate codes. The bound holds for any kind of noise and depends on the rank of the Choi-Jamiołkowski operator representing the noise process. The quantum Hamming bound is then recovered in the particular case of arbitrary noise acting independently on a fixed number of encoding systems. While the quantum Hamming bound has not been violated so far, in the case of correlated noise, we have shown how to exploit degeneracy to violate the quantum packing bound and achieve perfect quantum error correction with fewer resources than those needed for nondegenerate codes.

ACKNOWLEDGMENTS

This work was supported by Italian Ministry of Education through PRIN 2008 and by the European Community through COQUIT and CORNER projects. Research at Perimeter Institute for Theoretical Physics is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MRI.

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

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

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

[4] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[5] M. Keyl and R. F. Werner, Lect. Notes Phys. **611**, 263 (2002).

[6] M. Gregoratti and R. F. Werner, J. Mod. Opt. **50**, 915 (2003).

[7] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).

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

[9] D. Aharonov, A. Kitaev, and J. Preskill, Phys. Rev. Lett. **96**, 050504 (2006).

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

[11] D. Gottesman, e-print arXiv:0904.2557v1.

[12] P. Sarvepalli and A. Klappenecker, Phys. Rev. A **81**, 032318 (2010).

[13] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); A. Garg, *ibid*. **77**, 964 (1996).

[14] D. Loss and D. P. Di Vincenzo, Phys. Rev. A **57**, 120 (1998); M. Thorwart, J. Eckel, and E. R. Mucciolo, Phys. Rev. B **72**, 235320 (2005).

[15] Y. Makhlin, G. Schön, and A. Shnirman, Rev. Mod. Phys. **73**, 357 (2001); A. Schnirman, Y. Makhlin, and G. Schön, Phys. Scr. T **102**, 147 (2002).

[16] F. Vatan, V. P. Roychowdhury, and M. P. Anantram, IEEE Trans. Inf. Theory **45**, 1703 (1999).

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

[18] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **81**, 062348 (2010).

[19] B. Schumacher and M. D. Westmoreland, J. Quantum Inf. Proc. **1**, 5 (2002).

[20] D. Kretschmann, D. W. Kribs, and R. W. Spekkens, Phys. Rev. A **78**, 032330 (2008).

[21] Clearly, if there is a channel $\mathcal{R}$ that corrects all such Pauli errors, then $\mathcal{R}$ also corrects their randomization $\mathcal{E}$. The converse follows from the fact that if $\mathcal{R}$ corrects $\mathcal{E}$ and $\mathcal{E} = \sum_i \mathcal{E}_i$, where $\mathcal{E}_i$ are arbitrary quantum operations, then necessarily $\mathcal{R}$ corrects $\mathcal{E}_i$, that is, $\mathcal{R}\mathcal{E}_i(\sigma) = p_i\sigma$ for every σ such that $\mathrm{supp}(\sigma) \subseteq Q$.

[22] C. Macchiavello and G. M. Palma, Phys. Rev. A **65**, 050301 (2002).