Algebraic and information-theoretic conditions for operator quantum error correction

Michael A. Nielsen and David Poulin
School of Physical Sciences, The University of Queensland, Queensland 4072, Australia
(Received 14 February 2007; published 21 June 2007)

Operator quantum error correction is a technique for robustly storing quantum information in the presence of noise. It generalizes the standard theory of quantum error correction, and provides a unified framework for topics such as quantum error correction, decoherence-free subspaces, and noiseless subsystems. This paper develops (a) easily applied algebraic and information-theoretic conditions that characterize when operator quantum error correction is feasible; (b) a representation theorem for a class of noise processes that can be corrected using operator quantum error correction; and (c) generalizations of the coherent information and quantum data processing inequality to the setting of operator quantum error correction.

DOI: 10.1103/PhysRevA.75.064304 PACS number(s): 03.67.Lx

To develop quantum technologies such as quantum computers and quantum communication networks, it will be necessary to protect quantum systems against the effects of noise. Considerable progress toward this goal was made in the late 1990s, when a theory of fault-tolerant quantum computing was developed [1–5], based on the theory of quantum error-correcting codes [6–10].

The early theory of quantum error-correcting codes was based on the following ideas. (1) Quantum information is stored in a subspace A of a larger state space $V=A\oplus C$. A is known as the *code space*, while V is the state space of the physical system being used to store the information. (2) Some physically motivated noise process corrupts the physical system. (3) A recovery step is performed, restoring the original quantum information stored in A.

Since its development this theory has been refined and generalized in a variety of ways, notably through the introduction of decoherence-free subspaces [11–14], noiseless subsystems [15–17], and operator quantum error correction. In particular, the framework of *operator quantum error correction* [18,19] provides a single framework integrating and unifying all of these techniques.

Operator quantum error correction is based on the following ideas: (1) quantum information is stored in a space A which appears as a tensor factor in a subspace of the overall state space, V, i.e., $V=(A\otimes B)\oplus C$; (2) some physically motivated noise process $\mathcal{E}$ corrupts the physical system; (3) a recovery step is performed, restoring the original encoded quantum information stored in A. The subsystem A is said to be $\mathcal{E}$ correctable.

Operator quantum error correction is a generalization of standard quantum error correction. Kribs *et al.* [18,19] have shown that operator quantum error correction provides a natural framework unifying and generalizing earlier approaches, including standard quantum error correction, decoherence-free subspaces, and noiseless subsystems. Bacon [20] has recently exhibited interesting examples in which operator quantum error correction plays a critical role. A stabilizer formalism for operator quantum error correction was presented in [21].

The purpose of this paper is to develop necessary and sufficient conditions for operator quantum error correction. In particular, we obtain a set of algebraic conditions characterizing operator quantum error correction. These conditions generalize the well-known conditions for standard quantum error correction [8,22], which are one basis for the theory of quantum error-correcting codes, enabling the construction of large classes of codes [9,23]. The necessity of these conditions for operator quantum error correction was proved in [18], but the proof of sufficiency was left open. We establish the sufficiency of these conditions, and use the conditions to establish a representation theorem for a class of noise processes which can be corrected using operator quantum error correction.

We also prove a set of information-theoretic conditions characterizing operator quantum error correction, based on generalizations of the coherent information and the quantum data processing inequality. In the context of quantum error-correction codes these concepts were developed in [24], and were critical in developing the theory of quantum channel capacity [24–30].

Definition of operator quantum error correction. Suppose V is the Hilbert space for some quantum system, and we decompose $V=(A\otimes B)\oplus C$ for some choice of A, B, and C. Suppose $\mathcal{E}$ is a quantum operation acting on V. Then we say A is an $\mathcal{E}$-correcting subsystem with respect to the decomposition $V=(A\otimes B)\oplus C$ if there exists a trace-preserving quantum operation $\mathcal{R}$ (the recovery operation) such that for all ρ with support on A, and all σ with support on B, we have $(\mathcal{R}\circ\mathcal{E})(\rho\otimes\sigma)\propto\rho\otimes\sigma'$, for some σ' with support on B. This procedure is named operator quantum error correction. Physically, this means that we can store information in the subsystem A, and recover the information after noise $\mathcal{E}$ by applying the recovery operation $\mathcal{R}$. Quantum error-correcting codes arise as the special case of this definition where B is trivial (i.e., one dimensional), which is equivalent to decomposing $V=A\oplus C$. That is, in an error-correcting code we encode information in a *subspace*, while in an operator error-correcting code we may encode information in a *subsystem* of a subspace.

Algebraic characterization of operator quantum error correction. Remember that a quantum operation $\mathcal{E}$ can be expressed in an operator-sum representation $\mathcal{E}(\rho)=\Sigma_j E_j\rho E_j^\dagger$, where the (nonunique) E_j's are called operation elements. Suppose that the noise $\mathcal{E}$ has operation elements E_j. We will prove that the following two conditions are equivalent.

(a) A is an $\mathcal{E}$-correcting subsystem with respect to the decomposition $V=(A\otimes B)\oplus C$.

(b) $PE_j^\dagger E_k P = I_A \otimes B_{jk}$ for all j and k, where P projects onto $A\otimes B$, and the B_{jk} are operators on B.

Condition (b) provides a checkable set of necessary and sufficient conditions for operator quantum error correction, generalizing the standard quantum error-correction conditions [8,22]. As in standard quantum error correction, the correctability of a map with operation elements $\{E_j\}$ implies the correctability of any map whose operations elements $\{F_i\}$ are linear combinations of the E_j. A straightforward calculation shows that if condition (b) holds for E_j, it also holds for any $F_i=\Sigma_j \alpha_{ij} E_j$. Physically, this follows from the linearity of quantum mechanics and the possibility of expressing any noise operation as a unitary transformation acting on the system of interest and the environment.

Proof that (a) implies (b). This was proved in [18], and is a straightforward generalization of the corresponding part of the proof of the quantum error-correction conditions as given in, e.g., Chap. 10 of [31]. One of the ideas used in the proof is used again later, so for completeness we give a brief outline. Suppose the recovery operation $\mathcal{R}$ has operation elements R_j. Define an operation $\mathcal{P}(\rho)\equiv P\rho P$. Then it can be shown that $\mathcal{R}\circ\mathcal{E}\circ\mathcal{P}=\mathcal{I}_A\otimes\mathcal{N}$ for some operation $\mathcal{N}$ on system B. Standard results (see, e.g., Chap. 9 of [31]) about the unitary freedom in operation elements imply that $R_j E_k P = I \otimes N_{jk}$ for some set of operators N_{jk} acting on system B. Multiplying this equation by its adjoint, for a suitable choice of indices we obtain $PE_l^\dagger R_j^\dagger R_j E_k P = I\otimes N_{jl}^\dagger N_{jk}$. Summing over j and using the fact that $\mathcal{R}$ is trace preserving (i.e., $\Sigma_j R_j^\dagger R_j = I$) gives the result. ■

We will give two proofs that (b) implies (a). The first proof is deeper, and is based on a third equivalent condition (c); we prove (b)⇒(c)⇒(a). (c) has many rich consequences, including the information-theoretic characterization of operator error correction described later, and a representation theorem (described below) for correctable $\mathcal{E}$ in the special case when $V=A\otimes B$. Our second proof that (b) implies (a) is a more straightforward extension of the standard quantum error-correction conditions. This proof is arguably simpler than the first, but does not appear to have the same rich consequences, and so we merely provide a sketch.

To state condition (c) involves a somewhat elaborate construction involving auxiliary systems, inspired by [24]. We introduce systems R_A and R_B whose Hilbert spaces are copies of A and B, respectively. We define (unnormalized) maximally entangled states $|\alpha\rangle\equiv\Sigma_j|j\rangle|j\rangle$ of $R_A A$ and $|\beta\rangle\equiv\Sigma_k|k\rangle|k\rangle$ of $R_B B$. The state $|\alpha\rangle|\beta\rangle$ may be regarded as a joint state of $R_A R_B V$ in a natural way.

Next, we introduce a system E which will act as a model environment for the operation $\mathcal{E}$. We suppose E has an orthonormal basis $|j\rangle$ whose elements are in one-to-one correspondence with the operation elements E_j. Supposing $|s\rangle$ is some fixed initial state of E, we define a linear operation L on VE which has the action $L|\psi\rangle|s\rangle\equiv\Sigma_j E_j|\psi\rangle|j\rangle$. Note that the effect of L on VE, after tracing out, is equivalent to the action of $\mathcal{E}$ on V.

Define a state $|\psi'\rangle\equiv(I_{R_A R_B}\otimes L)|\alpha\rangle|\beta\rangle|s\rangle$. $|\psi'\rangle$ can be thought of as the combined state of $R_A R_B VE$ after the noise is applied. We define a corresponding density matrix $\rho'\equiv|\psi'\rangle\langle\psi'|$, and use notations like $\rho'_{R_B E}$ to denote the result when all systems but R_B and E are traced out. With these definitions we may state condition (c).

(c) $\rho'_{R_A R_B E}=\rho'_{R_A}\otimes\rho'_{R_B E}$.

Proof that (b) implies (c). The definition of ρ' and a direct calculation show that

$$\rho'_{R_A R_B E}=\sum_{jk} PE_j^T E_k^* P\otimes|j\rangle\langle k|, \tag{1}$$

where $PE_j^T E_k^* P$ is understood as an operator on $R_A R_B$. To do this we identify the bases $|j\rangle_{R_A}$ and $|j\rangle_A$, and take the complex conjugate and transpose with respect to this basis. Taking the complex conjugate of (b) and substituting gives the desired result. [The converse, that (c) implies (b), also follows directly from Eq. (1), although we will not need this implication.] ■

Proof that (c) implies (a). (cf. [24].) We Schmidt decompose $|\psi'\rangle$ with respect to the bipartite decomposition $R_A R_B E:V$. Making use of the fact that the Schmidt vectors of $R_A R_B E$ are eigenvectors of $\rho'_{R_A R_B E}=\rho'_{R_A}\otimes\rho'_{R_B E}$, this gives rise to the Schmidt form (this and subsequent states are only written up to normalization)

$$|\psi'\rangle=\sum_{jk}\sqrt{q_k}|j\rangle_{R_A}|k\rangle_{R_B E}|e_{jk}\rangle_V, \tag{2}$$

where the $|j\rangle_{R_A}$ are orthonormal eigenvectors of ρ'_{R_A}, the $|k\rangle_{R_B E}$ and q_k are orthonormal eigenvectors and eigenvalues of $\rho'_{R_B E}$, and the $|e_{jk}\rangle_V$ are orthonormal Schmidt vectors on V.

Define an orthonormal set of projectors $P_k\equiv\Sigma_j|e_{jk}\rangle_V\langle e_{jk}|$ acting on V. We define the first step of recovery $\mathcal{R}$ to be performing a measurement of P_k, resulting in the state

$$|\psi_k'\rangle=\sum_j|j\rangle_{R_A}|k\rangle_{R_B E}|e_{jk}\rangle_V. \tag{3}$$

The second and final step of recovery is to apply a unitary U_k which takes $|e_{jk}\rangle_V$ to $|j\rangle_A|s\rangle_B$, where $|s\rangle_B$ is some standard state of B. The net effect of the recovery procedure is to produce the following state of $R_A R_B VE$:

$$|\psi_k''\rangle=\sum_j|j\rangle_{R_A}|j\rangle_A|s\rangle_B|k\rangle_{R_B E}. \tag{4}$$

Thus, we have restored the initial maximal entanglement between R_A and A.

Summarizing, we have shown that if $R_A A$ and $R_B B$ each start out maximally entangled, and we apply the noise $\mathcal{E}$ followed by the recovery $\mathcal{R}$ to V, then the resulting state of $R_A A$ is the original maximally entangled state. Standard techniques (e.g., [25]) imply that we must have $(\mathcal{R}\circ\mathcal{E})(\rho\otimes\sigma)=\rho\otimes\sigma'$ for all ρ on system A and all σ on system B. ■

In the above proof that (c) implies (a), we have constructed a particular recovery procedure $\mathcal{R}$ that satisfies the condition, and has the particularity of resetting the B subsystem to a pure state. In this sense, it operates as a quantum error-correction code (see Remark 3.8 in [19]). However, this procedure is not unique. In particular, any other transformation $\mathcal{R}'$ that differs from $\mathcal{R}$ by an extra transformation on the

B subsystem—i.e., $\mathcal{R}'=\mathcal{R}\circ(\mathrm{id}_A\otimes\mathcal{F}_B)$ where id_A denotes the identity map on A and $\mathcal{F}_B$ is an arbitrary map on B—will also restore the information in A. The existence of several distinct recovery procedures is the main advantage of operator quantum error correction and may prove useful in fault-tolerant constructions (see [20,21]).

Representation theorem for correctable operations. When $V=A\otimes B$, i.e., when C is trivial, the proof that (c) implies (a) has as a consequence the representation $\mathcal{E}=\mathcal{U}\circ(\mathcal{I}_A\otimes\mathcal{N}_B)$ for some noisy operation $\mathcal{N}_B$ on B alone, and some unitary operation $\mathcal{U}$ on V.

To see this, note that when $V=A\otimes B$ the recovery procedure may be modified, omitting the step where P_k is measured, and instead simply applying a single unitary operation $W|e_{jk}\rangle_V\equiv|j\rangle_A|k\rangle_B$. If $\mathcal{W}$ is the quantum operation corresponding to W then we see that $\mathcal{W}\circ\mathcal{E}=\mathcal{I}_A\otimes\mathcal{N}_B$, so using $\mathcal{U}\equiv\mathcal{W}^\dagger$ gives the desired representation. ■

Alternate proof that (b) implies (a) (sketch). Fix a state $\sigma=|s\rangle\langle s|$ of B, and define a quantum operation $\mathcal{E}_s(\rho)\equiv\mathcal{E}(\rho\otimes\sigma)$ mapping states of A to states of V. We will use condition (b) to show that there exists a single universal recovery operation $\mathcal{R}$ which acts as a recovery operation for all $\mathcal{E}_s$. Linearity then implies that $(\mathcal{R}\circ\mathcal{E})(\rho\otimes\sigma)=\rho\otimes\sigma'$ for all ρ and σ.

To prove this, note that a set of operation elements for $\mathcal{E}_s$ is the set $E_{j,s}:A\to V$ defined by $E_{j,s}\equiv E_jP|s\rangle$. That is, $\mathcal{E}_s(\rho)=\sum_j E_{j,s}\rho E_{j,s}^\dagger$. (This can be verified by a calculation.) We will show that the set of errors $E_{j,s}$, where j and $|s\rangle$ are both allowed to vary over all possible values, is a correctable set of errors mapping A to V, in the sense of standard error correction. This suffices to establish the existence of a single universal recovery operation $\mathcal{R}$ which acts as a recovery operation for all $\mathcal{E}_s$. To see this, note that using (b) we obtain

$$I_AE_{j,s}^\dagger E_{k,t}I_A=\langle s|PE_j^\dagger E_kP|t\rangle=e_{jkst}I_A, \tag{5}$$

for complex numbers e_{jkst}. Thus the standard error-correction conditions apply, which suffices to establish the existence of a suitable recovery $\mathcal{R}$. ■

Information-theoretic characterization of correctability. For quantum error-correcting codes an information-theoretic necessary and sufficient condition for the correctability of trace-preserving $\mathcal{E}$ was found in [24], and subsequently generalized to non-trace-preserving $\mathcal{E}$ in [32]. We now find a set of information-theoretic necessary and sufficient conditions for operator quantum error correction, generalizing the earlier conditions, and actually simplifying those in [32].

Most of the work has already been done in arriving at condition (c), above. Suppose we normalize the state $|\psi'\rangle$ so ρ' and the corresponding reduced density matrices all have trace 1. The subadditivity inequality for entropy (see pp. 515 and 516 of [31]) implies that $S(\rho'_{R_AR_BE})\leq S(\rho'_{R_A})+S(\rho'_{R_BE})$, with equality if and only if $\rho'_{R_AR_BE}=\rho'_{R_A}\otimes\rho'_{R_BE}$. It follows that a necessary and sufficient condition for $\mathcal{E}$ to be correctable is that $S(\rho'_{R_A})+S(\rho'_{R_BE})=S(\rho'_{R_AR_BE})$. This may be rewritten in a more convenient form by noting that $S(\rho'_{R_A})=S(\rho_{R_A})=S(\rho_A)$, and that $S(\rho'_{R_AR_BE})=S(\rho'_V)$. This gives us the following necessary and sufficient condition for $\mathcal{E}$ to be correctable. [Note that in an obvious notation $S(\rho_A)=\log(d_A)$, where d_A is the dimension of system A, since A is initially maximally entangled with R_A.]

(d) $S(\rho_A)=S(\rho'_V)-S(\rho'_{R_BE})$.

The conditions (d) generalize the necessary and sufficient conditions in [24,32] (cf. [33,34]), which correspond to the case when B is trivial. Note that [24,32] allow A and R_A to start out in a state which is not maximally entangled, but rather are merely of full Schmidt rank. Our arguments are easily generalized to this case.

Data processing inequality. We have described the condition (d) as information theoretic, but have not suggested an information-theoretic interpretation of the quantities involved. Such an interpretation is suggested by the following argument, which generalizes the coherent information introduced in [24]. [24] showed that the coherent information satisfied a monotonicity property known as the quantum data processing inquality, which states that quantum information can only ever be lost as it is passed through multiple quantum channels; once lost, quantum information can never be recovered. The coherent information and quantum data processing inequality played a key role in subsequent investigations of the quantum channel capacity [24–30].

We now prove an analog of the quantum data processing inequality which applies to operator quantum error correction. Our analysis is based on the conditional entropy of R_A given V, $-S(R_A|V)\equiv S(\rho_V)-S(\rho_{R_AV})$, which generalizes the coherent information. The following argument suggests that this may be regarded as a measure of the amount of quantum information about the initial state of A which is still stored in V. Suppose we apply a sequence of trace-preserving quantum operations $\mathcal{E}_1,\mathcal{E}_2,\ldots$ to V. Standard monotonicity properties of the conditional entropy imply that

$$-S(R_A|V)\geq -S(R'_A|V')\geq -S(R''_A|V'')\geq\cdots, \tag{6}$$

where a single prime indicates that $\mathcal{E}_1$ has been applied, a double prime indicates that $\mathcal{E}_2\circ\mathcal{E}_1$ has been applied, and so on. Equation (6) is a generalization of the data processing inequality obtained in [24].

Condition (d) is equivalent to the condition $-S(R'_A|V')=-S(R_A|V)$, i.e., that the coherent information be preserved by the operation $\mathcal{E}$.

Indeed, a consequence of (6) is an informative alternative proof of the necessity of (d). Suppose $\mathcal{E}_1=\mathcal{E}$ and $\mathcal{E}_2=\mathcal{R}$. The fact that $\mathcal{R}$ restores the information stored in A implies that $-S(R_A|V)=-S(R''_A|V'')$. It follows from (6) that we must have $-S(R'_A|V')=-S(R_A|V)$, which implies (d).

Conclusion. Operator quantum error correction is a recently introduced technique for stabilizing quantum information, which generalizes and unifies previous approaches, including standard quantum error-correcting codes, decoherence-free subspaces, and noiseless subsystems. In this paper we have developed algebraic and information-theoretic necessary and sufficient conditions for operator quantum error correction, and used these conditions to develop an elegant representation theorem for a wide class of correctable noise processes, as well as generalizations of the coherent information and quantum data processing inequality. Open problems include the systematic investigation of specific operator quantum codes, and the investigation of techniques for fault-tolerant quantum-information processing using operator quantum codes.

The authors thank Dave Bacon, Steve Bartlett, Dominic Berry, Jennifer Dodd, and Andrew Doherty for helpful discussions and suggestions for improvement.

[1] P. W. Shor, in *Proceedings, 35th Annual Symposium on Fundamentals of Computer Science* (IEEE Press, Los Alamitos, CA, 1996), pp. 56–65.
[2] A. Y. Kitaev, in *Quantum Communication, Computing, and Measurement*, edited by A. S. H. O. Hirota and C. M. Caves (Plenum Press, New York, 1997), pp. 181–188.
[3] E. Knill, R. Laflamme, and W. H. Zurek, Proc. R. Soc. London, Ser. A **454**, 365 (1998).
[4] D. Aharonov and M. Ben-Or, in *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing* (ACM, New York, 1997), pp. 176.
[5] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 385 (1998).
[6] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[7] A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[8] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[9] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[10] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).
[11] L. M. Duan and G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).
[12] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[13] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[14] G. M. Palma, K.-A. Suominen, and A. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).
[15] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
[16] P. Zanardi, Phys. Rev. A **63**, 012301 (2001).
[17] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).
[18] D. W. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).
[19] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, Quantum Inf. Comput. **6**, 383 (2006).
[20] D. Bacon, Phys. Rev. A **73**, 012340 (2006).
[21] D. Poulin, Phys. Rev. Lett. **95**, 230504 (2005).
[22] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[23] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[24] B. W. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
[25] B. W. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[26] H. Barnum, M. A. Nielsen, and B. W. Schumacher, Phys. Rev. A **57**, 4153 (1998).
[27] H. Barnum, E. Knill, and M. A. Nielsen, IEEE Trans. Inf. Theory **46**, 1317 (2000).
[28] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[29] P. W. Shor, http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/ (unpublished).
[30] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[31] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).
[32] M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum, Proc. R. Soc. London, Ser. A **454**, 277 (1998).
[33] B. Schumacher and M. D. Westmoreland, J. Math. Phys. **43**, 4279 (2002).
[34] T. Ogawa, e-print arXiv:quant-ph/0505167.