Quantum Information Processing: Review / Synthèse

Symmetrization methods for characterization and benchmarking of quantum processes[1]

Joseph Emerson

Abstract: The detailed characterization of controlled quantum processes is a fundamental problem in experimental physics, and is a crucial requirement for the development of robust quantum information processing. Standard approaches for complete characterization of a quantum process require an number of experiments that grows exponentially with the number of interacting subsystems. Hence these methods are infeasible for many situations of practical interest. This paper reviews recent approaches to process estimation that overcome this problem by identifying subsets of the information that is of practical interest, and then demonstrating how this partial information can be estimated through the application of symmetrizing operations.

PACS Nos.: 03.67.Pp, 03.65.Yz, 03.65.wj

Résumé : La caractérisation détaillée des mécanismes quantiques contrôlés est un problème fondamental en physique expérimentale et une besoin crucial dans le développement de méthodes fiables de traitement de l'information quantique. Les approches standard pour caractériser de façon complète un mécanisme quantique requièrent des expériences en nombre croissant exponentiellement avec le nombre de sous-systèmes qui y jouent un rôle. Il en ressort que ces approches sont essentiellement inutiles pour les cas d'intérêt pratique. Nous passons ici en revue les approches qui surmontent ce problème, en estimant directement de l'information partielle d'intérêt pratique par le biais d'opérations de symétrisation.

[Traduit par la Rédaction]

1. Introduction

Precise, coherent control over the quantum dynamics of multibody systems, such as laser-cooled trapped ions, quantum dots, nuclear spin systems, and superconducting circuits, is an active area of research that holds the promise of new quantum technologies, and, in particular, quantum computation and quantum communication. As is well known, the quantum features of these systems are extremely sensitive to the noise and decoherence effects due to the environment and any other control limitations. Hence, a key experimental challenge is to characterize the quality of the implementation of an intended quantum process, and, in particular, the properties of the decoherence affecting a given experimental arrangement.

Methods for measuring the complete properties of a quantum process, known as process tomography [1–3], require a number of experiments that grow exponentially with the number of interacting subsystems. This task is infeasible for the kinds of systems that are required for the eventual practical application of quantum computation, which would require hundreds or even thousands of coherently coupled two-level systems (hereafter referred to as quantum bits, or *qubits*). Indeed, it is impractical already for the few qubits that can be coherently controlled in today's laboratories [4, 5]. However, in many contexts (discussed below) there is only a small subset of parameters that are of practical relevance. Hence, approaches to process characterization that can avoid this exponential overhead and directly estimate some or all of the relevant parameters are needed.

In this paper, I review an approach to partial characterization developed in refs. 6–8 that overcomes the exponential overhead of process tomography by symmetrizing the given quantum process with operations drawn from appropriate symmetry groups. Each symmetry group isolates distinct features of the process by averaging out all other details. The symmetrized process is described by a greatly reduced number of independent parameters that may be estimated by sampling the process with a standard input state followed by an appropriate measurement. This review paper is based on previously published work [6–8].

Received 4 October 2007. Accepted 22 October 2007. Published on the NRC Research Press Web site at http://cjp.nrc.ca/ on 2 May 2008.

J. Emerson. Department of Applied Mathematics and Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: jemerson@uwaterloo.ca).

[1]This paper was presented at the Theory CANADA 3 conference, held at the Theoretical Physics Institute of the University of Alberta, Edmonton, Alberta, Canada on 13–16 June 2007.

2. Mathematical description of quantum processes

In standard quantum mechanics an ideal transformation from time t_1 to time t_2, applied to input state ρ, is represented by a

 doi: 10.1139/P07-192

unitary operator U according to

$$\rho(t_1) \rightarrow \rho(t_2) = U\rho(t_1)U^\dagger$$

However, in practice the actual quantum transformation may be affected by noise due to imperfect control and unwanted interactions with other quantum systems. Provided that the system input state $\rho(t_1)$ is uncorrelated with any degrees of freedom of the noise that affect the subsequent quantum transformation, the most general transformation that can occur may be described by the following operator-sum decomposition:

$$\rho(t_2) = \Lambda(\rho(t_1)) = \sum_k A_k \rho(t_1) A_k^\dagger$$

where the set $\{A_k\}$ consists of arbitrary (bounded) linear operators subject to the probability-conservation constraint

$$\sum_k A_k^\dagger A_k = \mathbb{1}$$

Letting D denote the Hilbert space dimension, it is always possible to limit the sum to D^2 terms. Hence, it is immediately clear that the most general transformation is parameterized by $O(D^4)$ independent parameters. More precisely, it is easy to show that the number of independent parameters is $D^4 - D^2$. In the case of n-coupled two-level systems (qubits), we have $D = 2^n$, and hence the complete characterization of the process Λ is governed by an number of independent parameters that grows exponentially with the number of qubits.

There are three established methods for complete characterization via process tomography: standard quantum process tomography [1], ancilla-assisted process tomography [2], and direct-characterization [3]. Each of these requires an exponential number of distinct experimental configurations (distinct state preparations and (or) distinct measurements) in order to estimate the $O(2^{4n})$ independent parameters.

As noted above, often there are only a few parameters characterizing the process that are of practical interest. In the following, we consider two such contexts in detail followed by a discussion of the appropriate symmetrization groups that isolate these properties.

3. Fidelity estimation and bench-marking of quantum control

A natural criterion for bench-marking the accuracy with which an implemented quantum transformation Λ approaches the intended transformation U_t is the *average process fidelity*

$$F_{ave}(\Lambda) \equiv \int d\mu(\psi)\ \langle\psi|U_t^\dagger(\Lambda(|\psi\rangle\langle\psi|))U_t|\psi\rangle \tag{1}$$

where, without loss of generality, we may express Λ in terms of the decomposition,

$$\Lambda(\rho) = \mathcal{E}(U_t\rho U_t^\dagger) = \sum_k A_k U_t(\rho) U_t^\dagger A_k^\dagger \tag{2}$$

In this way, the map $\mathcal{E}$, and the associated operators $\{A_k\}$, represent the pure noise that has accumulated over the course of the implementation of U_t. The measure $d\mu(\psi)$ denotes the unitarily-invariant measure on the set of pure states (this is sometimes called the Haar-measure). If the implementation is perfect then $\Lambda(\rho) = U_t\rho U_t^\dagger$ and hence $F_{ave} = 1$. Under increasing decoherence F_{ave} decreases. Due to the invariance of the measure under unitary operations, it is clear that the average fidelity depends only on the noise itself, suggesting a more compact expression is possible. Indeed it has been shown that F_{ave} can been expressed in the form [9–11]

$$F_{ave}(\mathcal{E}) = \frac{\sum_k |\mathrm{Tr}(A_k)|^2 + D}{D^2 + D} \tag{3}$$

We note here that the average fidelity is also trivially related to two other standard fidelity benchmarks: (*i*) the entanglement-fidelity F_e, which has been proposed as means of characterizing the fidelity of a quantum channel $\mathcal{E}$ [12], and (*ii*) the gate-fidelity F_g, which has been used to characterize the quality of quantum memory [13] and the fidelity of an implementation of a target unitary U_t on a noisy quantum processing device [14, 15]. If the average process fidelity is applied to characterize a quantum channel or quantum memory then the target unitary is just the identity map, i.e., $U_t = \mathbb{1}$, and hence $\Lambda = \mathcal{E}$. Under this conceptual connection it can be shown [6, 11, 14] that in spite of the distinct mathematical definitions (and proposed methods of measurement) the Haar-average fidelity and the previously proposed gate-fidelity and entanglement-fidelity are related as follows,

$$F_{ave} = \frac{DF_g + 1}{D + 1} = \frac{DF_e + 1}{D + 1} \tag{4}$$

and hence all yield the same physical bench-marking information.

Any of these fidelities can be calculated if the noisy quantum process has been characterized experimentally. In the case of a quantum channel or quantum memory where $U_t = \mathbb{1}$, the noise process $\mathcal{E}$ can be determined experimentally by any method of process tomography. In the case of a nonidentity transformation then an additional step is required where one numerically factors out the inverse of the target map $U_t^{-1} \cdot U_t$ from the measured map Λ to determine the effective noise map $\mathcal{E}$. These procedures have been carried out, for example, for three qubits in recent implementations of the identity map and quantum Fourier transform using liquid-state nuclear magnetic resonance (NMR) techniques [13, 15]. However, as noted above, these methods require $\mathcal{O}(2^{4n})$ experiments and the conventional manipulation of matrices of dimension $2^{2n} \times 2^{2n}$.

How can we overcome this exponential cost? Consider the case where the target unitary is actually an identity map, $U_t = \mathbb{1}$. This situation is relevant in many contexts, for example, when the noisy transformation consists of quantum communication channel or of quantum memory. We first note that the average fidelity is equivalent to

$$F_{ave} = \int_{U(D)} dU\ \mathrm{Tr}\left[\rho U^{-1}\mathcal{E}(U(|0\rangle\langle 0|)U^{-1})U\right] \tag{5}$$

where dU refers to the unitarily-invariant Haar-measure on the unitary group and $|0\rangle\langle 0|$ is a fixed pure input state. Then, following the protocol developed in refs. 16 and 6, we can estimate

F_{ave} directly as follows: apply a unitary operator U randomly drawn from the Haar-measure to the initial state $|0\rangle$, followed by the quantum operation $\mathcal{E}$, and then apply $U^\dagger$ to the output state, followed by a measurement of the projector $|0\rangle\langle 0|$. F_{ave} can be estimated by repeating this procedure with U sampled randomly from the Haar measure in each experiment, where F_{ave} is just the probability of obtaining outcome 0 in the final measurement. Because we are only interested in a binary outcome, for an arbitrary, but fixed, average fidelity, the Chernoff bound guarantees that the number of experiments required to estimate F_{ave} to a given precision δ is independent of the Hilbert-space dimension D.

However, there are is a problem: implementing an exactly (or uniformly) random U requires an exponential number of gates. Numerical and analytic evidence that there exist efficiently constructable approximations to Haar-random unitary operators was demonstrated in refs. 17 and 18. Furthermore, it is shown in refs. 7 and 19 that there is a more structured solution to this problem, using the techniques of refs. 20–22. Specifically, the exponential cost can be overcome by noting that averaging over the Clifford group yields the same average fidelity as averaging over the Haar-measure,

$$\int_{U(D)} \mathrm{d}U\ U\dagger\mathcal{E}(U\rho)U\dagger)U = \frac{1}{|\mathcal{C}_n|}\sum_{U_i\in\mathcal{C}_n} U_i\dagger\mathcal{E}(U_i\rho U_i\dagger)U_i$$

where each U_i is an element of the Clifford group $\mathcal{C}_n$, which consists of the subgroup of the unitary group $U(D)$ for which the relation

$$U_i P_j U_i^\dagger = P_k$$

holds, for any $P_j, P_k \in \mathcal{P}_n$, where $\mathcal{P}_n$ is the set of all n-fold tensor products of single qubit Pauli operators $\{1, X, Y, Z\}$. The important point is that any element of the Clifford group can be implemented with $O(n^2)$ gates. An approximate approach to generating Clifford operations is developed in ref. 7, which reduces this overhead to $O(n\log(1/\epsilon))$, where ϵ is a measure of the accuracy of the average using this approximation. While this approach yields an efficient protocol for estimating F_{ave}, there are three shortcomings:

(*i*) significant noise can occur under the $O(n)$ gates required for the fidelity estimation protocol and this noise will typically lead to a significant over-estimation of the noise associated with Λ,

(*ii*) there is no information about more detailed features of the noise that can be obtained by this method, and

(*iii*) the protocol only works when the target transformation is the identity operation.

For partial solutions of how to adapt these methods to characterize nonidentity gates and factor out the noise from the symmetrizing operations see refs. 8 and 23. In the next section, we will consider a method for noise characterization that addresses how to extract additional information of interest about the noise.

4. Noise correlations and selection of error-correction strategy

The physical realization of robust quantum computation has been proven to be possible even in the presence of decoherence, *provided that* the decoherence affecting the quantum computer is sufficiently weak and also satisfies certain other desirable properties. This is the result of the theory of quantum error correction codes [24, 25] and the celebrated fault-tolerant threshold theorems [26–29]. These theorems demonstrate that certain kinds of errors occurring over the course of a quantum computation can be corrected and, moreover, that this error-followed-by-correction process can continue indefinitely, enabling arbitrarily complex quantum computations.

The problem is to determine if the noise affecting a given prototype quantum processor satisfies the various assumptions of these theorems. Two important properties of the noise in the context of these theorems are multiqubit and temporal correlations. Multiqubit noise correlations determine, for example, the failure probability of specific error-correction codes, which in turn affects the thresholds determined from various fault-tolerance theorems. Furthermore, knowledge of the multiqubit noise correlations is relevant to selecting optimal quantum error correction algorithms. The temporal correlations are associated with whether the decoherence is non-Markovian, basically meaning that it has "memory", and many useful threshold theorems are derived under the assumption that the decoherence is memoryless.

In this section, I describe a randomization protocol first reported in ref. 8 that enables direct determination of whether the noise exhibits some multiqubit or memory correlations without requiring the exponential overhead of quantum process tomography. The protocol requires only $2n$ single-qubit gates, a constant circuit depth, and $O(\log(n))$ experimental trials. This protocol is of immediate practical relevance for the characterization of noise in prototype quantum information processing systems, such as NMR, ion traps, superconducting circuits, and fiber-optic quantum communication channels.

The protocol requires symmetrizing the channel $\Lambda \to \overline{\Lambda}$ by averaging over trials in which the channel is conjugated by the elements of $\mathcal{C}_1$ applied independently to each qubit. An average over conjugations is known as a "twirl" [7, 20], and hence the above is a $\mathcal{C}_1^{\otimes n}$ twirl. The effect of this averaging procedure is expressed in the form

$$\mathcal{E}(\rho) \to \overline{\mathcal{E}(\rho)} = \frac{1}{|\mathcal{C}_1^{\otimes n}|}\sum_{i=1}^{|\mathcal{C}_1^{\otimes n}|}\sum_k C_i^\dagger A_k C_i \rho C_i^\dagger A_k^\dagger C_i \qquad (6)$$

We can give some intuitive idea of how twirling leads to a reduction of the number of independent parameters by considering the case of a noisy channel for a single qubit. To demonstrate the main idea most directly, we consider a simple stochastic noise model of the form

$$\mathcal{E}(\rho) = p_0 1\rho 1 + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z$$

which has three independent parameters (where $p_0 + p_x + p_y + p_z = 1$). Under conjugation, the Clifford operators map each

nonidentity Pauli operator to another Pauli operator [30]. For example, conjugation of the Pauli operators under the Hadamard gate H, which is an element of the Clifford group, has the following effect: $HXH^\dagger = HXH = Z$, $HYH = -Y$, and $HZH = X$. Hence, the H-conjugated noise model takes the form

$$H\mathcal{E}(H\rho H)H = p_0 1\rho 1 + p_x Z\rho Z + p_y Y\rho Y + p_z X\rho X$$

More generally, there are 12 elements of the Clifford group for a single qubit that divide into subsets, where the elements of each subset map each nonidentity Pauli operator to one of the three possible nonidentity Pauli operators with equal frequency. By averaging over each possible conjugation (operationally defined by the circuit given in Fig. 2), each of the possible Pauli errors becomes equiprobable, and the noise model transforms to the twirled form

$$\mathcal{E}(\rho) \to \overline{\mathcal{E}}(\rho) = p_0\rho + \left(\frac{p_1}{3}\right)(X\rho X + Y\rho Y + Z\rho Z)$$

where $p_1 = p_x + p_y + p_z$. As a result, we only need to estimate the probability of any one Pauli error in the twirled channel, and from that we can estimate the total probability of all three distinct single qubit Pauli errors in the untwirled channel.

Evaluation the full expression (6) requires expanding the noise operators $\{A_k\}$ in a basis of Pauli operators $P_i \in \mathcal{P}_n$, and then directly evaluating the action of the conjugation under elements of $\mathcal{C}_1^{\otimes n}$. An important quantity is the weight $w \in \{0, \ldots, n\}$ of a Pauli operator, which is the number of nonidentity factors in P_l. Aside from making use of the commutation relations amongst the Pauli operator as well as the orthogonality relation $\mathrm{Tr}[P_i P_j] = D\delta_{ij}$, the key step is to observe that conjugation via the full set of Clifford operators maps any nonidentity Pauli operator of a given weight to any possible nonidentity Pauli operator of that same weight with equal frequency [22]. This "decorrelates" each Pauli operator in a given weight class with the associated coefficient. Hence, separating out terms according to their Pauli weight w, letting the index $\nu_w \in \{1, \ldots, \binom{n}{w}\}$ count the number of distinct ways that w nonidentity Pauli operators can be distributed over the n factor spaces and the index $\mathbf{i}_w = \{i_1, \ldots, i_w\}$ with $i_j \in \{1, 2, 3\}$ denote which of the nonidentity Pauli operators occupies the jth occupied site, we obtain

$$\overline{\mathcal{E}(\rho)} = \sum_{w=0}^{n} \sum_{\nu_w=1}^{\binom{n}{w}} r_{w,\nu_w} \sum_{\mathbf{i}_w} P_{w,\nu_w,\mathbf{i}_w} \rho P_{w,\nu_w,\mathbf{i}_w} \tag{7}$$

where $r_{w,\nu_w} = (1/3^w)\sum_{\mathbf{i}_w} a_{w,\nu_w,\mathbf{i}_w}$ (for complete details of this derivation see ref. 8). If the symmetrized channel is probed by the initial state $|0\rangle \equiv |0\rangle^{\otimes n}$, followed by a projective measurement of the output state in the basis $|l\rangle$, this yields an n-bit string $l \in \{0, 1\}^n$. Let $q_{w'}$ denote the probability that a random subset of w' bits of the binary string l has even parity. Noting that $c_{w'} \equiv \langle \overline{Z^{\otimes w'}} \rangle = 2q_{w'} - 1$, where $\overline{Z^{\otimes w'}}$ is the average of all Pauli operators with w' factors of Z and $n - w'$ identity factors, we obtain $p_w = \sum_{w'} \Omega^{-1}_{w,w'} c_{w'}$ where the matrix $\Omega^{-1}_{w,w'}$ is a matrix of combinatorial factors given in ref. 8), and the p_w are probabilities of interest, i.e., the probabilities of w simultaneous qubit errors occurring over the course of the quantum process. If in each single shot experiment the Clifford operators are chosen uniformly at random then with $K = \mathcal{O}(\log(2n)/\delta^2)$ experiments we can estimate each of the coefficients c_w to precision δ with constant probability.

We can apply these measured quantities to determine the performance of a broad class of quantum-error-correcting codes (QECCs) and the applicability of certain assumptions underlying FT thresholds. In general, QECCs protect quantum information only against certain types of noise. A distance-$(2t + 1)$ code refers to codes that correct all errors simultaneously affecting up to t qubits. Hence, the distance of a QECC determines which terms in the noise will be corrected and which will remain uncorrected. The latter contribute to the overall failure probability. The p_w enable a direct estimate of the failure probability (and hence the performance of a given quantum error correcting code) without making any assumptions about the absence of correlations in the noise. This test is efficient for correlations up to a fixed scale b (where b is the number of a qubits in the multibody correlation), in which case n^b measurements are required. The c_w can be applied directly to test some of the assumptions that yield rigorous estimates of the fault-tolerance threshold [31]. In particular, a noisy channel with an uncorrelated distribution of error locations, but with arbitrary correlations in the error type at each location, is mapped under the symmetrization to a channel, which is a tensor product of n single-qubit depolarizing channels. A channel satisfying this property will exhibit the scaling $c_w = c_1^w$. Hence, observed deviations from this scaling imply a violation of the above assumption. However, there are correlated error models that also give rise to this scaling and hence experimental verification of it does not imply the absence of any correlations in the untwirled noise. Furthermore, the question of whether the noise exhibits non-Markovian properties can be tested efficiently by repeating the above scheme for distinct time-intervals $m\tau$ with increasing m. If over the time-scale τ the noise can be described by a master equation in Lindblad form [32], then it satisfies the Markovian semigroup property $\Lambda_\tau \circ \Lambda_\tau = \Lambda_{2\tau}$, as will the twirled map $\overline{\Lambda_\tau} \circ \overline{\Lambda_\tau} = \overline{\Lambda_{2\tau}}$. Consequently, the measured noise coefficients $c_w(m\tau)$ for the time scale $m\tau$ will satisfy the scaling $c_w(m\tau) = c_w(\tau)^m$. Hence, any observed deviations from this scaling imply non-Markovian effects in the untwirled noise. However, it should be stressed that experimental verification of this scaling does not guarantee that the untwirled noise is Markovian.

5. Related work

Recently, related methods have been proposed to characterize other features of the decoherence using symmetrization methods. In ref. 33, independent twirling of individual qubits is applied to estimate features of the effective Hamiltonian governing the decoherence. In ref. 23, the asymptotic properties of noise affecting a single qubit is estimated by considering long Pauli-randomized sequences of random Clifford gates. Furthermore, in a paper being prepared[2], independent Pauli-twirling

[2] M. Silva, E. Magesan, D. Kribs, and J. Emerson. Manuscript in preparation.

of individual qubits is shown to enable a scalable experimental protocol for the identification of whether there exists some encoding structures, such as noiseless subsystems, that allow for approximately or exactly protected storage of quantum information under the given decoherence process.

Acknowledgements

This review paper is based on talk given at the Theory CANADA 3 conference in Edmonton, Alberta, that summarizes previously published work [6–8] developed with the following collaborators: Robert Alicki, Jonathan Baugh, Richard Cleve, David Cory, Christoph Dankert, Etera Livine, Ray Laflamme, Martin Laforest, Osama Moussa, Colm Ryan, Marcus Silva, and Karol Zyczkowski. This paper was supported in part by MITACS (Mathematics of Information Technology and Complex Systems) and the Natural Sciences and Engineering Research Council.

References

1. I. Chuang and M. Nielsen. J. Mod. Opt. **44**, 2455 (1997).
2. G.M. D'Ariano and P. Lo Presti. Phys. Rev. Lett. **86**, 4195 (2001).
3. M. Mohseni and D. Lidar. Phys. Rev. Lett. **97**, 170501 (2006).
4. H. Häffner, W. Hänsel, C.F. Roos, J. Benhelm, D. Chek-al-kar, M. Chwalla, T. Körber, U.D. Rapol, M. Riebe, P.O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt. Nature, **438**, 643 (2005).
5. C. Negrevergne, T.S. Mahesh, C.A. Ryan, M. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D.G. Cory, and R. Laflamme. Phys. Rev. Lett. **96**, 170501 (2006).
6. J. Emerson, R. Alicki, and K. Zyczkowski. J. Opt. B: Quantum Semiclassical Opt. **7** S347 (2005).
7. C. Dankert, R. Cleve, J. Emerson, and E. Livine. quant-ph/0606161 (2006).
8. J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D.G. Cory, and R. Laflamme. Science, **317**, 1893 (2007).
9. M. Horodecki, P. Horodecki, and R. Horodecki. Phys. Rev. A, **60**, 1888 (1999).
10. M.D. Bowdrey, D.K.L. Oi, A.J. Short, K. Banaszek, and J.A. Jones. Phys. Lett. **294A**, 258 (2002).
11. M. Nielson. Phys. Lett. **303A**(4), 249 (2002).
12. B. Schumacher. Phys. Rev. A, **54**, 2614 (1996).
13. N. Boulant, T.F. Havel, M.A. Pravia, and D.G. Cory. Phys. Rev. A, **67**, 042322 (2003).
14. E.M. Fortunato, M.A. Pravia, N. Boulant, G. Teklemariam, T.F. Havel, and D.G. Cory. J. Chem. Phys. **116**, 7599 (2002).
15. Y. Weinstein, T.F. Havel, J. Emerson, N. Boulant, M. Saraceno, and D. Cory. J. Chem. Phys. **121**, 6117 (2004).
16. J. Emerson, Y.S. Weinstein, S. Lloyd, and D.G. Cory. Phys. Rev. Lett. **89**, 284102 (2002).
17. J. Emerson, Y. Weinstein, M. Saraceno, S. Lloyd, and D. Cory. Science, **302**, 2098 (2003).
18. J. Emerson, E. Livine, and S. Lloyd. Phys. Rev. A, **72**, 060302(R) (2005).
19. W. Dür, M. Hein, J.I. Cirac, and H.-J. Briegel. Phys. Rev. A, **72**, 052326 (2005).
20. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters. Phys. Rev. A, **54**(5), 3824 (1996).
21. D. DiVincenzo, D. Leung, and B. Terhal. IEEE Trans. Inform. Theory, **48**(3), 580 (2002).
22. H. Chau. IEEE Trans. Inform. Theory, **51**(4), 1451 (2005).
23. E. Knill, D. Leibfried, R. Reichle, J. Britton, R.B. Blakestad, J.D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D.J. Wineland. arXiv:0707.0963.
24. P.W. Shor. Phys. Rev. A, **52**, R2493 (1995).
25. A.M. Steane. Phys. Rev. Lett. **77**, 793 (1996).
26. P.W. Shor. Proceedings of the Symposium on the Foundations of Computer Science, 14–16 October 1996. IEEE Press, Los Alamitos, Calif. 1996. pp. 56–65.
27. D. Aharonov and M. Ben-Or. Proceedings of the 29th Annual ACM Symposium on the Theory of Computing, ACM Press, New York. 1996. p. 176.
28. A.Y. Kitaev. Uspekhi Mat. Nauk, **52**, 53 (1997).
29. E. Knill and R. Laflamme. Science, **279**, 342 (1998).
30. D. Gottesman. Ph.D. thesis, California Institute of Technology. cquant-ph/9705052 (1997).
31. P. Aliferis, D. Gottesman, and J. Preskill. Quant. Inf. Comp. **6**, 97 (2006).
32. R. Alicki and K. Lendi. Lect. Notes Phys. **286**, (1987).
33. B. Levi, C. Lopez, J. Emerson, and D.G. Cory. Phys. Rev. A, **75**, 022314 (2007).