Pis'ma v ZhETF, vol. 79, iss. 5, pp. 291 – 295 © 2004 March 10

A small error-correction code for protecting three-qubit quantum information

Chui-Ping Yang[+*], *Shih-I Chu*[*], *Siyuan Han*[+]

[+]*Department of Physics and Astronomy, University of Kansas, 66045 Lawrence, Kansas USA*

[*]*Department of Chemistry, University of Kansas, and Kansas for Advanced Scientific Computing, 66045 Lawrence, Kansas, USA*

Submitted 16 December 2003

We present a quantum error correction code which protects three quantum bits (qubits) of quantum information against one erasure, i.e., a single-qubit arbitrary error at a known position. The present code has a high encoding efficiency since only one auxiliary qubit is needed for one message qubit on average. In addition, we note that the code can also work even in a worse case that the interaction with environment causes a leakage out of the qubit space. The code may have some applications in the storage of quantum information for a small-scale quantum computing, quantum information processing, and quantum communication.

PACS: 03.65.Bz, 03.67.Lx, 89.70.+c

Quantum computing has become an active aspect of current research fields with the discovery of Shor's algorithm for factorizing a large number [1, 2]. It has become clear that quantum computer are in principle able to solve hard computational problems more efficiently than present classical computers [1 – 4]. However, the biggest difficulty inhibiting realizations is the fragility of quantum states. Decoherence of qubits caused by the interaction with environment will collapse the state of the quantum computer and thus lead to the loss of information. To solve this problem, Shor, and independently Stean, inspired by the theory of classical error correction, proposed the first two quantum error correction codes (QECCs), i.e., the nine-qubit code [5] and the seven-qubit code [6], which are able to correct errors that occur during the store of qubits. Following this work, many new QECCs have been discovered [7 – 20]. For the most general error model, Laflamme et al. have shown that the smallest quantum error correction code, for encoding one qubit of quantum information and correcting a single-qubit arbitrary error at an unknown position, is the five-qubit code [7]. On the other hand, apart from the QECCs, many alternative quantum codes have been proposed, such as the quantum error preventing codes (based on the quantum Zeno effect) [21, 22] and the quantum error-avoiding codes (based on decoherence-free subspaces (DFSs) [23 – 25]. Moreover, dynamical suppression of decoherence [26 – 28] and noiseless subsystems [29 – 32] have been presented.

In 1997 M. Grassl et al. [33] considered an error model where the position of the erroneous qubits is known. In accordance with classical coding theory, they called this model the quantum erasure channel. Some physical scenarios to determine the position of an error have been given [33]. For instance, if errors are accompanied by the emission of quanta, they can in principle be detected. In their work, they showed that only four-qubit error correction code is required to encode one qubit and correct one erasure (i.e., a single-qubit arbitrary error for which the position of the "damaged" qubit is known). Also, they showed that two qubits of quantum information could be encoded and one erasure could be corrected by extending such four-qubit code, in a sense that only one additional qubit is required for encoding one "message" qubit on average. Clearly, this code is a very compact code for protecting one or two qubits of quantum information as long as the position of the "bad" qubit is known. However, at least *eight* qubits are needed in protecting three-qubit quantum information by using such a code (four qubits required for encoding one qubit of quantum information plus another four qubits necessary for encoding the remaining two qubits of quantum information). In this letter we will present a new error-correction code which requires only three auxiliary qubits (i.e., totally six qubits) for protecting three qubits of quantum information against one erasure. We will show how the present code works through the encoding, decoding, and error recovery operations.

The Hilbert space of a three-qubit system is a tensor product of two-dimensional spaces C_2 (qubits), i.e., $C = C_2^{\otimes 3}$. An arbitrary state of three qubits (labeled by 1, 2 and 3) can be expanded as follows

$$|\psi\rangle_{123} = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \\ + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle , \quad (1)$$

where $\sum_{i=0}^{7} |\alpha_i|^2 = 1$; $\{|ijk\rangle\}$ forms a set of complete orthogonal states in the eight-dimensional space, $i, j, k \in \{0, 1\}$; and we are taking the $|0\rangle$ and $|1\rangle$ states of a qubit to correspond to the " down" and "up" states, respectively, of a fictitious spin $\frac{1}{2}$ particle. Using three ancillary qubits (1′, 2′, 3′), we encode the original state into

$$|\psi\rangle_L = \alpha_0 |0\rangle_L + \alpha_1 |1\rangle_L + \alpha_2 |2\rangle_L + \alpha_3 |3\rangle_L + \\ + \alpha_4 |4\rangle_L + \alpha_5 |5\rangle_L + \alpha_6 |6\rangle_L + \alpha_7 |7\rangle_L , \qquad (2)$$

where the eight logical states are

$$\begin{aligned} |0\rangle_L &= (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) , \\ |1\rangle_L &= (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) , \\ |2\rangle_L &= (|010\rangle + |101\rangle) \otimes (|010\rangle + |101\rangle) , \\ |3\rangle_L &= (|010\rangle - |101\rangle) \otimes (|010\rangle - |101\rangle) , \\ |4\rangle_L &= (|100\rangle + |011\rangle) \otimes (|100\rangle + |011\rangle) , \\ |5\rangle_L &= (|100\rangle - |011\rangle) \otimes (|100\rangle - |011\rangle) , \\ |6\rangle_L &= (|110\rangle + |001\rangle) \otimes (|110\rangle + |001\rangle) , \\ |7\rangle_L &= (|110\rangle - |001\rangle) \otimes (|110\rangle - |001\rangle) \end{aligned} \qquad (3)$$

(here, for every logical state, the left part of the product corresponds to the three "message" qubits while the right part of the product corresponds to the three ancillary qubits, and the arrangement sequence of the six qubits is 1, 2, 3, 1′, 2′ and 3′ from left to right; to simplify the notation, normalization factors are omitted here and in the remainder of this section).

Let us first briefly review some basics of quantum error correction codes. It has been shown that one can model the errors by the use of error operators A. For the general case, Kill and Laflamme [17] derived the following necessary and sufficient conditions on quantum error correction codes

$$\langle i_L | A_a^+ A_b | i_L \rangle = \langle j_L | A_a^+ A_b | j_L \rangle , \qquad (4)$$

and

$$\langle i_L | A_a^+ A_b | j_L \rangle = 0 \quad for \, \langle i_L | j_L \rangle = 0, \qquad (5)$$

where $|i_L\rangle$ and $|j_L\rangle$ are any two orthonormal basis states of the code (i.e., any two logical states). For the purpose of error correction, it is enough to consider errors of the type σ_x (bit flip), σ_z (phase flip), and σ_y (bit and phase flip), since, by linearity, a code that can correct these errors can correct any arbitrary errors [8]. For a $[n, k, t]$ code, i.e., a code encoding k qubits through n qubits and correcting t errors at most, the error operators $\{A_a\}$ are the tensor product of the identity on $n - t$ qubits and t one-bit error operators on the altered qubits. The one-bit error operators are any linear combinations of the algebra basis $\{1, \sigma_x, \sigma_y, \sigma_z\}$.

The above conditions have been generalized to the quantum erasure channel [33, 34]. Since the positions of the errors are known, it is not necessary to separate the spaces which correspond to errors at different positions. For the case of correcting erasure errors, the error operators A_a and A_b differ from each other by one-bit error operators at the same positions only. Since the product of such t-error operators is also a t-error operator which can be written as a linear combination of the A_a, it follows from Eqs. (4) and (5) that the necessary and sufficient conditions corresponding to the erasure-correcting case will be [33, 34]

$$\langle i_L | A_a | i_L \rangle = \langle j_L | A_a | j_L \rangle , \qquad (6)$$

$$\langle i_L | A_a | j_L \rangle = 0 \quad for \, \langle i_L | j_L \rangle = 0. \qquad (7)$$

Now we give the interpretations of the encoding (3) in terms of error correction codes. For the case of one erasure, the error operators A_a in Eqs. (6) and (7) are the one-bit error operators for the "bad" qubit, which are any linear combinations of the algebra basis $\{1, \sigma_x, \sigma_y, \sigma_z\}$. One can easily verify that no matter which qubit goes "bad", any two of the eight logical states (3) satisfy the above conditions (6) and (7). Thus, these logical states in (3) can be regarded as an erasure-correcting code: it can, in principle, encode three qubits and correct one erasure. In the following, we will show explicitly how this can be done.

The encoding (3) can be fulfilled by the quantum CNOT (controlled-NOT) operations C_{ij}, where the first subscript of C_{ij} refers to the control bit and the second to the target. The three ancillary qubits 1′, 2′ and 3′ are initially in the state $|000\rangle$. Throughout this paper, every joint operation will follow the sequence from right to left. Let a joint encoding operation on the six qubits

$$U_e = C_{3'2'} C_{3'1'} \; C_{32} C_{31} H_{3'} H_3 C_{33'} C_{22'} C_{11'} , \qquad (8)$$

where H_i is a Hadamard transformation on the qubit i which sends $|0\rangle \to (|0\rangle + |1\rangle)$ and $|1\rangle \to (|0\rangle - |1\rangle)$, thus we have

$$U_e \left(|\psi\rangle_{123} |000\rangle_{1'2'3'} \right) = \; |\psi\rangle_L . \qquad (9)$$

One can certainly envision situations where one might, in fact, know where the error has occurred (by using the methods for determining the position of an error [33]). Let us first consider the case in which qubit 1 undergoes decoherence. Because $|0\rangle$ and $|1\rangle$ form a basis for the qubit 1, we need only know what happens

to these two states. In general, the decoherence process must be

$$\begin{aligned} |e_0\rangle|0\rangle &\to |\epsilon_0\rangle|0\rangle + |\epsilon_1\rangle|1\rangle, \\ |e_0\rangle|1\rangle &\to |\epsilon_0'\rangle|0\rangle + |\epsilon_1'\rangle|1\rangle, \end{aligned} \tag{10}$$

where $|\epsilon_0\rangle, |\epsilon_1\rangle, |\epsilon_0'\rangle$ and $|\epsilon_1'\rangle$ are appropriate environment states, not necessarily orthogonal or normalized and $|e_0\rangle$ is the initial state of the environment. As will be shown below, during the restoration operation there is no need of performing any operations on the qubit 1. For the simplicity, we can rewrite Eq. (10) as

$$\begin{aligned} |e_0\rangle|0\rangle &\to \left|\widetilde{0}\right\rangle, \\ |e_0\rangle|0\rangle &\to \left|\widetilde{1}\right\rangle, \end{aligned} \tag{11}$$

where the above environment states $|\epsilon_0\rangle$, $|\epsilon_1\rangle$, $|\epsilon_0'\rangle$ and $|\epsilon_1'\rangle$ have been included in $\left|\widetilde{0}\right\rangle$ and $\left|\widetilde{1}\right\rangle$. Let us now see what will happen to the encoded state $|\psi\rangle_L$. After decoherence, it goes to

$$\begin{aligned} |\psi\rangle_L \otimes |e_0\rangle = \alpha_0 \left|\widetilde{0}\right\rangle_L + \alpha_1 \left|\widetilde{1}\right\rangle_L + \alpha_2 \left|\widetilde{2}\right\rangle_L + \\ + \alpha_3 \left|\widetilde{3}\right\rangle_L + \alpha_4 \left|\widetilde{4}\right\rangle_L + \alpha_5 \left|\widetilde{5}\right\rangle_L + \alpha_6 \left|\widetilde{6}\right\rangle_L + \alpha_7 \left|\widetilde{7}\right\rangle_L, \end{aligned} \tag{12}$$

where

$$\begin{aligned} \left|\widetilde{0}\right\rangle_L &= \left(\left|\widetilde{0}00\right\rangle + \left|\widetilde{1}11\right\rangle\right) \otimes (|000\rangle + |111\rangle), \\ \left|\widetilde{1}\right\rangle_L &= \left(\left|\widetilde{0}00\right\rangle - \left|\widetilde{1}11\right\rangle\right) \otimes (|000\rangle - |111\rangle), \\ \left|\widetilde{2}\right\rangle_L &= \left(\left|\widetilde{0}10\right\rangle + \left|\widetilde{1}01\right\rangle\right) \otimes (|010\rangle + |101\rangle), \\ \left|\widetilde{3}\right\rangle_L &= \left(\left|\widetilde{0}10\right\rangle - \left|\widetilde{1}01\right\rangle\right) \otimes (|010\rangle - |101\rangle), \\ \left|\widetilde{4}\right\rangle_L &= \left(\left|\widetilde{1}00\right\rangle + \left|\widetilde{0}11\right\rangle\right) \otimes (|100\rangle + |011\rangle), \\ \left|\widetilde{5}\right\rangle_L &= \left(\left|\widetilde{1}00\right\rangle - \left|\widetilde{0}11\right\rangle\right) \otimes (|100\rangle - |011\rangle), \\ \left|\widetilde{6}\right\rangle_L &= \left(\left|\widetilde{1}10\right\rangle + \left|\widetilde{0}01\right\rangle\right) \otimes (|110\rangle + |001\rangle), \\ \left|\widetilde{7}\right\rangle_L &= \left(\left|\widetilde{1}10\right\rangle - \left|\widetilde{0}01\right\rangle\right) \otimes (|110\rangle - |001\rangle). \end{aligned} \tag{13}$$

Comparing Eq. (13) with Eq. (3), one can see that for each "bad" logical state in (13), the right part of the product, which corresponds to the encoding of the three ancillary qubits, is intact. We can first perform a unitary transformation on the three ancillary qubits which we regard as the partial decoding operation (since the qubits 1, 2 and 3 are not involved in the decoding operation). The decoding operation is shown as follows

$$U_d = H_{3'} C_{3'2'} C_{3'1'}. \tag{14}$$

After decoding, we have

$$\begin{aligned} \left|\widetilde{0}\right\rangle_L &\to \left(\left|\widetilde{0}00\right\rangle + \left|\widetilde{1}11\right\rangle\right) \otimes |000\rangle, \\ \left|\widetilde{1}\right\rangle_L &\to \left(\left|\widetilde{0}00\right\rangle - \left|\widetilde{1}11\right\rangle\right) \otimes |001\rangle, \\ \left|\widetilde{2}\right\rangle_L &\to \left(\left|\widetilde{0}10\right\rangle + \left|\widetilde{1}01\right\rangle\right) \otimes |010\rangle, \\ \left|\widetilde{3}\right\rangle_L &\to \left(\left|\widetilde{0}10\right\rangle - \left|\widetilde{1}01\right\rangle\right) \otimes |011\rangle, \\ \left|\widetilde{4}\right\rangle_L &\to \left(\left|\widetilde{1}00\right\rangle + \left|\widetilde{0}11\right\rangle\right) \otimes |100\rangle, \\ \left|\widetilde{5}\right\rangle_L &\to \left(\left|\widetilde{1}00\right\rangle - \left|\widetilde{0}11\right\rangle\right) \otimes |101\rangle, \\ \left|\widetilde{6}\right\rangle_L &\to \left(\left|\widetilde{1}10\right\rangle + \left|\widetilde{0}01\right\rangle\right) \otimes |110\rangle, \\ \left|\widetilde{7}\right\rangle_L &\to \left(\left|\widetilde{1}10\right\rangle - \left|\widetilde{0}01\right\rangle\right) \otimes |111\rangle. \end{aligned} \tag{15}$$

What we need to do now is to perform an error recovery operation in order to extract the original state (1). It can be done by a unitary transformation on the qubits 2, 3, $1', 2'$ and $3'$, which is described by

$$U_r = T_{1'3'2} Z_{3'2} T_{1'3'2} C_{2'2} C_{1'2} C_{1'3}, \tag{16}$$

where $T_{1'3'2}$ is a Toffoli gate operation [35], and $Z_{3'2}$ is a controlled Pauli σ_z operation. A Toffoli gate operation T_{ijk} has the two control bits corresponding to the first two subscripts (i, j), and the target bit k. When the two control bits are in the state $|11\rangle$, the state of the target bit will change, following $|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$; while when the two control bits are in the state $|00\rangle, |01\rangle$ or $|10\rangle$, the state of the target bit will be invariant. A controlled Pauli σ_z operation Z_{ij} has the control bit i and the target bit j, which sends the state of the target bit $|0\rangle \to |0\rangle$ and $|1\rangle \to -|1\rangle$ when the control bit is in the state $|1\rangle$; otherwise, when the control bit is in $|0\rangle$, the state of the target bit will not change. One can easily verify that after the operation U_r, the system composed of the six qubits and the environment will be in the state

$$\left(\left|\widetilde{0}00\right\rangle + \left|\widetilde{1}11\right\rangle\right) \otimes |\psi\rangle_{1'2'3'}, \tag{17}$$

where

$$\begin{aligned} |\psi\rangle_{1'2'3'} = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \\ + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle. \end{aligned} \tag{18}$$

From Eqs. (17), (18), one can see that the above restoration operation is actually a disentangling operation, which has made the three qubits $1', 2'$ and $3'$ no longer entangled with the remaining system (i.e., the three qubits 1, 2, 3 and the environment). Even though the three qubits 1, 2 and 3 are entangled with the environment, the information, originally carried by the qubits 1, 2 and 3, has been completely transferred into the three qubits $1', 2'$ and $3'$, and the original state (1)

has been exactly reconstructed through the three qubits $1', 2'$ and $3'$.

It is straightforward to extract the original state when the error occurs on the qubit 2 or 3. To simplify our presentation, however, we will not give a detailed discussion. In the case of qubit 2 or qubit 3 going "bad", the decoding operation is the same as above. If the qubit 2 goes "bad", the error recovery operation will be $T_{2'3'1}Z_{3'1}T_{2'3'1}C_{1'1}C_{2'1}C_{2'3}$; while when the qubit 3 goes "bad", the error recovery operation is much simpler, i.e., $Z_{3'2}C_{2'2}C_{1'1}$. After performing the error recovery operations, the final state, corresponding to the case when the error occurs on the qubit 2 or 3, will be

$$\left(\left|0\widetilde{0}0\right\rangle + \left|1\widetilde{1}1\right\rangle\right) \otimes |\psi\rangle_{1'2'3'}\,, \tag{19}$$

or

$$\left(\left|00\widetilde{0}\right\rangle + \left|11\widetilde{1}\right\rangle\right) \otimes |\psi\rangle_{1'2'3'}\,. \tag{20}$$

In above we discussed how to recover the original state when the qubit 1, 2 or 3 undergoes decoherence. From Eq. (3) one can easily see that for each logical state, the qubits 1, 2, 3 and the qubits $1'$, $2'$, $3'$ are in the same GHZ states, i.e., each logical state is a product of two copies of a three-qubit GHZ state. Thus, the decoding and error recovery operations for the case of the qubit $1'$, $2'$ or $3'$ going "bad" are similar to those, respectively, for the case of the qubit 1, 2 or 3 going "bad". The only thing to be noted is that when the qubits $1'$, $2'$ or $3'$ goes "bad", the subscripts ($1'$, $2'$, $3'$, 1, 2, 3), which are involved in the above decoding and error-recovery unitary transformations, need to be permuted into (1, 2, 3, $1'$, $2'$, $3'$), respectively. Thus, we have (a) when the qubits $1'$, $2'$ or $3'$ goes "bad", the decoding operation is given by $H_3C_{32}C_{31}$; (b) for the case of the qubit $1'$, $2'$ or $3'$ going "bad", the error recovery operation is given by $T_{132'}Z_{32'}T_{132'}C_{22'}C_{12'}C_{13'}$, $T_{231'}Z_{31'}T_{231'}C_{11'}C_{21'}C_{23'}$ or $Z_{32'}C_{22'}C_{11'}$, respectively. After performing the decoding and error recovery operations, the original state will be restored through the qubits 1, 2 and 3; while the qubits $1', 2'$ and $3'$ are entangled with the environment.

It is interesting to note that the present code can also work when error happens out of qubit spaces. The above decoherence process (10), in fact, corresponds to the case when qubits are represented by ideal "two-state" or "two-level" systems. In most cases, physical systems (particles or solid state devices) may have many levels, such as atoms, ions and SQUIDs. If a qubit is represented by a two-dimensional (2D) subspace of the Hilbert space of a multi-level physical system, the interaction with environment may lead to the leakage out of the 2D qubit space (i.e., the space spanned by the two states $|0\rangle$ and $|1\rangle$ of a qubit). The decoherence process, therefore, is given by

$$\begin{aligned} |e_0\rangle\,|0\rangle &\to |\epsilon_0\rangle\,|0\rangle + |\epsilon_1\rangle\,|1\rangle + \sum_{i\neq 0,1} |\epsilon_i\rangle\,|i\rangle\,, \\ |e_0\rangle\,|1\rangle &\to |\epsilon_0'\rangle\,|0\rangle + |\epsilon_1'\rangle\,|1\rangle + \sum_{i\neq 0,1} |\epsilon_i'\rangle\,|i\rangle\,, \end{aligned} \tag{21}$$

where $\{|i\rangle\}$, together with $|0\rangle$ and $|1\rangle$, forms a complete orthogonal basis of a multi-level system, and $|\epsilon_i\rangle$, $|\epsilon_i'\rangle$ are environment states. Note that during the above restoration operation, there is no need of performing any operations on the "bad"qubit. Thus, for the case when a qubit is represented by a 2D subspace of a multi-level physical system and decoherence happens like (21), one can still protect an arbitrary state of three qubits against one erasure by using the code and following the restoration operations described above.

Finally, we note that for some special types of three-qubit state, the protection against one erasure may be done by a code with a smaller number of qubits. For example, one can show that the following three-qubit states

$$\alpha\,|001\rangle + \beta\,|010\rangle + \gamma\,|100\rangle \tag{22}$$

(which, in the case of $|\alpha| = |\beta| = |\gamma| = 1/\sqrt{3}$, are called "entangled W states" [36] that have attracted much interest recently) can be protected against one erasure through the following five-qubit code

$$\begin{aligned} |001\rangle &\to |00001\rangle + |11110\rangle\,, \\ |010\rangle &\to |00100\rangle + |11011\rangle\,, \\ |100\rangle &\to |00010\rangle + |11101\rangle\,. \end{aligned} \tag{23}$$

The present code may have some application in protecting a few qubits of quantum information against decoherence. It is presumed that the first prototype quantum computer will be small and quantum information will be stored through only a few qubits. Moreover, there is much interest arising from quantum computing network which is based on the connection of locally distinct nodes each carrying out a small-scale quantum computing [37]. In addition, as noted in [33], quantum erasure-correcting codes may be applied in *fault tolerant quantum computing*, which was proposed by Shor and permits one to perform quantum computation and error correction with a network of erroneous quantum gates [38]. Thus, the present code may be also useful in a small-scale *fault tolerant* quantum computing or in the demonstration of quantum algorithm of a few qubits. Finally, since the "bad" qubit is not involved in

the above restoration operation (i.e., it does not contain any information so that it can be "thrown away" without affecting the recovery of the original message), the code is also one for hiding three qubits of quantum information over each qubit. Therefore, the present code may have some other applications in quantum information processing and quantum communication, such as quantum secret sharing [39] and quantum cryptography [40].

In summary, we have proposed a small code for protecting three-qubit quantum information against one erasure. As shown above, the encoding, decoding and error recovery operations presented here are straightforward. We believe that the present code is of some interest, especially because of its high encoding efficiency, i.e., only one ancillary qubit being required for one "message" qubit on average, and because of its usefulness in a worse case that the interaction with environment leads to a leakage out of the qubit space.

This work was partially supported by National Science Foundation (# EIA-0082499), and AFOSR (# F49620-01-1-0439), funded under the Department of Defense University Research Initiative on Nanotechnology (DURINT) Program and by the ARDA.

1. P. W. Shor, in *Proc. 35th Annual Symp. on Foundations of Computer Science*, IEEE Computer Society Press, New York 1994, pp. 124–134.
2. I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, Science **270**, 1633 (1995).
3. D. Deutsch, Proc. R. Soc. **A400**, 97 (1985); ibid. **425**, 73 (1989).
4. L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
5. P. W. Shor, Phys. Rev. **A52**, R2493 (1995).
6. A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
7. R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
8. A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
9. D. Gottesman, Phys. Rev. **A54**, 1862 (1996).
10. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. **A54**, 3824 (1996).
11. A. M. Steane, Phys. Rev. **A54**, 4741 (1996); A. M. Steane, Proc. R. Soc. London **A452**, 2551 (1996).
12. P. W. Shor, LANL eprint quant-ph/9605011; P. Shor and R. Laflamme, Phys. Rev. Lett. **78**, 1600 (1997).
13. D. P. DiVincenzo and P. W. Shor, Phys. Rev. Lett. **77**, 3260 (1996).
14. W. H. Zurek and R. Laflamme, Phys. Rev. Lett. **77**, 4683 (1996).
15. M. B. Plenio, V. Vedral, and P. L. Knight, Phys. Rev. **A55**, 67 (1997).
16. A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett **78**, 405 (1997).
17. E. Knill and R. Laflamme, Phys. Rev. **A55**, 900 (1997).
18. D. W. Leung, M. A. Nielsen, Isaac L. Chuang, and Y. Yamamoto, Phys. Rev. **A56**, 2567 (1997).
19. J. Preskill, LANL e-print quant-ph/9705031.
20. C. H. Bennett and P. W. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998).
21. L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. **A54**, R1745 (1996).
22. L. M. Duan and G. C. Guo, Phys. Rev. **A57**, 2399 (1998).
23. L. M. Duan and G. C. Guo, Phys. Rev. Lett. **79**, 1953 (1997).
24. P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997); P. Zanardi, Phys. Rev. **A57**, 3276 (1998).
25. D. A. Lidar, D. Bacon, and K. B. Whaley, Phys. Rev. Lett. **82**, 4556 (1999); D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
26. L. Viola and S. Lloyd, Phys. Rev. **A58**, 2733 (1998); L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **82**, 2417 (1999); L. Viola, S. Lloyd, and E. Knill, Phys. Rev. Lett. **83**, 4888 (1999).
27. D. Vitali and P. Tombesi, Phys. Rev. **A59**, 4178 (1999).
28. G. S. Agarwal, Phys. Rev. **A61**, 013809 (2000).
29. E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000); L. Viola, E. Knill and S. Lloyd, Phys. Rev. Lett. **85**, 3520 (2000).
30. S. De Filippo, Phys. Rev. **A62**, 052307 (2000).
31. P. Zanardi, Phys. Rev. **A63**, 12301 (2001).
32. C. P. Yang and J. Gea-Banacloche, Phys. Rev. **A63**, 022311 (2001).
33. M. Grassl, Th. Beth, and T. Pellizzari, Phys. Rev. **A56**, 33 (1997).
34. N. J. Cerf and Richard Cleve, Phys. Rev. **A56**, 1721 (1997).
35. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, England, 2001.
36. W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. **A62**, 062314 (2000).
37. T. Pellizzari, Phys. Rev. Lett. **79**, 5242 (1997).
38. P. W. Shor, in *Proceedings of the 37th Symposium on Foundations of Computer Science*, IEEE, Los Alamitos, 1996, p. 56.
39. M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. **A59**, 1829 (1999).
40. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, IEEE, New York, 1984; C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).