Pauli Exchange Errors in Quantum Computation

Mary Beth Ruskai
Department of Mathematics, University of Massachusetts Lowell, Lowell, Massachusetts 01854
(Received 30 June 1999)

In many physically realistic models of quantum computation, Pauli exchange interactions cause a subset of 2-qubit errors to occur as a first-order effect of couplings within the computer, even in the absence of interactions with the computer's environment. We give an explicit 9-qubit code that corrects both Pauli exchange errors and all 1-qubit errors.

PACS numbers: 03.67.Lx

Most schemes for fault tolerant quantum computation treat single-qubit errors as the primary error event, and correct multiple-qubit errors as a higher-order side effect. Discussions of quantum error correction also often ignore the Pauli exclusion principle and permutational symmetry of the states of multiqubit systems. This can often be justified approximately by considering the full wave function, including spatial as well as spin components. However, an analysis of these more complete wave functions suggests that exchange errors, in which interactions between identical particles cause an error in two qubits simultaneously, may be an important error mechanism in some circumstances. Moreover, because they result from interactions within the quantum computer, exchange errors cannot be reduced by better isolating the quantum computer from its environment. After describing the physical mechanism of exchange errors, we discuss codes designed specifically to correct them.

A (pure) state of a quantum mechanical particle with spin q corresponds to a one-dimensional subspace of the Hilbert space $\mathcal{H} = \mathbf{C}^{2q+1} \otimes L^2(\mathbf{R}^3)$ and is typically represented by a vector in that subspace. The state of a system of N such particles is then represented by a vector $\Psi(x_1, x_2, \ldots, x_N)$ in $\mathcal{H}^N$. However, when dealing with identical particles, Ψ must also satisfy the Pauli principle, i.e., it must be symmetric or antisymmetric under exchange of the coordinates $x_j \leftrightarrow x_k$, depending on whether the particles in question are bosons (e.g., photons) or fermions (e.g., electrons). In either case, we can write the full wave function in the form

$$\Psi(x_1,x_2,\ldots,x_N) = \sum_k \chi_k(s_1,s_2,\ldots,s_N)\Phi_k(\mathbf{r}_1,\mathbf{r}_2,\ldots,\mathbf{r}_N)\,, \qquad (1)$$

where the "space functions" Φ_k are elements of $L^2(\mathbf{R}^{3N})$, the "spin functions" χ_k are in $[\mathbf{C}^{2q+1}]^N$ and $x_k = (\mathbf{r}_k, s_k)$ with $\mathbf{r}_k$ a vector in $\mathbf{R}^3$ and the so-called "spin coordinates" s_k in $0, 1, \ldots, 2q$. [In the parlance of quantum computing a spin state χ is a (possibly entangled) N-qubit state.] It is not necessary that χ and Φ each satisfy the Pauli principle; indeed, when $q = \frac{1}{2}$ so that $2q + 1 = 2$ and we are dealing with $\mathbf{C}^2$, it is *not* possible for χ to be antisymmetric when $N \geq 3$. Instead, we expect that χ and Φ satisfy certain duality conditions which guarantee that Ψ has the correct permutational symmetry.

With this background, we now restrict attention to the important special case in which $q = \frac{1}{2}$ yielding two spin states labeled so that $s = 0$ corresponds to $|0\rangle$ and $s = 1$ corresponds to $|1\rangle$, and the particles are electrons so that Ψ must be antisymmetric. We present our brief for the importance of Pauli exchange errors by analyzing the 2-qubit case in detail, under the additional simplifying assumption that the Hamiltonian is spin-free. Analogous considerations apply in other cases.

For multiparticle states, it is sometimes convenient to replace $|0\rangle$ and $|1\rangle$ by $\uparrow$ and $\downarrow$, respectively. The notation $|01\rangle$ describes a 2-qubit state in which the particle in the first qubit has spin "up" ($\uparrow$) and that in the second has spin "down" ($\downarrow$). What does it mean for a particle to "be" in a qubit? A reasonable answer is that each qubit is identified by the spatial component of its wave function $f_A(\mathbf{r})$, where $A, B, C, \ldots$ label the qubits and wave functions for different qubits are orthogonal. Thus,

$$|01\rangle = \frac{1}{\sqrt{2}}[f_A(\mathbf{r}_1)\uparrow f_B(\mathbf{r}_2)\downarrow - f_B(\mathbf{r}_1)\downarrow f_A(\mathbf{r}_2)\uparrow]. \qquad (2)$$

Notice that the electron whose spatial function is f_A always has spin up regardless of whether its coordinates are labeled by 1 or 2. We can rewrite (2) as

$$|01\rangle = \frac{1}{\sqrt{2}}[\chi^+(s_1,s_2)\phi^-(\mathbf{r}_1,\mathbf{r}_2) + \chi^-(s_1,s_2)\phi^+(\mathbf{r}_1,\mathbf{r}_2)], \qquad (3)$$

where $\chi^\pm = \frac{1}{\sqrt{2}}[\uparrow\downarrow \pm \downarrow\uparrow]$ denotes the indicated Bell states and $\phi^\pm = \frac{1}{\sqrt{2}}[f_A(\mathbf{r}_1)f_B(\mathbf{r}_2) \pm f_B(\mathbf{r}_1)f_A(\mathbf{r}_2)]$.

The assumption of a spin-free Hamiltonian H, implies that the time development of (2) is determined by $e^{-iHt}\phi^\pm$, and the assumption that the particles are electrons implies that H includes a term corresponding to the $\frac{1}{r_{12}} \equiv \frac{1}{|\mathbf{r}_1 - \mathbf{r}_2|}$ electron-electron interaction. The Hamiltonian must be symmetric so that the states $\phi^\pm$ retain their permutational symmetry; however, the interaction term implies that they will not retain the simple form of symmetrized (or antisymmetrized) product states. Hence, after some time the states $\phi^\pm$ evolve into

 0031-9007/00/85(1)/194(4)$15.00

$$\Phi^- = \sum_{m<n} c_{mn} \frac{1}{\sqrt{2}} [f_m(\mathbf{r}_1) f_n(\mathbf{r}_2) - f_n(\mathbf{r}_1) f_m(\mathbf{r}_2)], \quad (4a)$$

$$\Phi^+ = \sum_{m\leq n} d_{mn} \frac{1}{\sqrt{2}} [f_m(\mathbf{r}_1) f_n(\mathbf{r}_2) + f_n(\mathbf{r}_1) f_m(\mathbf{r}_2)]. \quad (4b)$$

where f_m denotes any orthonormal basis whose first two elements are f_A and f_B, respectively. There is no reason to expect that $c_{mn} = d_{mn}$ in general. On the contrary, only the symmetric sum includes pairs with $m = n$. Hence if one $d_{mm} \neq 0$, then one must have some $c_{mn} \neq d_{mn}$. Inserting (4) into (3) yields

$$\begin{aligned} e^{-iHt}|01\rangle &= \frac{c_{AB} + d_{AB}}{2} [f_A(\mathbf{r}_1)\uparrow f_B(\mathbf{r}_2)\downarrow - f_B(\mathbf{r}_1)\downarrow f_A(\mathbf{r}_2)\uparrow] \\ &\quad + \frac{c_{AB} - d_{AB}}{2} [f_B(\mathbf{r}_1)\uparrow f_A(\mathbf{r}_2)\downarrow - f_A(\mathbf{r}_1)\downarrow f_B(\mathbf{r}_2)\uparrow] + \Psi^{\text{Remain}} \\ &= \frac{c_{AB} + d_{AB}}{2} |01\rangle + \frac{c_{AB} - d_{AB}}{2} |10\rangle + \Psi^{\text{Remain}}, \end{aligned} \quad (5)$$

where Ψ^{Remain} is orthogonal to $\phi^{\pm}$.

A measurement of qubit A corresponds to projecting onto f_A. Hence a measurement of qubit A on the state (3) yields spin up with probability $\frac{1}{4}|c_{AB} + d_{AB}|^2$ and spin down with probability $\frac{1}{4}|c_{AB} - d_{AB}|^2$, and zero with probability $\|\Psi^{\text{Remain}}\|^2$. Note that the *full* wave function is *necessarily* an *entangled* state and that the measurement process leaves the system in state $|10\rangle$ or $|01\rangle$ with probabilities $\frac{1}{4}|c_{AB} \pm d_{AB}|^2$, respectively, i.e., subsequent measurement of qubit B always gives the opposite spin. With probability $\frac{1}{4}|c_{AB} - d_{AB}|^2$ the initial state $|10\rangle$ has been converted to $|01\rangle$.

Although the probability of this may be small, it is *not* zero. Precise estimates require a more detailed model of the actual experimental implementation. However, it would seem that any implementation which provides a mechanism for 2-qubit gates would necessarily permit some type of interaction between particles in different qubits. Because one expects qubits to be less isolated from each other than from the external environment, Pauli exchange errors seem to merit more attention.

If the implementation involves charged particles, whether electrons or nuclei, then the interaction includes a contribution from the $\frac{1}{r_{12}}$ Coulomb potential which is known to have long-range effects. This suggests that implementations involving neutral particles, such as the Briegel *et al.* proposal [1] using optical lattices, may be advantageous for minimizing exchange errors.

A Pauli exchange error is a special type of "2-qubit" error which has the same effect as "bit flips" if (and *only* if) they are different. The exchange of bits j and k is equivalent to acting on a state with the operator

$$E_{jk} = \tfrac{1}{2}(I_j \otimes I_k + Z_j \otimes Z_k + X_j \otimes X_k + Y_j \otimes Y_k),$$

where X_j, Y_j, and Z_j denote the action of the Pauli matrices σ_x, σ_y, and σ_z, respectively, on the bit j.

As an example, we consider Pauli exchange errors in the simple 9-bit Shor code [2]:

$$|c_0\rangle = |\mathbf{000}\rangle + |\mathbf{011}\rangle + |\mathbf{101}\rangle + |\mathbf{110}\rangle, \quad (6a)$$

$$|c_1\rangle = |\mathbf{111}\rangle + |\mathbf{100}\rangle + |\mathbf{010}\rangle + |\mathbf{001}\rangle, \quad (6b)$$

where boldface denotes a triplet of 0's or 1's. It is clear that these code words are invariant under exchange of electrons within the 3-qubit triples $(1,2,3)$, $(4,5,6)$, or $(7,8,9)$. To see what happens when electrons in different triplets are exchanged, consider the exchange E_{34} acting on $|c_0\rangle$. This yields $|000\,000\,000\rangle + |001\,011\,111\rangle + |110\,100\,111\rangle + |111\,111\,000\rangle$ so that

$$\begin{aligned} E_{34}|c_0\rangle &= |c_0\rangle + Z_8|c_0\rangle + |001\,011\,111\rangle \\ &\quad + |110\,100\,111\rangle, \\ E_{34}|c_1\rangle &= |c_1\rangle - Z_8|c_1\rangle + |110\,100\,000\rangle \\ &\quad + |001\,011\,000\rangle. \end{aligned}$$

If $|\psi\rangle = a|c_0\rangle + b|c_1\rangle$ is a superposition of code words,

$$E_{34}|\psi\rangle = \tfrac{1}{2}(|\psi\rangle + Z_8|\tilde{\psi}\rangle) + \tfrac{1}{\sqrt{2}}|\gamma\rangle,$$

where $|\tilde{\psi}\rangle = a|c_0\rangle - b|c_1\rangle$ differs from ψ by a "phase error" on the code words and $|\gamma\rangle$ is orthogonal to the space of code words and single-bit errors. Thus, this code cannot reliably distinguish between an exchange error E_{34} and a phase error on any of the last three bits. This problem occurs because, if $E_{34}|c_0\rangle = \alpha|c_0\rangle + \beta|d_0\rangle$ with $|d_0\rangle$ orthogonal to $|c_0\rangle$, then $|d_0\rangle$ need not be orthogonal to $|c_1\rangle$.

In order to be able to correct a given class of errors, we first identify a set of basic errors e_p in terms of which all other errors can be written as linear combinations. In the case of unitary transformations on single-bit, or 1-qubit errors, this set usually consists of X_k, Y_k, Z_k ($k = 1, \ldots, n$), where n is the number of qubits in the code and X_k, Y_k, Z_k now denote $I \otimes I \otimes I \cdots \otimes \sigma_p \otimes \cdots \otimes I$, where σ_p denotes one of the three Pauli matrices acting on qubit k. If we let $e_0 = I$ denote the identity, then a sufficient condition for error correction is

$$\langle e_p C_i \mid e_q C_j \rangle = \delta_{ij}\delta_{pq}. \quad (7)$$

However, (7) can be replaced [3–5] by the weaker

$$\langle e_p C_i \mid e_q C_j \rangle = \delta_{ij} d_{pq}\,. \tag{8}$$

where the matrix D with elements d_{pq} is independent of i, j. When considering Pauli exchange errors, it is natural to seek codes which are invariant under some subset of permutations. This is clearly incompatible with (7) since some of the exchange errors will then satisfy $E_{jk}|C_i\rangle = |C_i\rangle$. Hence we will need to use (8).

The most common code words have the property that $|C_1\rangle$ can be obtained from $|C_0\rangle$ by exchanging all 0's and 1's. For such codes, it is not hard to see that $\langle C_1 \mid Z_k C_1\rangle = -\langle C_0 \mid Z_k C_0\rangle$ which is consistent with 8 if and only if it is identically zero. Hence even when using (8) rather than (7) it is necessary to require

$$\langle C_1 \mid Z_k C_1\rangle = -\langle C_0 \mid Z_k C_0\rangle = 0 \tag{9}$$

when the code words are related in this way.

We now present a 9-bit code which can handle both Pauli exchange errors and all 1-bit errors. It is based on the realization that codes which are invariant under permutations are impervious to Pauli exchange errors. Let

$$|C_0\rangle = |000\,000\,000\rangle + \frac{1}{\sqrt{28}} \sum_{\mathcal{P}} |111\,111\,000\rangle, \tag{10a}$$

$$|C_1\rangle = |111\,111\,111\rangle + \frac{1}{\sqrt{28}} \sum_{\mathcal{P}} |000\,000\,111\rangle, \tag{10b}$$

where $\sum_{\mathcal{P}}$ denotes the sum over all permutations of the indicated sequence of 0's and 1's, and it is understood that permutations which result in identical vectors are counted only once. This differs from the 9-bit Shor code in that *all* permutations of $|111\,111\,000\rangle$ are included, rather than only three. The normalization of the code words is $\langle C_i \mid C_i\rangle = 1 + \frac{1}{28}\binom{9}{3} = 4$.

The coefficient $1/\sqrt{28}$ is needed to satisfy (9). Simple combinatorics implies

$$\langle C_i \mid Z_k C_i\rangle = (-1)^i \left[1 - \frac{1}{3}\binom{9}{3}\frac{1}{28}\right] = 0\,.$$

Moreover,

$$\langle Z_k C_i \mid Z_\ell C_i\rangle = 1 + \delta_{k\ell}\binom{9}{3}\frac{1}{28} = 1 + 3\delta_{k\ell}\,. \tag{11}$$

The second term in (11) is zero when $k \neq \ell$ because of the fortuitous fact that there are exactly the same number of positive and negative terms. If, instead, we had used all permutations of κ 1's in n qubits, this term would be $\frac{(n-2\kappa)^2-n}{n(n-1)}\binom{n}{\kappa}$ when $k \neq \ell$.

Since all components of $|C_0\rangle$ have 0 or 6 bits equal to 1, any single-bit flip acting on $|C_0\rangle$ will yield a vector whose components have 1, 5, or 7 bits equal to 1 and is thus orthogonal to $|C_0\rangle$, to $|C_1\rangle$, to a bit flip acting on $|C_1\rangle$, and to a phase error on either $|C_0\rangle$ or $|C_1\rangle$. Similarly, a single-bit flip on $|C_1\rangle$ will yield a vector orthogonal to $|C_0\rangle$, to $|C_1\rangle$, to a bit flip acting on $|C_0\rangle$, and to a phase error on $|C_0\rangle$ or $|C_1\rangle$. However, single-bit flips on a given code word are not mutually orthogonal.

To find $\langle X_k C_i \mid X_\ell C_i\rangle$ when $k \neq \ell$, consider

$$\langle X_k(\nu_1\nu_2\cdots\nu_9) \mid X_\ell(\mu_1\mu_2\cdots\mu_9)\rangle\,. \tag{12}$$

where ν_i, μ_i are in $0, 1$. This will be nonzero only when $\nu_k = \mu_\ell = 0$ and $\nu_\ell = \mu_k = 1$, or $\nu_k = \mu_\ell = 1$ and $\nu_\ell = \mu_k = 0$, and the other $n - 2$ bits are equal. From $\sum_{\mathcal{P}}$ with κ of n bits equal to 1, there are $2\binom{n-2}{\kappa-1}$ such terms. Thus, for the code (10), there are 42 such terms which yield an inner product of $\frac{42}{28} = \frac{3}{2}$ when $k \neq \ell$. If we consider instead, $\langle Y_k C_i \mid X_\ell C_i\rangle = -i\langle X_k Z_k C_i \mid X_\ell C_i\rangle$ for $k \neq \ell$, it is not hard to see that exactly half of the terms analogous to (12) will occur with a positive sign and half with a negative sign, yielding a net inner product of zero. We also find $\langle Y_k C_i \mid X_k C_i\rangle = -i\langle X_k Z_k C_i \mid X_k C_i\rangle = -i\langle Z_k C_i \mid C_i\rangle = 0$ so that $\langle Y_k C_i \mid X_\ell C_i\rangle = 0$ for all k, ℓ. In addition $\langle Y_k C_i \mid Z_\ell C_i\rangle = -i\langle X_k Z_k C_i \mid Z_\ell C_i\rangle = 0$ for the same reason that $\langle X_k C_i \mid C_i\rangle = 0$.

These results imply that (8) holds and that the matrix D is block diagonal with the form

$$D = \begin{pmatrix} D_0 & 0 & 0 & 0 \\ 0 & D_X & 0 & 0 \\ 0 & 0 & D_Y & 0 \\ 0 & 0 & 0 & D_Z \end{pmatrix}, \tag{13}$$

where D_0 is the 37×37 matrix corresponding to the identity and the 36 exchange errors, and D_X, D_Y, D_Z are 9×9 matrices corresponding respectively to the X_k, Y_k, Z_k single-bit errors. One easily finds that $d_{pq}^0 = 4$ for all p, q. The 9×9 matrices D_X, D_Y, D_Z all have $d_{kk} = 4$ while, for $k \neq \ell$, $d_{k\ell} = 3/2$ in D_X and D_Y but $d_{k\ell} = 1$ in D_Z. Orthogonalization of this matrix is straightforward. Since D has rank $28 = 3 \times 9 + 1$, we are using only a $54 < 2^6$ dimensional subspace of our 2^9 dimension space.

The simplicity of codes which are invariant under permutations makes them attractive. However, there are few such codes. All code words necessarily have the form

$$\sum_{\kappa=0}^{n} a_\kappa \sum_{\mathcal{P}} |\underbrace{1\cdots1}_{\kappa}\,\underbrace{0\cdots0}_{n-\kappa}\rangle\,. \tag{14}$$

Condition (8) places some severe restrictions on the coefficient a_κ. For example, in (10) only a_0 and a_6 are nonzero in $|C_0\rangle$ and only a_3 and a_9 in $|C_1\rangle$. If we try to change this so that a_0 and a_3 are nonzero in $|C_0\rangle$ and a_6 and a_9 in $|C_1\rangle$, then it is *not* possible to satisfy (9).

The 5-bit code in [4–5] does not have the permutationally invariant form (14) because the code words include components of the form $\sum_{\mathcal{P}} \pm|11\,000\rangle$, i.e., not all terms in the sum have the same sign. The nonadditive 5-bit code in [7] requires sign changes in the $\sum_{\mathcal{P}} \pm|10\,000\rangle$ term. Since such sign changes seem needed to satisfy (9), it appears that 5-bit codes cannot handle Pauli exchange errors (although we have no proof).

However, permutational invariance, which is based on a one-dimensional representation of the symmetric group, is not the only approach to exchange errors. Our analysis of (6) suggests a construction which we first describe in an oversimplified form. Let $|c_0\rangle$, $|d_0\rangle$, $|c_1\rangle$, and $|d_1\rangle$ be four mutually orthogonal n-bit vectors such that $|c_0\rangle, |c_1\rangle$ form a code for 1 -bit errors and $|c_0\rangle, |d_0\rangle$ and $|c_1\rangle, |d_1\rangle$ are each bases of a two-dimensional representation of the symmetric group S_n. If $|d_0\rangle$ and $|d_1\rangle$ are also orthogonal to 1-bit errors on the code words, then this code can correct Pauli exchange errors as well as 1 -bit errors. If, in addition, the vectors $|d_0\rangle, |d_1\rangle$ also form a code isomorphic to $|c_0\rangle, |c_1\rangle$ in the sense that the matrix D in (8) is identical for both codes, then the code should also be able to correct products of 1-bit and Pauli exchange errors.

But the smallest (excluding one-dimensional) irreducible representations of the symmetric group for use with n-bit codes have dimension $n - 1$. Thus we will seek a set of $2(n - 1)$ mutually orthogonal vectors denoted $|C_0^m\rangle, |C_1^m\rangle$ $(m = 1, \ldots, n - 1)$ such that $|C_0^1\rangle, |C_1^1\rangle$ form a code for 1-bit errors and $|C_0^m\rangle$ $(m = 1, \ldots, n - 1)$ and $|C_1^m\rangle$ $(m = 1, \ldots, n - 1)$ each form the basis of the same irreducible representation of S_n. Such a code will be able to correct *all* errors which permute qubits, not just single exchanges. If, in addition, (8) is extended to

$$\langle e_p C_i^m \mid e_q C_j^{m'} \rangle = \delta_{ij} \delta_{mm'} d_{pq} \tag{15}$$

with the matrix $D = \{D_{pq}\}$ independent of both i and m, then this code will also be able to correct products of 1-bit errors and permutation errors.

If the basic error set has size N (i.e., $p = 0, 1, \ldots, N - 1$), then a two-word code requires codes which lie in a space of dimension at least $2N$. For the familiar case of single-bit errors $N = 3n + 1$ and, since an n-bit code word lies in a space of dimension 2^n, any code must satisfy $3n + 1 < 2^{n-1}$ or $n \geq 5$. There are $n(n - 1)/2$ possible single-exchange errors compared to $9n(n - 1)/2$ 2-bit errors of all types. Similar dimension arguments yield $2N = n^2 + 5n + 2 \leq 2^n$ or $n \geq 7$ for correcting both single-bit and single-exchange errors and $2N = 9n(n - 1) + 2(3n + 1) \leq 2^n$ or $n \geq 10$ for correcting all 1- and 2-bit errors. The shortest code known [4] which can do the latter has $n = 11$. Correcting Pauli exchange errors can be done with shorter codes than required to correct all 2-bit errors.

However, this simple dimensional analysis need not yield the best bounds when exchange errors are involved. Consider the simple code $|C_0\rangle = |000\rangle, |C_1\rangle = |111\rangle$ which is optimal for single-bit flips (but cannot correct phase errors). In this case $N = n + 1$, and $n = 3$ yields equality in $2(n + 1) \leq 2^n$. But, since this code is invariant under permutations, the basic error set can be expanded to include all six exchange errors E_{jk} for a total of $N = 10$ without increasing the length of the code words.

In the construction proposed above, correction of exchange and 1-bit errors would require a space of dimension $2(n - 1)(3n + 1) \leq 2^n$ or $n \geq 9$. If codes satisfying (15) exist, they could correct *all* permutation errors as well as products of permutations and 1-bit errors. Exploiting permutational symmetry may have a big payoff.

Although codes which can correct Pauli exchange errors will be larger than the minimal 5-qubit codes proposed for single-bit error correction, this may not be a serious drawback. For implementations of quantum computers which have a grid structure (e.g., solid state or optical lattices) it may be natural and advantageous to use 9-qubit codes which can be implemented in 3×3 blocks [see, e.g., Ref. [1]]. However, codes larger than 9-bits may be impractical for a variety of reasons. Hence it is encouraging that both the code (10) and the proposed construction above do not require $n > 9$.

Several more complex coding schemes have been proposed [3,8–12] for multiple error correction. It may be worth investigating whether or not the codes proposed here can be used advantageously in some of these schemes, such as those [8] based on hierarchical nesting. Since the code (10) can already handle multiple exchange errors (and the proposed construction of some additional multiple errors), concatenation of one of our proposed 9-bit codes with itself will contain some redundancy and concatenation with a 5-bit code may be worth exploring.

Whether or not any 7-bit codes exist which can handle Pauli exchange errors is another open question, which we leave as a challenge for coding theorists.

It is a pleasure to thank Professor Eric Carlen for a useful comment and both Professor Chris King and Professor Harriet Pollatsek for several helpful discussions and comments on earlier drafts. This research was partially supported by National Science Foundation Grant No. DMS-97-06981 and Army Research Office Grant No. DAAG55-98-1-0374.

[1] H. J. Briegel, T. Calarco, D. Jaksch, J. I. Cirac, and P. Zoller, quant-ph/9904010.
[2] P. W. Shor, Phys. Rev. A **52**, 2493 (1995).
[3] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[4] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997); IEEE Trans. Inf. Theory (to be published).
[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[6] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[7] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **79**, 953 (1997).
[8] E. Knill and R. Laflamme, quant-ph/9608012; see J. Preskill [Phys. Today **52**, No. 6, 24 (1999)] for a brief discussion and additional references.
[9] A. Y. Kitaev, quant-ph/9707021.
[10] A. M. Steane, Nature (London) **399**, 124 (1999).
[11] E. Knill, R. Laflamme, and L. Viola, quant-ph/9908066.
[12] D. A. Lidar *et al.*, Phys. Rev. Lett. **81**, 2594 (1998); **82**, 4556 (1999); see quant-ph/9907096 for an extension of their decoherence free subspace approach to exchange errors.