Pauli Exchange Errors in Quantum Computation

Mary Beth Ruskai *
Department of Mathematics
University of Massachusetts Lowell
Lowell, MA 01854 USA

June 29, 1999

Abstract

We argue that a physically reasonable model of fault-tolerant computation requires the ability to correct a type of two-qubit error which we call Pauli exchange errors as well as one qubit errors. We give an explicit 9-qubit code which can handle both Pauli exchange errors and all one-bit errors.

Most discussions of quantum error correction assume, at least implicitly, that errors result from interactions with the environment and that single qubit errors are much more likely than two qubit errors. Most discussions also ignore the Pauli exclusion principle and permutational symmetry of the states describing multi-qubit systems. Although this can be justified by consideration of the full wave function, including spatial as well as spin components, an analysis of these more complete wave functions suggests that an important source of error has been ignored. Exchange of identical particles and interactions between qubits give rise to a type of error, not seen classically, in which a *single* exchange error can affect two qubits.

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

*Partially supported by National Science Foundation Grant DMS-97-06981 and Army Research Office Grant DAAG55-98-1-0374

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 anti-symmetric 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

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

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 $\mathbf{r}$ with a vector in $\mathbf{R}^3$ and the so-called "spin coordinate" s_k in $0, 1, \ldots 2q$. [In the parlance of quantum computing a spin states 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 anti-symmetric when $N \geq 3$. Instead, we expect that χ and Φ satisfy certain duality conditions which guarantee that Ψ has the correct permutational symmetry. (For example, antisymmetric Ψ arise when the states χ_k and Φ_k form bases for irreducible representations of the symmetric group with dual Young tableaus.)

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 anti-symmetric. Although analogous considerations apply in other cases, the additional component of electron-electron interaction implies that Pauli exchange errors are particularly important in this case. We present our brief for the importance of Pauli exchange errors by analyzing the two-qubit case in detail. For multi-particle states, it is sometimes convenient to replace $|0\rangle$ and $|1\rangle$ by $\uparrow$ and $\downarrow$ respectively.

Thus, the notation $|01\rangle$ describes a two-qubit state in which the particle in the first qubit has spin "up" ($\uparrow$) and that in the second qubit spin "down" ($\downarrow$). What does it mean for a particle to "be" in a qubit? A reasonable model is that each qubit corresponds to some type of well in which a particle is trapped if the spatial component of its wave function is $f_A(\mathbf{r})$ where $A, B, C \ldots$ label the wells and wave functions for different wells are orthogonal. Thus, we write

$$|01\rangle = \frac{1}{\sqrt{2}}\Big([f_A(\mathbf{r_1})\uparrow]\,[f_B(\mathbf{r_2})\downarrow] - [f_B(\mathbf{r_1})\downarrow]\,[f_A(\mathbf{r_2})\uparrow]\Big). \qquad (2)$$

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 this as

$$|01\rangle = \frac{1}{\sqrt{2}}\left[\chi^+\phi^- + \chi^-\phi^+\right] \qquad (3)$$

where $\chi^{\pm}(s_1, s_2) = \frac{1}{\sqrt{2}}\left[|01\rangle \pm |10\rangle\right]$ denotes the indicated Bell states and $\phi^{\pm}(\mathbf{r_1}\mathbf{r_2}) = \frac{1}{\sqrt{2}}\left[f_A(\mathbf{r_1})f_B(\mathbf{r_2}) \pm f_B(\mathbf{r_1})f_A(\mathbf{r_2})\right]$.

If the Hamiltonian H is spin-free, then the time development of (2) is determined by $e^{iHt}\phi^{\pm}$. Since we assumed the particles are electrons, H must include a term corresponding to the $\frac{1}{r_{12}} \equiv \frac{1}{|\mathbf{r_1}-\mathbf{r_2}|}$ electron-electron interaction. Since the Hamiltonian must be symmetric, the states $\phi^{\pm}$ retain their permutational symmetry; however, the presence of the electron-electron interaction suggests that they cannot retain the simple form of symmetrized (or anti-symmetrized) product states. Hence, after some time the states $\phi^{\pm}$ evolve into

$$\begin{aligned}
\Phi^-(\mathbf{r_1}, \mathbf{r_2}) &= \sum_{m<n} c_{mn}\frac{1}{\sqrt{2}}\left[f_m(\mathbf{r_1})f_m(\mathbf{r_2}) - f_n(\mathbf{r_1})f_m(\mathbf{r_2})\right] \\
\Phi^+(\mathbf{r_1}, \mathbf{r_2}) &= \sum_{m\leq n} d_{mn}\frac{1}{\sqrt{2}}\left[f_m(\mathbf{r_1})f_m(\mathbf{r_2}) + f_n(\mathbf{r_1})f_m(\mathbf{r_2})\right].
\end{aligned}$$

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 this in (3) yields

$$\begin{aligned}
e^{iHt}|01\rangle &= (c_{AB} + d_{AB})\Big([f_A(\mathbf{r_1})\uparrow]\,[f_B(\mathbf{r_2})\downarrow] - [f_B(\mathbf{r_1})\downarrow]\,[f_A(\mathbf{r_2})\uparrow]\Big) \\
&\quad +(c_{AB} - d_{AB})\Big([f_B(\mathbf{r_1})\uparrow]\,[f_A(\mathbf{r_2})\downarrow] - [f_A(\mathbf{r_1})\downarrow]\,[f_B(\mathbf{r_2})\uparrow]\Big) \\
&\quad +\Psi^{\text{Remain}} \\
&= (c_{AB} + d_{AB})|01\rangle + (c_{AB} - d_{AB})|10\rangle + \Psi^{\text{Remain}} \qquad (4)
\end{aligned}$$

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

A measurement of qubit-A (or B) corresponds to projecting onto f_A (or f_B). Hence a measurement of qubit-A on the state (3) yields spin "up" with with probability $|c_{AB} + d_{AB}|^2$ and spin down with probability $|c_{AB} - d_{AB}|^2$, 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 $|c_{AB} \pm d_{AB}|^2$ respectively, i.e., subsequent measurement of qubit-B always gives the opposite spin. With probability $|c_{AB} - d_{AB}|^2$ the initial state $|10\rangle$ has been converted to $|01\rangle$

Although the probability of this is small, it is not zero. Precise estimates would require a more detailed model of the actual experimental implementation. However, it would seems that any implementation which provides a mechanism for two-qubit gates would necessarily involve a model in which the interactions between particles in different qubits is at least as large as their interaction with the environment. Since the environment is assumed to be the cause of one-bit errors, Pauli exchange errors seems at least as likely and worthy of more attention.

If the implementation involves charged particles, such as electrons in ion traps, 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 Briegel, et al's proposal [1] using optical lattices, may be advantageous for minimizing exchange errors.

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

$$E_{jk} = \tfrac{1}{2}\Big(I_j \otimes I_k + Z_j \otimes Z_k + X_j \otimes X_k + Y_j \otimes Y_k\Big) \tag{5}$$

where X_j, Y_j, Z_j denote the action of the Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ respectively on the bit j. One can easily verify that

$$\begin{aligned} \tfrac{1}{2}\Big(I_j \otimes I_k + Z_j \otimes Z_k\Big)|s_1, s_2 \ldots s_N\rangle &= \delta_{s_j,s_k} \\ \tfrac{1}{2}\Big(X_j \otimes X_k + Y_j \otimes Y_k\Big)|s_1, s_2 \ldots s_N\rangle &= \delta_{s_j,s_k+1} = 1 - \delta_{s_j,s_k} \end{aligned}$$

As an example, we consider Pauli exchange errors in the simple 9-bit code of Shor [7]

$$|c_0\rangle = \tfrac{1}{2}\Big(|000000000\rangle + |000111111\rangle + |111000111\rangle + |111111000\rangle\Big)$$

$$
\begin{aligned}
&= \tfrac{1}{2}\Big(|\mathbf{000}\rangle + |\mathbf{011}\rangle + |\mathbf{101}\rangle + |\mathbf{110}\rangle\Big) && (6)\\
|c_1\rangle &= \tfrac{1}{2}\Big(|111111111\rangle + |111000000\rangle + |000111000\rangle + |000000111\rangle\Big)\\
&= \tfrac{1}{2}\Big(|\mathbf{111}\rangle + |\mathbf{100}\rangle + |\mathbf{010}\rangle + |\mathbf{001}\rangle\Big) && (7)
\end{aligned}
$$

where we have used boldface to denote 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}.

$$
\begin{aligned}
E_{34}|c_0\rangle &= \tfrac{1}{2}\Big(|000000000\rangle + |001011111\rangle + |110100111\rangle + |111111000\rangle\Big)\\
&= \tfrac{1}{2}\Big(|c_0\rangle + Z_8|c_0\rangle + |001011111\rangle + |110100111\rangle\Big)\\
E_{34}|c_1\rangle &= \tfrac{1}{2}\Big(|111111111\rangle + |110100000\rangle + |001011000\rangle + |000000111\rangle\Big)\\
&= \tfrac{1}{2}\Big(|c_1\rangle - Z_8|c_1\rangle + |110100000\rangle + |001011000\rangle\Big)
\end{aligned}
$$

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

$$
E_{34}|\psi\rangle = \tfrac{1}{2}\Big(|\psi\rangle + Z_2|\tilde{\psi}\rangle\Big) + \frac{1}{\sqrt{2}}|\gamma\rangle
$$

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 codewords and single bit errors. Therefore, this code cannot reliably distinguish between an exchange error E_{34} and a phase error on any of the last 3 bits. This problem arises because if we write

$$
E_{34}|c_0\rangle = \tfrac{1}{2}\Big(|c_0\rangle + |d_0\rangle\Big) \tag{8}
$$

then $|d_0\rangle = \frac{1}{2}\Big(|001011111\rangle + |110100111\rangle - |000111111\rangle - |111000111\rangle\Big)$ is not orthogonal to the codewords.

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 one-qubit errors, this set usually consists of $X_k, Y_k, Z_k \quad (k = 1 \ldots n)$ where n is the number of qubits in the code and X_k, Y_k, Z_k now denote $I \otimes I \otimes I \ldots \otimes \sigma_p \otimes \ldots \otimes I$ 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

$$\langle e_p C_i | e_q C_j \rangle = \delta_{ij} \delta_{pq} \tag{9}$$

However, this condition is not necessary and can be replaced [4] by the weaker condition

$$\langle e_p C_i | e_q C_j \rangle = \delta_{ij} d_{pq} \tag{10}$$

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 (9) since some of the exchange errors will then satisfy $E_{jk}|C_i\rangle = |C_i\rangle$. Hence we will need to use (10).

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 $\langle C_1 | Z_k C_1 \rangle = -\langle C_0 | Z_k C_0 \rangle$ which is consistent with (10) if and only if it is identically zero. Hence even when using (10) rather than (9) it is necessary to require

$$\langle C_1 | Z_k C_1 \rangle = -\langle C_0 | Z_k C_0 \rangle = 0 \tag{11}$$

when the code words are related in this complementary way.

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

$$\begin{aligned} |C_0\rangle &= |000000000\rangle + \frac{1}{\sqrt{28}} \sum_{\mathcal{P}} |111111000\rangle \\ &= |\mathbf{000}\rangle + \frac{1}{\sqrt{28}} \sum_{\mathcal{P}} |\mathbf{100}\rangle \end{aligned} \tag{12}$$

$$\begin{aligned} |C_1\rangle &= |111111111\rangle + \frac{1}{\sqrt{28}} \sum_{\mathcal{P}} |000000111\rangle \\ &= |\mathbf{111}\rangle + \frac{1}{\sqrt{28}} \sum_{\mathcal{P}} |\mathbf{011}\rangle \end{aligned} \tag{13}$$

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 we count permutations which result in identical vectors only once. As before, boldface denotes a triple , but $\sum_{\mathcal{P}}$ includes permutations between triples (rather than *of* triples). This differs from the 9-bit Shor code in that *all* permutations of $|111111000\rangle$ are included, rather than only three. The normalization of the code words is $\langle C_i|C_i\rangle = 1 + \frac{1}{\sqrt{28}} \begin{pmatrix} 9 \\ 3 \end{pmatrix} = 4.$

The coefficient $1/\sqrt{28}$ is needed to satisfy (11). Simple combinatorics implies

$$\langle C_i|Z_k C_i\rangle = (-1)^i \left[1 - \frac{1}{3}\begin{pmatrix} 9 \\ 3 \end{pmatrix}\frac{1}{28}\right] = 0.$$

Moreover,

$$\langle Z_k C_i|Z_\ell C_i\rangle = 1 + \delta_{k\ell}\begin{pmatrix} 9 \\ 3 \end{pmatrix}\frac{1}{28} = 1 + 3\delta_{k\ell}. \tag{14}$$

The second term in (14) 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 $\frac{(n-2\kappa)^2 - n}{n(n-1)}\begin{pmatrix} n \\ \kappa \end{pmatrix}$ 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 $\langle X_k C_i|X_\ell C_i\rangle$ when $k \neq \ell$, consider

$$\langle X_k\ (\nu_1\nu_2\ldots\nu_9)|X_\ell\ (\mu_1\mu_2\ldots\mu_9)\rangle. \tag{15}$$

where ν_i, μ_i are in $0, 1$. This will be nonzero only when $\nu_k = \nu_\ell = 0,\ \ \nu_\ell = \mu_k = 1$ or $\nu_k = \nu_\ell = 1,\ \ \nu_\ell = \mu_k = 0$ and the other $n-2$ bits are equal. From $\sum_{\mathcal{P}}$ with κ of n bits equal to 1, there are $2\begin{pmatrix} n-2 \\ \kappa-1 \end{pmatrix}$ such terms. Thus, for the code (12), there are 42 such terms which yields an inner product of $\frac{42}{28} = \frac{3}{2}$ when $k \neq \ell$.

If we consider instead,

$$\langle Y_k C_i | X_\ell C_i \rangle = -i \langle X_k Z_k C_i | X_\ell C_i \rangle \tag{16}$$

for $k \neq \ell$ it is not hard to see that exactly half of the terms analogous to (15) will occur with a positive sign and half with a negative sign, yielding a net inner product of zero in (16). We also find

$$\langle Y_k C_i | X_k C_i \rangle = -i \langle X_k Z_k C_i | X_k C_i \rangle = -i \langle Z_k C_i | C_i \rangle = 0 \tag{17}$$

so that $\langle Y_k C_i | X_\ell C_i \rangle = 0$ for all k, ℓ. In addition

$$\langle Y_k C_i | Z_\ell C_i \rangle = -i \langle X_k Z_k C_i | Z_\ell C_i \rangle = 0 \tag{18}$$

for the same reason that $\langle X_k C_i | C_i \rangle = 0$.

These results imply that imply (10) holds and that the matrix D is block diagonal with the form

$$D = \begin{pmatrix} D_0 & 0 & 0 & 0 \\ 0 & D_X & 0 & 0 \\ 0 & 0 & D_Y & 0 \\ 0 & 0 & 0 & D_Z \end{pmatrix} \tag{19}$$

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 $d^0_{pq} = 4$ for all p, q. The 9×9 matrices D_X, D_Y, D_Z all have the form

$$d_{k\ell} = \begin{cases} \alpha = 4 & \text{for} \quad k = \ell \\ \beta & \text{for} \quad k \neq \ell \end{cases} \tag{20}$$

with $\beta = 3/2$ in D_X and D_Y and $\beta = 1$ in D_Z. Orthogonalization of this matrix is straightforward. Since D has rank $28 = 3 \cdot 9 + 1$, i.e., we are using only a $54 < 2^6$-dimensional subspace of our 2^9 dimension space or 28 mutually orthogonal subspaces.

The simplicity of codes which are impervious to Pauli exchange errors because they are invariant under permutations makes them are attractive. However, there are few such codes. All code words necessarily have the form

$$\sum_{\kappa=0}^{n} a_\kappa \sum_{\mathcal{P}} |\underbrace{1 \ldots 1}_{\kappa} \underbrace{0 \ldots 0}_{n-\kappa}\rangle. \tag{21}$$

Condition (10) places some severe restrictions on the coefficient a_κ. For example, in (12) only a_0 and a_6 are non-zero 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 non-zero in $|C_0\rangle$ and a_6 and a_9 in $|C_1\rangle$, then it is *not* possible to satisfy (11).

The 5-bit code in [4, 5, 2] does not quite have the form (21). Instead

$$\begin{aligned} |C_0\rangle &= |00000\rangle + \sum_{\mathcal{P}} \pm|11000\rangle + \sum_{\mathcal{P}} |11110\rangle \\ |C_1\rangle &= |11111\rangle + \sum_{\mathcal{P}} \pm|11100\rangle + \sum_{\mathcal{P}} |10000\rangle \end{aligned}$$

These code words are not permutationally invariant because the components of $\sum_{\mathcal{P}} \pm|11000\rangle$ and $\sum_{\mathcal{P}} \pm|11100\rangle$ do not all have the same sign. This is needed to satisfy (11). The non-additive 5-bit code in [6] also requires sign changes in the $\sum_{\mathcal{P}} |10000\rangle$ term. We do not believe that 5-bit codes can handle Pauli exchange errors, but have no proof.

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

If (9) is required and 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 example, 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 $\frac{n(n-1)}{2}$ possible single exchange errors. Hence, the basic error set for correcting both single bit and single exchange errors will have $N = \frac{1}{2}(n^2 + 5n + 2)$ elements and the condition $2N \leq 2^n$ implies $n \geq 7$. Codes of the generalized stabilizer type proposed above will require a space of dimension $4N$. Hence, one needs $4(3n + 1) \leq 2^n$ which implies $n \geq 7$. To correct *all* two-bit errors as well as one-bit errors, the basic error set will have $N = \frac{9n(n-1)}{2} + 3n + 1 = \frac{1}{2}(9n^2 - 3n + 2)$ elements which requires $n \geq 10$. Thus it appears that correcting Pauli exchange errors can be done with shorter codes than correcting all two-bit errors. Moreover, further reduction in size may be possible.

Consider the simple codes

$$
\begin{array}{lll}
 & |C_0\rangle = |000\rangle & |C_1\rangle = |111\rangle \\
\text{and} & & \\
 & |C_0\rangle = |000\rangle + \sum_{\mathcal{P}} |110\rangle & |C_1\rangle = |111\rangle + \sum_{\mathcal{P}} |011\rangle
\end{array}
$$

It is well-known that the first can correct single bit flips, but not phase errors; the second single phase errors, but not bit flips. In the first case, the basic error set is I, X_1, X_2, X_3 and in the second I, Z_1, Z_2, Z_3. Hence, in both cases, N $= 4$, and since $n = 3$ satisfies $2n = 8 = 2^n$ one would not expect to be able to handle additional errors. However, both codes are invariant under permutations. Hence in both cases, basic error set can be expanded to include all 6 exchange errors E_{jk} for a total of $N = 10$ without increasing the size of the code words. Thus, the minimal size analysis when two-bit or exchange errors are included does not seem straightforward. If one requires that code words be invariant under some permutation, that constraint would appear to increase the size of the space. However, some permutational invariance may hold accidentally.

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 cold atoms) it may be natural and advantageous to use 9-qubit codes codes which can be implemented in 3×3 blocks. See [1] for further discussion of this point.

Whether or not any 7-bit codes exist which can handle Pauli exchange errors – either via permutational invariance or the generalization of stabilizer codes suggest above – is an open question. We leave the actual construction of such 7-bit codes as a challenge for coding theorists.

Acknowledgment It is a pleasure to thank Professor Eric Carlen for a useful comment and Professor Chris King for several helpful discussions and comments on a draft of this manuscript.

References

[1] H.J. Briegel, T. Calarco, D. Jaksch, J.I. Cirac, and P. Zoller "Quantum Computing with Neutral Atoms" lanl preprint quant-ph/9904010.

[2] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin and W.K. Wooters, "Mixed State Entanglement and Quantum Error Correction" *Phys. Rev. A* **54**, 3824–3851 (1996).

[3] R. Calderbank and P. Shor, "Good quantum error-correcting codes exist" *Phys. Rev. A* **54**, 1098–1106 (1996).

[4] R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum Error Correction and Orthogonal Geometry" *Phys. Rev. Lett.* **78**, 405–408 (1997); 'Quantum Error Correction via Codes Over $GF(4)$" *IEEE Trans. Info. Theory* (in press).

[5] R. Laflamme, C. Miquel, J.P. Paz, W.H. Zurek, "Perfect Quantum Error Correction Code" *Phys. Rev. Lett.* **77**, 198–201 (1996).

[6] E.M. Rains, R. H. Hardin, P.W. Shor and N.J.A. Sloane, "A Nonadditive Quantum Code" *Phys. Rev. Lett.* **79**, 953–954 (1997).

[7] P. Shor, "Scheme for reducing decoherence in quantum computer memory" *Phys. Rev. A* **52**, 2493-2496 (1995).

[8] A.M. Steane, "Error Correcting Codes in Quantum Theory" *Phys. Rev. Lett.* **77**, 793-797 (1996).