Quantum Error Correction and Orthogonal Geometry

A. R. Calderbank,[1] E. M. Rains,[2] P. W. Shor,[1] and N. J. A. Sloane[1]
[1] *AT&T Labs—Research, Murray Hill, New Jersey, 07974*
[2] *Institute for Defense Analyses, Princeton, New Jersey, 08540*

A group theoretic framework is introduced that simplifies the description of known quantum error-correcting codes and greatly facilitates the construction of new examples. Codes are given which map 3 qubits to 8 qubits correcting 1 error, 4 to 10 qubits correcting 1 error, 1 to 13 qubits correcting 2 errors, and 1 to 29 qubits correcting 5 errors.

PACS: 03.65.Bz

A quantum error-correcting code is a way of encoding quantum states into qubits (two-state quantum systems) so that error or decoherence in a small number of individual qubits has little or no effect on the encoded data. The existence of quantum error-correcting codes was discovered only recently [1]. Although the subject is relatively new, a large number of papers on quantum error correction have already appeared. Many of these describe specific examples of codes [1–9]. However, the theoretical aspects of these papers have been concentrated on properties and rates of the codes [7,10–12], rather than on recipes for constructing them. This letter introduces a unifying framework which explains all the codes discovered to date and greatly facilitates the construction of new examples.

The basis for this unifying framework is group theoretic. It rests on the structure of certain finite subgroups $E \subset L$ in $O(2^n)$ and $E' \subset L'$ in $U(2^n)$ [13]. Since the natural setting for quantum mechanics is complex space, it might appear more appropriate to focus on the complex groups E' and L'. However, we shall begin by discussing the real groups E and L, since their structure is easier to understand and they are sufficient for the construction of the known quantum error-correcting codes. We will first construct the subgroup E of $O(2^n)$. This group E provides a bridge between quantum error-correcting codes in Hilbert space and binary orthogonal geometry. We then construct the larger subgroup $L \subset O(2^n)$ as the normalizer of E.

The group E is the group of tensor products $\pm w_1 \otimes \ldots \otimes w_n$ where each w_j is either the identity or one of the Pauli matrices σ_x, σ_y or σ_z applied to the jth qubit. Mathematically, the group E is realized as an irreducible group of 2^{1+2n} orthogonal $2^n \times 2^n$ matrices. The center of E, $\Xi(E)$, is $\{\pm I\}$ and the group E has the *extraspecial property* that $\bar{E} = E/\Xi(E)$ is elementary abelian (hence a binary vector space). Let V denote the vector space $\mathbb{Z}_2^n$ (where $\mathbb{Z}_2 = \{0,1\}$) and label the standard basis of $\mathbb{R}^{2^n}$ by $|v\rangle$, $v \in V$. Every element e of E can be written uniquely in the form

$$e = X(a)Z(b)(-I)^\lambda \tag{1}$$

where $\lambda \in \mathbb{Z}_2$, $X(a) : |v\rangle \to |v+a\rangle$, $Z(b) : |v\rangle \to (-1)^{b\cdot v}|v\rangle$, for $a, b \in V$.

Consider the jth qubit in a quantum channel which is transmitting n qubits. Let v_j be the vector with a 1 in the jth bit and 0's in the remaining bits. Then $X(v_j)$ is the transformation which applies the Pauli matrix $\sigma_x = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ to the jth qubit and does nothing to the remaining $n-1$ qubits. The transformation $Z(v_j)$ applies the Pauli matrix $\sigma_z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ to the jth bit and does nothing to the other $n-1$ qubits. In the language of quantum error correction, $X(v_j)$ is a bit error and $Z(v_j)$ is a phase error in the jth qubit. The element $X(a)Z(b)$ corresponds to bit errors in the qubits for which $a_j = 1$ and phase errors in the qubits for which $b_j = 1$. It has been shown that for the purposes of quantum error correction, we need consider only errors of the types $\sigma_x = X(v_j)$, $\sigma_z = Z(v_j)$, and $\sigma_y = X(v_j)Z(v_j)$, since if we can correct errors of these types in t qubits, we can correct arbitrary errors in t qubits [4,7,10].

Our construction yields quantum codes as simultaneous eigenspaces of the matrices in an Abelian subgroup of E. For this construction, we need a criterion for whether two elements of E commute. Define a quadratic form Q on $\bar{E} = E/\Xi(E)$ by

$$Q(\bar{e}) = \sum_{j=0}^{n} a_j b_j \pmod 2, \tag{2}$$

where $e = \pm X(a)Z(b)$ is any element of E whose image in $\bar{E}$ is $\bar{e}$. Then $e^2 = (-I)^{Q(\bar{e})}$ and $Q(\bar{e}) = 0$ or 1 according as $X(a)$ and $Z(b)$ commute or anticommute. If $e = w_1 \otimes \ldots \otimes w_n$ then $Q(\bar{e})$ is the parity of the number of components w_j that are equal to $\sigma_x\sigma_z$. Define a binary inner product on $\bar{E}$ by $(\bar{e}, \bar{e}') = Q(\bar{e}+\bar{e}') + Q(\bar{e}) + Q(\bar{e}')$. For $\bar{e} = (a|b)$, $\bar{e}' = (a'|b')$,

$$(\bar{e}, \bar{e}') = a \cdot b' + a' \cdot b \pmod 2. \tag{3}$$

Now consider two elements of E: $e = \pm X(a)Z(b)$ and $e' = \pm X(a')Z(b')$. Then e and e' commute or anticommute according as $(\bar{e}, \bar{e}') = 0$ or 1.

A subspace $\bar{S}$ of $\bar{E}$ is said to be totally singular if $Q(\bar{s}) = 0$ for all $\bar{s} \in \bar{S}$. It follows that for $\bar{s}$, $\bar{s}'$ in $\bar{S}$ the inner product $(\bar{s}, \bar{s}') = 0$. If $\bar{M}$ is a maximal totally singular subspace, then the group $\bar{M}$ has 2^n distinct linear characters, and the corresponding eigenvectors determine

a coordinate frame $\mathcal{F}(\bar{M})$ (an orthonormal basis of $\mathbb{R}^{2^n}$). For example, the image of $Z(V)$ in $\bar{E}$ determines the coordinate frame $|v\rangle$, $v \in V$, and the image of $X(V)$ determines the coordinate frame $2^{-n/2}\sum_v (-1)^{u\cdot v}|v\rangle$, $u \in V$. If $\bar{S} \subseteq \bar{M}$ is a k-dimensional totally singular subspace, then the group $\bar{S}$ has 2^k distinct linear characters. The 2^n vectors in $\mathcal{F}(\bar{M})$ are partitioned into 2^k sets of size 2^{n-k} with each set corresponding to a different eigenspace. We view each eigenspace as a quantum error-correcting code which maps $n-k$ qubits into n qubits. The 2^{n-k} vectors from $\mathcal{F}(\bar{M})$ in that eigenspace constitute the codewords.

More generally, we may use complex space, and so we define a quantum error-correcting code encoding k qubits into n qubits to be any 2^k-dimensional subspace C of $\mathbb{C}^{2^n}$. This code will protect against errors in a certain error set $\mathcal{E}$, which we take to be a subset of the extraspecial group E. As remarked earlier, there is no loss of generality in restricting to error sets in E.

For such a code C to protect against all errors in an error set $\mathcal{E}$, it is necessary and sufficient [7,12] that for any two vectors $|c_1\rangle$ and $|c_2\rangle$ in C with $\langle c_1|c_2\rangle = 0$, and any two transformations e_1 and e_2 from $\mathcal{E}$, we have

$$\langle c_1|e_1^{-1}e_2|c_2\rangle = 0, \tag{4}$$
$$\langle c_1|e_1^{-1}e_2|c_1\rangle = \langle c_2|e_1^{-1}e_2|c_2\rangle. \tag{5}$$

Note that since we are assuming that $\mathcal{E}$ is contained in E, we can replace $e_1^{-1}e_2$ by e_1e_2 in the above equations, since $e_1 = \pm e_1^{-1}$. An interesting special case occurs when both sides of Eq. (5) are always equal to 0 for $e_1 \neq e_2 \in \mathcal{E}$. This implies that there is a measurement which will uniquely determine the error without affecting the encoded subspace. After this measurement, the error can subsequently be corrected by a unitary operation. If both sides of Eq. (5) are not always 0, then there can be two errors e_1 and e_2 between which it is impossible to distinguish. However, these two errors are guaranteed to have identical effects on vectors within the subspace C, and so need not be distinguishable in order to be correctable.

We now can show the connection between orthogonal geometry and quantum error correcting codes.

Theorem 1. Suppose that $\bar{S}$ is a k-dimensional totally singular subspace of $\bar{E}$. Let $\bar{S}^\perp$ be the $(2n-k)$-dimensional subspace orthogonal to $\bar{S}$ with respect to the inner product (3). Further suppose that for any two vectors e_1 and e_2 in an error set $\mathcal{E} \subseteq E$, either $\bar{e}_1\bar{e}_2 \in \bar{S}$ or $\bar{e}_1\bar{e}_2 \notin \bar{S}^\perp$. Then the eigenspace C corresponding to any character of the group $\bar{S}$ is an error-correcting code which will correct any error $e \in \mathcal{E}$.

Proof. We first show that if $e \in E$, then e permutes the 2^k spaces C_i which are generated by the 2^k different linear characters of $\bar{S}$. Consider an element $\bar{s} \in \bar{S}$ with eigenvalue λ_s. We write s for the associated representation. Then for any $|c\rangle \in C$ we have $s|c\rangle = \lambda_s|c\rangle$, and $se|c\rangle = (-1)^{(\bar{s},\bar{e})}es|c\rangle = (-1)^{(\bar{s},\bar{e})}\lambda_s e|c\rangle$, where $(\bar{s},\bar{e})$ is the inner product (3). Since $(-1)^{(\bar{s},\bar{e})}\lambda_s$ is independent of $|c\rangle$, this shows that the action of e permutes the eigenspaces generated by the characters of S.

We next divide the proof into two cases, according as $\bar{e}_1\bar{e}_2 \in \bar{S}$ or $\bar{e}_1\bar{e}_2 \notin \bar{S}^\perp$.

Case 1. Suppose $\bar{e}_1\bar{e}_2 \in \bar{S}$. It follows that for $|c_1\rangle$ and $|c_2\rangle \in C$ with $\langle c_1|c_2\rangle = 0$,

$$\langle c_1|e_1e_2|c_2\rangle = \lambda_{e_1e_2}\langle c_1|c_2\rangle = 0, \tag{6}$$

and for all $|c\rangle \in C$,

$$\langle c|e_1e_2|c\rangle = \lambda_{e_1e_2}\langle c|c\rangle = \lambda_{e_1e_2}, \tag{7}$$

establishing Eqs. (4) and (5).

Case 2. Suppose $\bar{e}_1\bar{e}_2 \notin \bar{S}^\perp$. It follows that for some $\bar{s} \in \bar{S}$, $se_1e_2 = -e_1e_2s$. Thus, for $|c\rangle \in C$,

$$se_1e_2|c\rangle = -e_1e_2s|c\rangle = -\lambda_s e_1e_2|c\rangle, \tag{8}$$

so $e_1e_2|c\rangle \notin C$. Thus $e_1e_2|c\rangle$ is in a different eigenspace, so

$$\langle c_1|e_1e_2|c_2\rangle = 0 \tag{9}$$

for all c_1, $c_2 \in C$ (including $c_1 = c_2$). Again Eqs. (4) and (5) hold. QED

Example 1. We first describe the code mapping 1 qubit into 5 qubits presented in Ref. [7], which contains two codewords,

$$\begin{aligned}
|c_0\rangle = {} & |00000\rangle \\
& + |11000\rangle + |01100\rangle + |00110\rangle + |00011\rangle + |10001\rangle \\
& - |10100\rangle - |01010\rangle - |00101\rangle - |10010\rangle - |01001\rangle \\
& - |11110\rangle - |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle, \\
|c_1\rangle = {} & |11111\rangle \\
& + |00111\rangle + |10011\rangle + |11001\rangle + |11100\rangle + |01110\rangle \\
& - |01011\rangle - |10101\rangle - |11010\rangle - |01101\rangle - |10110\rangle \\
& - |00001\rangle - |10000\rangle - |01000\rangle - |00100\rangle - |00010\rangle.
\end{aligned}$$

Essentially the same code is given in Ref. [5], but we use the above presentation since it is fixed under cyclic permutations. It is easily verified that $X(11000)Z(00101)$ fixes $|c_0\rangle$ and $|c_1\rangle$. Thus we may take the vector $(11000|00101) \in \bar{E}$ to be in the subspace $\bar{S}$. Using the fact that the code is closed under cyclic permutations, we find that $\bar{S}$ is the 4-dimensional totally singular subspace generated by the vectors

$$\begin{array}{c|c}
11000 & 00101 \\
01100 & 10010 \\
00110 & 01001 \\
00011 & 10100
\end{array} \tag{10}$$

[The fifth cyclic shift, (10001|01010), is also in this subspace.] The dual $\bar{S}^\perp$ is generated by $\bar{S}$ and the two additional vectors (11111|00000) and (00000|11111). It is straightforward to verify that the minimal weight vectors in $\bar{S}^\perp$ have weight three [one such vector is (00111|00101)] and thus the code can correct one error.

Example 2. Suppose we have a classical linear $[n,k,d]$ binary error correcting code C (i.e., it is over $\mathbb{Z}_2^n$, it is k-dimensional, and it has minimal distance d, so that it corrects $t = \lfloor (d-1)/2 \rfloor$ errors). Suppose furthermore that $C^\perp \subset C$. We can define a subspace $\bar{S}$ to consist of all vectors $(v_1|v_2) \in \bar{E}$, where v_1, $v_2 \in C^\perp$. The dual $\bar{S}^\perp$ consists of all vectors $(v_1|v_2)$ with v_1, $v_2 \in C$, showing that the corresponding quantum error-correcting code corrects t errors. The subspace $\bar{S}$ is $2(n-k)$-dimensional, so the quantum code maps $n-2k$ qubits into n qubits. This is the method described in Refs. [3,4].

Example 3. Consider the subspace $\bar{S}$ obtained by modifying the classical [8,4,4] Hamming code as follows:

$$\begin{array}{c|c} 01110100 & 00111010 \\ 00111010 & 00011101 \\ 00011101 & 01001110 \\ 11111111 & 00000000 \\ 00000000 & 11111111. \end{array} \tag{11}$$

It is straightforward to verify that these vectors generate a 5-dimensional totally singular subspace $\bar{S}$ which is invariant under cyclic permutations of the last 7 bits, and that $\bar{S}^\perp$ has minimal weight 3. This gives a quantum code mapping 3 qubits into 8 qubits which can correct one error. The same code was discovered by Gottesman [8], who used similar group-theoretic techniques, and by Steane [9].

Example 4. By duplicating the 5-qubit code (10) and adding two vectors, we can obtain a code which maps 4 qubits into 10 qubits and corrects one error:

$$\begin{array}{cc|cc} 01100 & 11110 & 10010 & 01100 \\ 00110 & 01111 & 01001 & 00110 \\ 00011 & 10111 & 10100 & 00011 \\ 10001 & 11011 & 01010 & 10001 \\ 11111 & 11111 & 00000 & 00000 \\ 00000 & 00000 & 11111 & 11111. \end{array} \tag{12}$$

Example 5. The following construction is a generalization of the 5-qubit code (10) inspired by classical quadratic residue codes. It works for any prime p of the form $8j+5$. We have not found good theoretical bounds on the minimal distance, but for small primes these codes are excellent. To construct the first vector $(a|b)$, put $a_j = 1$ when j is a nonzero quadratic residue mod p (that is, $j = k^2 \bmod p$ for some k) and put $b_j = 1$ when j is a quadratic nonresidue. To obtain $p-1$ vectors that generate the subspace $\bar{S}$, take $p-2$ cyclic shifts of the first vector. For $p = 13$, the first basis vector is

$$0101100001101|0010011110010$$

and the remaining vectors are obtained by cyclic shifts. The minimal weight of $\bar{S}^\perp$ was calculated by computer to be 5. This gives a code mapping one qubit into 13 qubits which corrects 2 errors. For $p = 29$, ths subspace $\bar{S}^\perp$ has minimal distance 11, so this construction gives a code mapping 1 qubit to 29 which corrects 5 errors.

We now give the construction of the group $L \subset O(\mathbb{R}^{2^n})$ from its subgroup E. The group L is the normalizer of E in the real orthogonal group $O(\mathbb{R}^{2^n})$; that is, it is the subgroup of elements $g \in O(\mathbb{R}^{2^n})$ such that $g^{-1}Eg = E$. This normalizer acts on E by conjugation, fixing the center $\Xi(E)$ ($g \in L$ acts on E as the permutation $e \to g^{-1}eg$). Hence there is a well-defined action of L on the binary vector space $\bar{E}$ that preserves the quadratic form Q. The quotient L/E is the orthogonal group $O^+(2n,2)$, a finite classical group [14]. The group L appears in recent connections between classical Kerdock error-correcting codes, orthogonal geometry, and extremal Euclidean line sets [13]. This group also appears [7] as the group of Bell-state-preserving bilateral local transformations that two experimenters (A and B) can jointly perform on n pairs of particles (each pair being in a Bell state). Hence there is a one-to-one correspondence between Bell states and elements of $\bar{E}$ (cf. Eqs. (39) and (67) of Ref. [7]). The quadratic form $Q(\bar{e})$ is 0 or 1 according as the Bell states are symmetric or antisymmetric under interchange of A and B.

The following are group elements that generate L from E, shown together with their induced action on the binary vector space $\bar{E}$.

(1) $H = 2^{-n/2}[(-1)^{u\cdot v}]_{u,v\in V}$, which interchanges $X(a)$ and $Z(b)$. This applies the transformation $R = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ to every qubit.

(2) $\hat{H}_2 = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \otimes I_{2^{n-1}}$, which applies R to the first qubit and leaves the other qubits unchanged. This acts on $\bar{E}$ by interchanging a_1 and b_1.

(3) Every matrix A in the general linear group $\mathrm{GL}(V)$ determines a permutation matrix $|v\rangle \to |vA\rangle$ in $O(\mathbb{R}^{2^n})$. The action on $\bar{E}$ induced by conjugation is $X(a) \to X(aA)$, $Z(b) \to Z(bA^{-\mathrm{T}})$. For example the quantum XOR taking $|q_1 q_2\rangle \to |q_1(q_1 \oplus q_2)\rangle$ is represented by

$$(a_1a_2|b_1b_2) \to (a_1a_2|b_1b_2)\left(\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right). \tag{13}$$

The back action of the XOR on the phases is evident in its effect on b_1 and b_2. Any orthogonal matrix in $O(\mathbb{R}^{2^n})$ that normalizes both $X(V)$ and $Z(V)$ is of this type for some A [13, Lemma 3.14].

(4) Diagonal matrices $d_M = \mathrm{diag}[(-1)^{Q_M(v)}]$, where Q_M is a binary quadratic form on V for which the associated bilinear form $Q_M(u+v) - Q_M(u) - Q_M(v)$ is uMv^{T}. Note that M is symmetric with zero diagonal. The induced action on $\bar{E}$ is given by

$$(a|b) \to (a|b)\left(\begin{array}{c|c} I & M \\ \hline 0 & I \end{array}\right). \tag{14}$$

These matrices are precisely the elements of L that induce the identity on the subgroup $Z(V)$. In terms of their effect on qubits, these are the transformations in L that change the phases of the qubits while fixing their values.

Remark. The group E' is generated by E and iI in the unitary group $U(2^n)$. Now we cannot define $Q(\bar{e}) = e^2$ because $(ie)^2 \neq e^2$. However, we still have the nonsingular alternating binary form

$$\left(\bar{X}(a)\bar{Z}(b), \bar{X}(a')\bar{Z}(b')\right) = a \cdot b' + a' \cdot b \pmod 2. \quad (15)$$

The group L' is the normalizer of E' and is generated by L and by diagonal transformations $d_P = \mathrm{diag}[i^{T_P(v)}]$ where T_P is a $\mathbb{Z}_4$-valued quadratic form [13, Section 4]. The induced action on $\bar{E}' = E'/\Xi(E')$ is described by

$$(a|b) \to (a|b) \left(\begin{array}{c|c} I & P \\ \hline 0 & I \end{array}\right) \quad (16)$$

where P is symmetric and may have a nonzero diagonal. For example, applying the $\pi/2$ rotation around the z-axis $\left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$ to each qubit corresponds to $P = I$. The quotient L'/E' is the symplectic group $\mathrm{Sp}(2n, 2)$ [14]. As the quadratic form Q played no role in the proof of Theorem 1, it is only necessary for a quantum code that $\bar{S}$ satisfy $(\bar{S}, \bar{S}) = 0$ with respect to the alternating form. This means the complex groups E' and L' can be used for code construction.

The group L acts transitively on the totally singular subspaces $\bar{S}$ of dimension k, so there is some element $g \in L$ taking any particular k-dimensional totally singular subspace to the subspace corresponding to a quantum code generated as in Theorem 1. This implies that some $g \in L$ takes the canonical 2^{n-k}-dimensional Hilbert space generated by the first $n - k$ qubits to the encoded subspace. Since L can be generated by NOT's, XOR's and $\pi/2$ rotations around the x-axis, these three quantum gates are therefore sufficient for encoding any of these quantum codes.

We next give a Gilbert–Varshamov lower bound for the asymptotic rate of this class of codes. It matches the Gilbert–Varshamov lower bounds known for general quantum error-correcting codes [10].

Theorem 2. There exist quantum error-correcting codes with asymptotic rate

$$R = 1 - 2\delta \log_2 3 - H_2(2\delta) \quad (17)$$

where δ is the fraction of qubits that are subject to decoherence and $H_2(\delta) = -\delta \log_2 \delta - (1 - \delta) \log_2(1 - \delta)$ is the binary entropy function.

Proof. Let N_k denote the number of k-dimensional totally singular subspaces. We count pairs $(e, \bar{S})$ where $e \in E$ is in $\mathcal{E}^2$ (i.e., $e = e_1 e_2$ with e_1, e_2 in the error set $\mathcal{E}$) and $\bar{S}$ is a k-dimensional totally singular subspace with $\bar{e} \in \bar{S}^\perp \backslash \bar{S}$. Transitivity of L on singular points ($\bar{e} \neq 0$, $Q(\bar{e}) = 0$), and on nonsingular points ($Q(\bar{e}) \neq 0$) implies that each $e \in E$ satisfies $\bar{e} \in \bar{S}^\perp \backslash \bar{S}$ for μN_k subspaces $\bar{S}$, where the fraction $\mu \approx 2^{-k}$. If $|\mathcal{E}^2| < 2^k$ then there exists a k-dimensional totally singular subspace $\bar{S}$ that satisfies $\bar{e} \notin \bar{S}^\perp \backslash \bar{S}$ for all $e \in \mathcal{E}^2$. Hence the achievable rate R satisfies

$$\begin{aligned} 1 - R &= \log_2 |\mathcal{E}^2|/n \\ &= \log_2 \left[3^{2\delta n} \tbinom{n}{2\delta n}\right]/n \\ &= 2\delta \log_2 3 + H_2(2\delta). \end{aligned} \quad (18)$$

We would like to thank David DiVincenzo for discussions about the group L as presented in [7].

[1] P. W. Shor, Phys. Rev. A. **52,** 2493 (1995); A. Steane, Phys. Rev. Lett. **77,** 793 (1996).

[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76,** 722 (1996).

[3] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54,** 1098 (1996).

[4] A. Steane, Proc. R. Soc. London A (to be published).

[5] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. (to be published).

[6] B. B. Plenio, V. Vedral, and P. L. Knight, Phys. Rev. A (to be published); L. Vaidman, L. Goldenberg, and S. Wiesner, "Error prevention scheme with four particles," Phys. Rev. A (to be published). P. W. Shor and J. A. Smolin, LANL e-print quant-ph/9604006 (unpublished); S. L. Braunstein and J. A. Smolin, Phys. Rev. A (to be published).

[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54,** 3824 (1996).

[8] D. Gottesman, Phys. Rev. A (to be published).

[9] A. Steane, Phys. Rev. A (to be published).

[10] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77,** 2585 (1996).

[11] B. Schumacher, LANL e-print quant-ph/9604023 (unpublished); B. Schumacher and M. A. Nielsen, LANL e-print quant-ph/9604022 (unpublished); S. Lloyd, LANL e-print quant-ph/9604015 (unpublished).

[12] E. Knill and R. Laflamme, Phys. Rev. A (to be published).

[13] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, *Proc. London Math. Soc.* (to be published).

[14] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups* (Cambridge University Press, Cambridge, England, 1990).