Quantum Error Correction and Orthogonal Geometry

A. R. Calderbank,\textsuperscript{1} E. M. Rains,\textsuperscript{2} P. W. Shor,\textsuperscript{1} and N. J. A. Sloane\textsuperscript{1}
\textsuperscript{1}AT&T Research, Murray Hill, New Jersey, 07974
\textsuperscript{2}Institute for Defense Analysis, 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 \[ [1,2,3,4,5,6,7,8,9,10,11,12]. \] However, the theoretical aspects of this work have been concentrated on properties and rates of these codes \[ [13,14,15,16,17,18,19,20,21,22] \], and not on combinatorial recipes for constructing such codes. This letter introduces a unifying framework which explains most of the codes discovered to date, provides new fundamental insights, and greatly facilitates the construction of new examples.

The basis for this unifying framework is group theoretic. It rests on the structure of certain subgroups of \( \text{O}(2^n) \) and \( \text{U}(2^n) \) called Clifford groups \[ [23] \]. We first construct a subgroup \( E \) of \( \text{O}(2^n) \). The group \( E \) is an extraspecial 2-group and it provides a fundamental bridge between quantum error-correcting codes in Hilbert space and binary orthogonal geometry. We then obtain the Clifford groups by taking the normalizer \( L \) of \( E \) in \( \text{O}(2^n) \) or the normalizer \( L' \) of the group \( E' \) generated by \( E \) and \( i1 \) in \( \text{U}(2^n) \). Since the natural setting for quantum mechanics is complex space, it would appear more natural to focus on the complex group \( L' \). However, we shall spend considerable time discussing the real Clifford group \( L \). We do this for two reasons. First, the structure of the real group \( L \) is easier to understand, and second, it is all that is required for the construction of known quantum error-correcting codes.

The Group Theoretic Framework. The extraspecial 2-group \( E = E_n \) is realized as an irreducible group of \( 2^n \times \mathbb{Z}_2 \) matrices of size \( 2^{n+2} \). The center \( Z(E) = \{ \pm I \} \) and the extraspecial condition is that \( E = E/Z(E) \) is elementary abelian (and hence a binary vector space). Let \( V \) denote the vector space \( \mathbb{Z}_2^2 \) and label the standard basis of \( \mathbb{R}^{2^n} \) as \( \{ v \}, v \in V \). Every element \( e \) of \( E \) can be written uniquely in the form

\[
e = X(a)Z(b)(-1)^\lambda
\]

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

Given a quantum channel which transmits \( n \) qubits, we consider the \( i \)-th qubit of our \( n \) qubits. Let \( v_i \) be the vector with a 1 in the \( i \)-th bit and 0’s in the remaining bits. Then \( X(v_i) \) is the transformation which applies the Pauli matrix \( \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) to the \( i \)-th qubit and does nothing to the remaining \( n-1 \) qubits. The transformation \( Z(v_i) \) applies the Pauli matrix \( \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) to the \( i \)-th bit and does nothing to the other \( n-1 \) qubits. In the language of quantum error correction, \( X(v_i) \) is a bit error in the \( i \)-th qubit and \( Z(v_i) \) is a phase error in the \( i \)-th qubit. The element \( X(a)Z(b) \) then corresponds to bit errors in the qubits for which \( a_i = 1 \) and phase errors in the qubits for which \( b_i = 1 \).

Observe that \( E \) is the group of tensor products \( \pm w_1 \otimes \ldots \otimes w_n \), where each \( w_i = I, \sigma_x, \sigma_z, \) or \( \sigma_y \sigma_z \).

For the purposes of quantum error correction, we only need to consider the three types of errors \( \sigma_x, \sigma_z \), and \( \sigma_y \sigma_z \), as any error correcting code which corrects these three types of errors will be able to correct arbitrary errors \[ [24,25] \].

Define a quadratic form \( Q \) on \( E \) by

\[
Q(\bar{v}) = \sum_{i=0}^{n} a_i b_i,
\]

where \( \epsilon = \pm X(a)Z(b) \) and \( \bar{v} \) is the image of \( \epsilon \) in the quotient \( E/Z(E) \). Then \( \epsilon^2 = (-1)^{Q(\bar{v})} \) and \( Q(\bar{v}) = 0 \) or 1 according as \( X(a) \) and \( Z(b) \) commute or anticommute \( (X(a)Z(b) = -Z(b)X(a)) \). Observe that if \( \epsilon = w_1 \otimes \ldots \otimes w_n \), then the value \( Q(\bar{v}) \) is just the parity of the number of components \( w_i \) that are equal to \( \sigma_x \).

The normalizer \( L = L \) of \( E \) in the real orthogonal group \( \text{O}(\mathbb{R}^{2^n}) \) is the subgroup of elements \( g \in \text{O}(\mathbb{R}^{2^n}) \) which preserve \( E \) under conjugation (i.e., elements such that \( g^{-1}Eg = E \)). This normalizer \( L \) acts on \( E \) by conjugation fixing the center \( Z(E) \) (\( g \in L \) acts as the permutation \( \epsilon \rightarrow g^{-1}eg \)). Hence there is a well defined
action on the binary vector space $E$ that preserves the quadratic form $Q$. The quotient $L/E$ is the orthogonal group $O^+(2n, 2)$, a finite classical group $[\square]$. The group $L$ appears in recent connections between classical Kerdock error-correcting codes, orthogonal geometry, and extremal Euclidean line sets $[\square]$. This group also appears $[\square]$ as the group of Bell states 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). Here there is a one-to-one correspondence between Bell states and elements of $E$ (cf. Eqs. (39) and (67) of [3]). The quadratic form $Q(e^2) = 0$ or 1 according as the Bell states are symmetric or antisymmetric under interchange of $A$ and $B$. Observe that the Bell states are the physical invariant conserved by this presentation of $L$.

Listed below are group elements that generate $L$ and the induced action on the binary vector space $E$.

1. $H = 2^{-n/2}(-1)^{a\cdot b}[a], v \in V$, which interchanges $X(b)$ and $Z(b)$.

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

$$
(a_1 a_2 | b_1 b_2) \rightarrow (a_1 a_2 | b_1 b_2) \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.
$$

That the XOR leaves the value of the first qubit unchanged can be seen in that is has no effect on $(00|00) \in E$, which is the transformation changing the phase of the first qubit. The back action of the XOR on the phases is evident in its effect on $b_1$ and $b_2$. Any orthogonal matrix in $O(\mathbb{R}^{2n})$ that normalizes both $X(V)$ and $Z(V)$ must have this special form $[\square]$ (Lemma 3.14).

3. $H_2 = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes I_{2^{n-1}}$ applies a $\pi/2$ rotation to the first qubit and leaves the other qubits unchanged. The effect of this transformation on $E$ is to interchange $a_1$ and $b_1$.

4. Diagonal matrices $d_M = \text{diag}([-1]Q_M(v)]$ 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 equal to $uM^{-T}v$. Note that $M$ is symmetric with zero diagonal. The induced action on $E$ is described by the matrix

$$
(a|b) \rightarrow (a|b) \begin{pmatrix} M & 0 \\ 0 & T \end{pmatrix}.
$$

These 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 but fix the values of the qubits.

Remark. The group $L'$ is the normalizer of the group $E'$ generated by $E$ and $iH$ in the unitary group $U(2^n)$. This time we cannot define $Q(e^2) = e^2$ because $(i)^2 \neq e^2$. However, we still have the nonsingular alternating binary form $(X(a)Z(b), X(a')Z(b')) = a \cdot b + a' \cdot b$. (5)

The group $L'$ is generated by $L$ and by diagonal transformations $d_P = \text{diag}[iP_{s}(v)]$ where $P_T$ is a $\mathbb{Z}$-valued quadratic form $[\square]$ Section 4]. The induced action on $E' = E' / Z(E')$ is described by the matrix

$$
(a|b) \rightarrow (a|b) \begin{pmatrix} 1 & P_T \\ 0 & 1 \end{pmatrix}.
$$

where $P$ is symmetric and the diagonal may be nonzero. For example, applying the transformation $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to each qubit corresponds to taking $P = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. The quotient $L'/E'$ is the symplectic group $Sp(2n, 2) \otimes \mathbb{Z}$. Quantum Error-Correcting Codes. A subspace $S$ of $E$ is said to be totally singular if $Q(s) = 0$ for all $s \in S$. It follows that for $s = (a|b)$, $s' = (a'|b')$ in $S$ the inner product $(s, s') = Q(s + s') - Q(s) - Q(s')$ satisfies

$$
(s, s') = a \cdot b' + a' \cdot b = 0.
$$

The group $L$ acts transitively on totally singular subspaces of a given dimension. Hence every $k$-dimensional totally singular subspace is contained in the same number of maximal $(n$-dimensional) totally singular subspaces. If $M$ is a maximal totally singular subspace, then the group $M$ has $2^n$ distinct linear characters, and the corresponding eigenspaces determine a coordinate frame $\mathcal{F}(M)$ (an orthonormal basis of $\mathbb{R}^{2^n}$). For example, $Y(V)$ determines the coordinate frame $[v], v \in V$, and $X(V)$ determines the coordinate frame $2^{-n/2}\sum_u(-1)^{a\cdot u}|v|, u \in V$. If $S \subseteq M$ is a $k$-dimensional totally singular subspace, then the group $S$ has $2^k$ distinct linear characters. The $2^k$ vectors in $\mathcal{F}(M)$ are partitioned into $2^k$ sets of size $2^{n-k}$ with each set corresponding to a different eigenspace. We view each eigenspace as an encoding of $n-k$ qubits into $n$ qubits. The $2^{n-k}$ vectors in $\mathcal{F}(M)$ in that eigenspace constitute $2^{n-k}$ different codewords in a quantum error-correcting code.

In general, a quantum error-correcting code encoding $k$ qubits into $n$ qubits is a $2^k$-dimensional subspace $C$ of $\mathbb{C}^2^n$. It will protect against errors in an error set $\mathcal{E}$ which we will take to be a set of elements of the extraspecial group $E$. We are not restricting ourselves by doing this, since it has been shown that protecting against $t$ errors...
corresponding to the three Pauli matrices $\sigma_x$, $\sigma_y$, and $\sigma_z$ is enough to protect against $t$ arbitrary errors $\mathcal{E}$.

For a quantum error correcting code to protect against all errors in the error syndrome $\mathcal{E}$, it is necessary and sufficient that for any two vectors $|1\rangle$ and $|2\rangle$ in $C$ with $\langle 1 | 2 \rangle = 0$, and any two transformations $e_1$ and $e_2$ from the error syndrome $\mathcal{E}$,

$$\langle e_1 | e_1^{-1} e_2 | e_2 \rangle = 0$$

and

$$\langle e_1 | e_1^{-1} e_2 | e_1 \rangle = \langle e_2 | e_1^{-1} e_2 | e_2 \rangle. \tag{9}$$

Note that if we assume the error set $\mathcal{E}$ is contained in $E$, we can use $e_1 e_2$ instead of $e_1^{-1} e_2$ in the above equations, since $e_1 = \pm e_1^{-1}$. An interesting special case occurs when both sides of Equation (9) 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 Equation (9) 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 it is not necessary to distinguish between these errors in order to correct the error.

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

**Theorem 1.** Suppose that $S$ is a $k$-dimensional totally singular subspace. Let $S^\perp$ be the $(2n-k)$-dimensional subspace orthogonal to $S$ with respect to the inner product $\langle \cdot | \cdot \rangle$. Further suppose that for any two vectors $e_1$ and $e_2$ in an error set $\mathcal{E} \subseteq E$, either $e_1 e_2 \in S$ or $e_1 e_2 \notin S^\perp$.

Then the eigenspace $C$ corresponding to any character of the group $S$ 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 $S$. Consider a vector $|e\rangle \in C$. Then for each $s \in S$, $s|e\rangle = \lambda_s |e\rangle$, where $\lambda_s$ is the eigenvalue associated with $s$ (which does not depend on $e$). Now, $s e |c\rangle = (-1)^{\langle s | c \rangle} e |c\rangle = (-1)^{\langle s | e c \rangle} e |c\rangle$ where $\langle s | t \rangle$ is the inner product $\langle \cdot | \cdot \rangle$. Since $(-1)^{\langle s | e c \rangle} = \lambda_s$ is independent of $c$, this shows that the action of $e$ permutes the eigenspaces generated by the characters of $S$.

We will divide the proof into two cases, according as $e_1 e_2 \in S$ or $e_1 e_2 \notin S^\perp$.

**Case 1.** We assume that $e_1 e_2 \in S$. It follows that for $|1\rangle$ and $|2\rangle \in C$ with $\langle e_1 | e_2 \rangle$,

$$\langle e_1 | e_1 e_2 | e_2 \rangle = \lambda_{e_1 e_2} \langle e_1 | e_2 \rangle = 0 \tag{10}$$

and that

$$\langle e_1 | e_1 e_2 | e_2 \rangle = \lambda_{e_1 e_2} \langle e_1 | e_2 \rangle = \lambda_{e_1 e_2} \tag{11}$$

for all $c \in C_i$, satisfying equations (8) and (9).

**Case 2.** We assume that $e_1 e_2 \notin S^\perp$. It follows that for some $s \in S$, $s e_1 e_2 = -e_1 e_2 s$. Thus, for $|c\rangle \in C$, $s e_1 e_2 |c\rangle = -e_1 e_2 s |c\rangle = -\lambda_s e_1 e_2 |c\rangle$, so $e_1 e_2 |c\rangle \notin C$. Thus, $e_1 e_2 |c\rangle$ is in a different eigenspace, so

$$\langle e_1 | e_1 e_2 | e_2 \rangle = 0 \tag{12}$$

for all $c_1, c_2 \in C$, including the case where $c_1 = c_2$. This shows that equations (8) and (9) are satisfied.

The quadratic form $Q$ plays no role in this proof and it is only necessary that $S$ and $S^\perp$ satisfy $(S, S) = 0$ with respect to the alternating form. This means the complex group $L'$ can also be used for code construction.

The totally singular subspaces $S$ of dimension $k$ are transitive under the action of $L$, so there is some group element $g \in L$ taking any canonical $k$-dimensional totally singular subspace to the subspace corresponding to a quantum code generated as in Theorem 1. This implies that $g$ takes the canonical $2^{n-k}$ Hilbert space generated by the first $n-k$ qubits to the encoded subspace. Since $L$ can be generated by XOR’s and $\pi/2$ rotations, these quantum gates are sufficient for encoding any of these quantum codes.

To illustrate the technique, we will now give some examples. We first describe the error-correcting code mapping 1 qubit into 5 qubits presented in Ref. [17]. This code contains two codewords,

$$|c_9\rangle = |00000\rangle \tag{13}$$

and

$$|c_1\rangle = |11111\rangle \tag{14}$$

Essentially the same code is given in Ref. [16], but we use the presentation above as it is symmetric under cyclic permutations. If $X(11000) Y(00101)$ is applied to $|c_9\rangle$ and $|c_1\rangle$, it is easily verified that these codewords are left invariant. Thus, the vector $(11000|00101) \in \tilde{E}$ is one of the vectors in the subspace $\tilde{S}$. Since the code is symmetric under cyclic permutations, four other vectors of $\tilde{S}$ is found, and it can easily be shown that the four vectors

\[
\begin{pmatrix}
11000 & 00101 \\
01000 & 10010 \\
00110 & 01001 \\
00011 & 10100
\end{pmatrix}
\]
generate a 4-dimensional totally singular subspace $\mathcal{S}$. [The fifth cyclic shift, (1001010101), is in the subspace generated by these four.] The dual $\mathcal{S}^\perp$ of $\mathcal{S}$ is generated by $\mathcal{S}$ and the additional two vectors (111111000000) and (000000111111). It is straightforward to verify that the minimum weight vector in $\mathcal{S}^\perp$ has weight three [one of these vectors is (001111001111)] and thus this code can correct one error.

Suppose we have a classical binary linear error-correcting code $C$ which is an $[n, k, d]$ code (i.e., it is over $\mathbb{F}_2^n$, it is k-dimensional, and it has minimum distance $d$) so that it corrects $t = (d - 1)/2$ errors. Suppose furthermore that $C^\perp \subseteq C$. We can define a subspace $\mathcal{S}$ containing all vectors of the form $(v_1|v_2)$ where $v_1, v_2 \in C^\perp$. The dual $\mathcal{S}^\perp$ consists of all vectors of the form $(v_1|v_2)$ where $v_1, v_2 \in C$, showing that the corresponding quantum error-correcting code corrects $t$ errors. The subspace $\mathcal{S}$ is $2(n - k)$-dimensional, so the quantum code maps $n - 2k$ qubits into $n$ qubits. This is the method described in Refs. 1-3.

Consider the subspace $\mathcal{S}$ obtained by modifying the classical [7,4,3] Hamming code as follows:

\begin{align}
01110100 & | 00111010 \\
00111010 & | 00011101 \\
00011101 & | 01001110 \\
11111111 & | 00000000 \\
00000000 & | 11111111 \\
\end{align}

It is straightforward to verify that these vectors generate a 5-dimensional totally singular subspace $\mathcal{S}$ which is invariant under cyclic permutation of the last 7 bits, and that $\mathcal{S}^\perp$ has minimum weight 3. This gives a quantum error-correcting code mapping 3 qubits into 8 qubits which can correct one error. A code with identical parameters was discovered by Gottesman [2], also via group-theoretic techniques. He has also found similar 1-error correcting codes encoding $2^k - k - 2$ qubits into $2^k$ qubits for $k \geq 3$.

By duplicating the 5-qubit code (15) and adding two vectors, we can obtain the following 10-qubit code which maps 4 qubits into 10 qubits and corrects one error:

\begin{align}
01110 & | 11110 | 10010 | 01100 \\
01110 & | 01111 | 01001 | 00110 \\
00111 & | 10111 | 10100 | 00011 \\
10011 & | 10111 | 01010 | 10001 \\
11111 & | 11111 | 00000 | 00000 \\
00000 & | 00000 | 11111 | 11111 \\
\end{align}

Inspired by classical quadratic residue codes and the 5-qubit code (15), we give the following new construction. This construction works for any prime $p$ of the form $8j + 5$. We have not found good theoretical bounds on the minimum distance, but for small primes we have found excellent codes. To construct the first vector $(a|b)$, put $a_j = 1$ when $j$ is a nonzero quadratic residue mod $p$ (that is, $j = k^2$ mod $p$ for some $k$) and put $b_j = 1$ when $b$ is a quadratic nonresidue. To obtain $p - 1$ vectors that generate the subspace $\mathcal{S}$, take $p - 2$ cyclic shifts of the first vector. For $p = 13$, the first basis vector is (010110001110) and the remaining vectors are obtained by cyclic shifts. The minimum weight of $\mathcal{S}^\perp$ was calculated by computer to be 5. This gives a code mapping one qubit into 13 qubits which corrects 2 errors. For $p = 29$, the subspace $\mathcal{S}^\perp$ has minimum distance 11 so this construction gives a code mapping 1 qubit to 29 which corrects 5 errors.

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

\[ R = 1 - \delta \log_2 3 - H_2(\delta) \]

where $\delta$ 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 $(e, \mathcal{S})$ where $e \in E$ is in the error set $E$, $\mathcal{S}$ is a $k$-dimensional totally singular subspace, and $e \in \mathcal{S}^\perp \setminus \mathcal{S}$. Transitivity of $L$ on singular points $(e \neq 0, Q(e) = 0)$, and on nonsingular points $(Q(e) \neq 0)$ implies that each $e \in E$ satisfies $e \in \mathcal{S}^\perp \setminus \mathcal{S}$ for $\mu N_k$ subspaces $\mathcal{S}$ where the fraction $\mu \approx 2^{-k}$. If $|E| < 2^k$ then there exists a $k$-dimensional totally singular subspace $\mathcal{S}$ that satisfies $\mathcal{S} \cap \mathcal{S}^\perp = \emptyset$ for all $e \in E$. Hence the achievable rate $R$ satisfies

\[ 1 - R = \log_2 |E|/n \]

\[ = [\log_2 3^{kn}(n)]/n \]

\[ = \delta \log_2 3 + H_2(\delta). \]

**Acknowledgment.** We would like to thank David DiVincenzo for discussions about the group $L$ as presented in [4].

---