Supporting Online Material for

Correcting Quantum Errors with Entanglement

Todd Brun,* Igor Devetak, Min-Hsiu Hsieh

*To whom correspondence should be addressed. E-mail: tbrun@usc.edu

Published 28 September 2006 on Science Express
DOI: 10.1126/science.1131563

This PDF file includes:

SOM Text
Supporting Online Material

The Pauli Group

We first review the properties of Pauli matrices, and relate them to symplectic binary and quaternary vector spaces.

A *qubit* is a quantum system corresponding to a two dimensional complex Hilbert space $H$. Fixing a basis for $H$, the set $\Pi$ of *Pauli matrices* is defined as

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The Pauli matrices are Hermitian unitary matrices with eigenvalues belonging to the set $\{1, -1\}$. The multiplication table of these matrices is given by:

<table>
<thead>
<tr>
<th>$\times$</th>
<th>$I$</th>
<th>$X$</th>
<th>$Y$</th>
<th>$Z$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I$</td>
<td>$I$</td>
<td>$X$</td>
<td>$Y$</td>
<td>$Z$</td>
</tr>
<tr>
<td>$X$</td>
<td>$X$</td>
<td>$I$</td>
<td>$iZ$</td>
<td>$-iY$</td>
</tr>
<tr>
<td>$Y$</td>
<td>$Y$</td>
<td>$-iZ$</td>
<td>$I$</td>
<td>$iX$</td>
</tr>
<tr>
<td>$Z$</td>
<td>$Z$</td>
<td>$iY$</td>
<td>$-iX$</td>
<td>$I$</td>
</tr>
</tbody>
</table>

Observe that the Pauli matrices either commute or anticommute. Let $A = \{\beta A \mid \beta \in \mathbb{C}, |\beta| = 1\}$ be the equivalence class of matrices equal to $A$ up to a phase factor. Then the set $[\Pi] = \{[I], [X], [Y], [Z]\}$ is readily seen to form a commutative group under the multiplication operation defined by $[A][B] = [AB]$. It is called the Pauli group.

We are interested in relating the Pauli group to the additive group $(\mathbb{Z}_2)^2 = \{00, 01, 10, 11\}$ of binary words of length 2 described by the table:

<table>
<thead>
<tr>
<th>+</th>
<th>00</th>
<th>01</th>
<th>11</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>11</td>
<td>10</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>00</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>10</td>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>01</td>
<td>00</td>
</tr>
</tbody>
</table>

This group is also a two-dimensional vector space over the field $\mathbb{Z}_2$. A bilinear form can be defined over this vector space, called the *symplectic form* or *symplectic product* $\odot : (\mathbb{Z}_2)^2 \times (\mathbb{Z}_2)^2 \rightarrow \mathbb{Z}_2$, given by the table

<table>
<thead>
<tr>
<th>$\odot$</th>
<th>00</th>
<th>01</th>
<th>11</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

In what follows we will often write elements of $(\mathbb{Z}_2)^2$ as $u = (z|x)$, with $z, x \in \mathbb{Z}_2$. For instance, 01 becomes (0|1). For $u = (z|x), v = (z'|x') \in (\mathbb{Z}_2)^2$ the symplectic product is equivalently defined by $u \odot v = zz' - x'.x$.

Define the map $N : (\mathbb{Z}_2)^2 \rightarrow \Pi$ by the following table:

<table>
<thead>
<tr>
<th>$(\mathbb{Z}_2)^2$</th>
<th>$\Pi$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>$I$</td>
</tr>
<tr>
<td>01</td>
<td>$X$</td>
</tr>
<tr>
<td>11</td>
<td>$Y$</td>
</tr>
<tr>
<td>10</td>
<td>$Z$</td>
</tr>
</tbody>
</table>

1It makes good physical sense to neglect this overall phase, which has no observable consequence.

2Strictly speaking it is not an inner product.
This map is defined in such a way that \( N(z|x) \) and \( Z^z X^x \) are equal up to a phase factor, i.e.

\[
[N(z|x)] = [Z^z X^x].
\]

We make two key observations

1. The map \([N] : (\mathbb{Z}_2)^2 \rightarrow [\Pi]\) induced by \( N \) is an isomorphism:

\[
[N_u][N_v] = [N_{u+v}].
\]

2. The commutation relations of the Pauli matrices are captured by the symplectic product \( N_u N_v = (-1)^{u \odot v} N_v N_u \).

Both properties are readily verified from the tables.

Now we generalize to \( n \) qubits. Consider an \( n \)-qubit system corresponding to the tensor product Hilbert space \( H^{\otimes n} \). Define an \( n \)-qubit Pauli matrix \( A \) to be of the form

\[
A = A_1 \otimes A_2 \otimes \cdots \otimes A_n,
\]

where \( A_j \in \Pi \). The set of all 4\(^n\) \( n \)-qubit Pauli matrices is denoted by \( \Pi^n \). The product of elements of \( \Pi^n \) is an element of \( \Pi^n \) up to a phase factor. Define as before the equivalence class \([A] = \{ \beta A \mid \beta \in \mathbb{C}, |\beta| = 1 \}\). Then

\[
[A][B] = [A_1 B_1] \otimes [A_2 B_2] \otimes \cdots \otimes [A_n B_n] = [AB].
\]

Thus the set \([\Pi^n]\) = \{\([A] : A \in \Pi^n\)\} is a commutative multiplicative group.

Now consider the group/vector space \((\mathbb{Z}_2)^{2n}\) of binary vectors of length \(2n\). Its elements may be written as \( u = (z|x), z = z_1 \ldots z_n \in (\mathbb{Z}_2)^2, x = x_1 \ldots x_n \in (\mathbb{Z}_2)^2\). We shall think of \( u, z \) and \( x \) as row vectors. The symplectic product of \( u = (z|x) \) and \( v = (z'|x') \) is given by

\[
u \odot v^T = zz^T - z'x' T.
\]

The right hand side are binary inner products and \( T \) denotes the transpose. This should be thought of as a kind of matrix multiplication of a row vector and a column vector. We use \( u \odot v^T \) rather than the more standard \( u v^T \) to emphasize that the symplectic form is used rather than the binary inner product. Equivalently,

\[
u \odot v^T = \sum_i u_i \odot v_i
\]

where \( u_i = (z_i|x_i), v_i = (z'_i|x'_i) \) and this sum represents Boolean addition. Observe that \( u \odot u^T = 0 \), i.e., every vector is “orthogonal” to itself.

The map \( N : (\mathbb{Z}_2)^{2n} \rightarrow \Pi^n \) is now defined as

\[
N_u = N_{u_1} \otimes \cdots \otimes N_{u_n}.
\]

Writing

\[
X^x = X^{x_1} \otimes \cdots \otimes X^{x_n},
\]

\[
Z^z = Z^{z_1} \otimes \cdots \otimes Z^{z_n},
\]

as in the single qubit case, we have

\[
[N(z|x)] = [Z^z X^x].
\]

The two observations made for the single qubit case also hold:
1. The map \([N] : (\mathbb{Z}_2)^{2n} \rightarrow [\Pi^n] \) induced by \(N\) is an isomorphism:

\[
[N_u][N_v] = [N_{u+v}].
\] (1)

Consequently, if \(\{u_1, \ldots, u_m\}\) is a linearly independent set then the elements of the Pauli group subset \([N_{u_1}], \ldots, [N_{u_m}]\) are independent in the sense that no element can be written as a product of others.

2. The commutation relations of the \(n\)-qubit Pauli matrices are captured by the symplectic product

\[
N_u N_v = (-1)^{u \odot v^T} N_v N_u.
\] (2)

**Proof of the theorems**

We now present two results which play a major role in the construction of EAQEC codes. Together they will enable us to conclude that any independent subset of the \(n\)-qubit Pauli group can be transformed via a unitary operation into a canonical set whose elements act nontrivially only on single qubits, proving the lemma used in the main paper.

A subspace \(V\) of \((\mathbb{Z}_2)^{2n}\) is called *symplectic* if there is no \(v \in V\) such that

\[
v \odot u^T = 0, \quad \forall u \in V.
\] (3)

\((\mathbb{Z}_2)^{2n}\) is itself a symplectic subspace. Consider the standard basis for \((\mathbb{Z}_2)^{2n}\), consisting of \(g_i = (e_i|0)\) and \(h_i = (0|e_i)\) for \(i = 1, \ldots, n\), where \(e_i = (0, \ldots, 0, 1, 0, \ldots, 0)\) \([1\text{ in the }i\text{th position}]\) are the standard basis vectors of \((\mathbb{Z}_2)^n\). Observe that

\[
g_i \odot g_j^T = 0, \quad \text{for all } i, j \quad \text{(4)}
\]

\[
h_i \odot h_j^T = 0, \quad \text{for all } i, j \quad \text{(5)}
\]

\[
g_i \odot h_j^T = 0, \quad \text{for all } i \neq j \quad \text{(6)}
\]

\[
g_i \odot h_i^T = 1, \quad \text{for all } i. \quad \text{(7)}
\]

Thus, the basis vectors come in \(n\) *hyperbolic pairs* \((g_i, h_i)\) such that only the symplectic product between hyperbolic partners is nonzero. The matrix \(J = [g_i \odot h_j^T]\) defining the symplectic product with respect to this basis is given by

\[
J = \begin{pmatrix} 0_{n \times n} & I_{n \times n} \\ I_{n \times n} & 0_{n \times n} \end{pmatrix},
\] (8)

where \(I_{n \times n}\) and \(0_{n \times n}\) are the \(n \times n\) identity and zero matrices, respectively. A basis for \((\mathbb{Z}_2)^{2n}\) whose symplectic product matrix \(J\) is given by (8) is called a *symplectic basis*. In the Pauli picture, the hyperbolic pairs \((g_i, h_i)\) correspond to \((Z^{e_i}, X^{e_i})\) – the anticommuting \(Z\) and \(X\) Pauli matrices acting on the \(i\)th qubit.

In contrast, a subspace \(V\) of \((\mathbb{Z}_2)^{2n}\) is called *isotropic* if (3) holds for all \(v \in V\). The largest isotropic subspace of \((\mathbb{Z}_2)^{2n}\) is \(n\)-dimensional. The span of the \(g_i, i = 1, \ldots, n\), is an example of a subspace saturating this bound.

A general subspace of \((\mathbb{Z}_2)^{2n}\) is neither symplectic nor isotropic. The following theorem says that an arbitrary subspace \(V\) can be decomposed as a direct sum of a symplectic part and an isotropic part.

**Theorem 0.1** Let \(V\) be an \(m\)-dimensional subspace of \((\mathbb{Z}_2)^{2n}\). Then there exists a symplectic basis of \((\mathbb{Z}_2)^{2n}\) consisting of hyperbolic pairs \((u_i, v_i), i = 1, \ldots, n\), such that \(\{u_1, \ldots, u_c+\ell, v_1, \ldots, v_c\}\) is a basis for \(V\), for some \(c, \ell \geq 0\) with \(2c + \ell = m\).
Equivalently,
\[ V = \text{symp}(V) \oplus \text{iso}(V) \]
where \( \text{symp}(V) = \text{span}\{u_1, \ldots, u_c, v_1, \ldots, v_c\} \) is symplectic and \( \text{iso}(V) = \text{span}\{u_{c+1}, \ldots, u_{c+\ell}\} \) is isotropic.

**Remark** It is readily seen that the space \( \text{iso}(V) \) is unique, given \( V \). In contrast, \( \text{symp}(V) \) is not. For instance, replacing \( v_1 \) by \( v'_1 = v_1 + u_{c+1} \) in the above definition of \( \text{symp}(V) \) does not change its symplectic property.

**Proof** Pick an arbitrary basis \( \{w_1, \ldots, w_m\} \) for \( V \) and extend it to a basis \( \{w_1, \ldots, w_{2n}\} \) for \((\mathbb{Z}_2)^{2n}\). We will describe an algorithm which yields the basis from the statement of the theorem.

The procedure consists of \( n \) rounds. In each round a new hyperbolic pair \((u, v)\) is generated; the index \( i \) is added to the set \( \mathcal{U}(V) \) if \( u \in V \) (\( v \in V \)).

Initially set \( i = 1 \), \( m' = m \), and \( \mathcal{U} = \mathcal{V} = \emptyset \). The \( i \)th round reads as follows.

1. We start with vectors \( w_1, \ldots, w_{2(n-i+1)} \), and \( u_1, \ldots, u_{i-1}, v_1, \ldots, v_{i-1} \), such that
   
   (a) \( w_1, \ldots, w_{2(n-i+1)}, u_1, \ldots, u_{i-1}, v_1, \ldots, v_{i-1} \) is a basis for \((\mathbb{Z}_2)^{2n}\),
   
   (b) each of \( u_1, \ldots, u_{i-1}, v_1, \ldots, v_{i-1} \) has vanishing symplectic product with each of \( w_1, \ldots, w_{2(n-i+1)} \),
   
   (c) \( V = \text{span}\{w_j : 1 \leq j \leq m'\} \oplus \text{span}\{u_j : j \in \mathcal{U}\} \oplus \text{span}\{v_j : j \in \mathcal{V}\} \).

   These conditions are satisfied for \( i = 1 \).

2. Define \( u_i = w_1 \). If \( m' \geq 1 \) then add \( i \) to \( \mathcal{U} \). Let \( j \geq 2 \) be the smallest index for which \( w_1 \odot w_j^T = 1 \). Such a \( j \) exists because of (a), (b) and the fact that there exists a \( w \in (\mathbb{Z}_2)^{2n} \) such that \( u_i \odot w^T = 1 \).

   Set \( v_i = w_j \).

3. If \( j \leq m' \):
   
   This means that there is a hyperbolic partner of \( u_i \) in \( V \). Add \( i \) to \( \mathcal{V} \); swap \( w_j \) with \( w_{2(n-i+1)} \); for \( k = 3, \ldots, 2(n-i+1) \) perform
   
   \[ w'_{k-2} := w_k - (v_i \odot w_k^T)u_i - (u_i \odot w_k^T)v_i, \]
   
   so that
   
   \[ w'_{k-2} \odot u_i^T = w'_{k-2} \odot v_i^T = 0; \quad (9) \]
   
   set \( m' := m' - 2 \).

   If \( j > m' \):
   
   This means that there is no hyperbolic partner of \( u_i \) in \( V \). Swap \( w_j \) with \( w_{2(n-i+1)} \); for \( k = 2, \ldots, 2(n-i) + 1 \) perform
   
   \[ w'_{k-1} := w_k - (v_i \odot w_k^T)u_i - (u_i \odot w_k^T)v_i, \]
   
   so that
   
   \[ w'_{k-1} \odot u_i^T = w'_{k-1} \odot v_i^T = 0; \quad (10) \]
   
   if \( m' \geq 1 \) then set \( m' := m' - 1 \).

4. Let \( w_k := w'_k \) for \( 1 \leq k \leq 2(n-i) \). We need to show that the conditions from item 1 are satisfied for the next round \( (i := i + 1) \). Condition (a) holds because \( \{u_i, v_i, w'_1, \ldots, w'_{2(n-i)}\} \) are related to the old \( \{w_1, \ldots, w_{2(n-i+1)}\} \) by an invertible linear transformation. Condition (b) follows from (9) and (10). Regarding condition (c), if \( m' = 0 \) then it holds because \( \mathcal{U} \)
and \( \mathcal{Y} \) did not change from the previous round. Otherwise, consider the two cases in item 3. If \( j \leq m' \) then \( \{ \mathbf{u}_1, \mathbf{v}_1, \ldots, \mathbf{w}'_{m'-2} \} \) are related to the old \( \{ \mathbf{w}_1, \ldots, \mathbf{w}_m \} \) by an invertible linear transformation. If \( j > m' \) then \( \{ \mathbf{u}_1, \mathbf{w}'_1, \ldots, \mathbf{w}'_{m'} \} \) are related to the old \( \{ \mathbf{w}_1, \ldots, \mathbf{w}_m \} \) by an invertible linear transformation (the \( (\mathbf{u}_i \odot \mathbf{w}_k^T) \mathbf{v}_i \) terms vanish for \( 1 \leq k \leq m' \) because there is no hyperbolic partner of \( \mathbf{u}_i \) in \( \mathcal{V} \)).

\[ 0 \leq m' \leq 2(n - i) \] at the end of the \( i \)th round. Thus \( m' = 0 \) after \( n \) rounds and hence \( \mathcal{V} = \text{span}\{ \mathbf{u}_j : j \in \mathcal{U} \} \oplus \text{span}\{ \mathbf{v}_j : j \in \mathcal{V} \} \). The theorem follows by suitably reordering the \( (\mathbf{u}_j, \mathbf{v}_j) \). \( \square \)

A symplectomorphism \( \mathcal{Y} : (\mathbb{Z}_2)^{2n} \to (\mathbb{Z}_2)^{2n} \) is a linear isomorphism which preserves the symplectic form, namely

\[ \mathcal{Y}(\mathbf{u}) \odot \mathcal{Y}(\mathbf{v})^T = \mathbf{u} \odot \mathbf{v}^T. \quad (11) \]

The following theorem relates symplectomorphisms on \((\mathbb{Z}_2)^{2n}\) to unitary maps on \( \mathcal{H}^{\otimes n} \).

**Theorem 0.2** For any symplectomorphism \( \mathcal{Y} \) on \((\mathbb{Z}_2)^{2n}\) there exists a unitary map \( U_\mathcal{Y} \) on \( \mathcal{H}^{\otimes n} \) such that for all \( \mathbf{u} \in (\mathbb{Z}_2)^{2n} \),

\[ [N_{\mathcal{Y}(\mathbf{u})}] = [U_\mathcal{Y} N_\mathbf{u} U_\mathcal{Y}^{-1}]. \]

**Remark.** The unitary map \( U_\mathcal{Y} \) may be viewed as a map on \( [\Pi] \) given by \( [A] \mapsto [U_\mathcal{Y} A U_\mathcal{Y}^{-1}] \). The theorem says that the following diagram commutes

\[ \begin{array}{ccc}
(\mathbb{Z}_2)^{2n} & \xrightarrow{\mathcal{Y}} & (\mathbb{Z}_2)^{2n} \\
[N] \downarrow & & \downarrow [N] \\
[\Pi] & \xrightarrow{U_\mathcal{Y}} & [\Pi]
\end{array} \]

**Proof** Consider the standard basis \( \mathbf{g}_i = (\mathbf{e}_i, \mathbf{0}) \), \( \mathbf{h}_i = (\mathbf{0}, \mathbf{e}_i) \). Define the unique (up to a phase factor) state \( |0\rangle \) on \( \mathcal{H}^{\otimes n} \) to be the simultaneous +1 eigenstate of the commuting operators \( N_{\mathbf{g}_i} \), \( j = 1, \ldots, n \). Define an orthonormal basis \( \{|\mathbf{b}\rangle : \mathbf{b} = b_1 \ldots b_n \in (\mathbb{Z}_2)^n \} \) for \( \mathcal{H}^{\otimes n} \) by

\[ |\mathbf{b}\rangle = N_{\sum_i b_i} |0\rangle. \]

The orthonormality follows from the observation that \( |\mathbf{b}\rangle \) is a simultaneous eigenstate of \( N_{\mathbf{g}_j} \), \( j = 1, \ldots, n \) with respective eigenvalues \((-1)^{b_j} \):

\[ N_{\mathbf{g}_j} |\mathbf{b}\rangle = N_{\mathbf{g}_j} N_{\sum_i b_i} |0\rangle = (-1)^{b_j} N_{\sum_i b_i} N_{\mathbf{g}_j} |0\rangle = (-1)^{b_j} N_{\sum_i b_i} |0\rangle = (-1)^{b_j} N_{\sum_i b_i} |\mathbf{b}\rangle. \quad (12) \]

The second line is an application of (2).

Define \( \tilde{\mathbf{g}}_i := \mathcal{Y}(\mathbf{g}_i) \). We repeat the above construction for this new basis. Define the unique (up to a phase factor) state \( |\tilde{0}\rangle \) to be the simultaneous +1 eigenstate of the commuting operators \( N_{\tilde{\mathbf{g}}_i} \), \( i = 1, \ldots, n \). Define an orthonormal basis \( \{|\tilde{\mathbf{b}}\rangle \} \) by

\[ |\tilde{\mathbf{b}}\rangle = N_{\sum_i \tilde{b}_i} |\tilde{0}\rangle. \quad (13) \]
Defining \( \mathbf{u} = \sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i \), \( \tilde{\mathbf{u}} = \sum_i z_i \tilde{\mathbf{g}}_i + x_i \tilde{\mathbf{h}}_i \) and \( \mathbf{x} = x_1 \ldots x_n \), we have

\[
N_{\mathbf{u}} |\tilde{\mathbf{b}}\rangle = N_{\tilde{\mathbf{u}}} N_{\sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i} |\tilde{\mathbf{0}}\rangle
\]

\[
= (-1)^{\tilde{\mathbf{u}} \cdot (\sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i)} N_{\sum_i z_i \tilde{\mathbf{g}}_i + x_i \tilde{\mathbf{h}}_i} N_{\sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i} |\tilde{\mathbf{0}}\rangle
\]

\[
= (-1)^{\tilde{\mathbf{u}} \cdot (\sum_i z_i \tilde{\mathbf{g}}_i + x_i \tilde{\mathbf{h}}_i)} e^{i\theta(\tilde{\mathbf{u}})} N_{\sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i} |\tilde{\mathbf{0}}\rangle
\]

\[
= (-1)^{\tilde{\mathbf{u}} \cdot (\sum_i z_i \tilde{\mathbf{g}}_i + x_i \tilde{\mathbf{h}}_i)} e^{i\theta(\tilde{\mathbf{u}})} |\mathbf{b} + \mathbf{x}\rangle
\]

\[
= (-1)^{\tilde{\mathbf{u}} \cdot (\sum_i z_i \tilde{\mathbf{g}}_i + x_i \tilde{\mathbf{h}}_i)} e^{i\theta(\tilde{\mathbf{u}})} |\mathbf{b} + \tilde{\mathbf{0}}\rangle,
\]

where \( \theta(\tilde{\mathbf{u}}) \) is a phase factor which is independent of \( \mathbf{b} \). The first equality follows from (13), the second from (2), the third from (1), the fourth from the definition of \( |\tilde{\mathbf{0}}\rangle \) and the fact that \( X^\mathbf{b} X^\mathbf{x} = X^{\mathbf{b} + \mathbf{x}} \), the fifth from (13), and the sixth from (11). Similarly

\[
N_{\mathbf{u}} |\mathbf{b}\rangle = (-1)^{\mathbf{u} \cdot (\sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i)} e^{i\varphi(\mathbf{u})} |\mathbf{b} + \mathbf{x}\rangle,
\]

where \( \varphi(\mathbf{u}) \) is a phase factor which is independent of \( \mathbf{b} \).

Define \( U_T \) by the change of basis

\[
U_T = \sum_b |\tilde{\mathbf{b}}\rangle \langle \mathbf{b}|.
\]

Combining (14) and (15) gives for all \(|\mathbf{b}\rangle\)

\[
N_{\tilde{T}(\mathbf{u})} U_T |\mathbf{b}\rangle = (-1)^{\mathbf{u} \cdot (\sum_i z_i \mathbf{g}_i + x_i \mathbf{h}_i)} e^{i\theta(\tilde{\mathbf{u}})} U_T |\mathbf{b} + \mathbf{x}\rangle
\]

\[
= e^{i[\theta(\tilde{\mathbf{u}}) - \varphi(\mathbf{u})]} U_T N_{\mathbf{u}} |\mathbf{b}\rangle.
\]

Therefore \(|N_{\tilde{T}(\mathbf{u})}| = |U_T N_{\mathbf{u}} U_T^{-1}| \).

\( \square \)

**Relation to quaternary codes**

We shall now show how to construct non-degenerate EAQEC codes from classical codes over GF(4). The addition table of the additive group of the quaternary field \( GF(4) = \{0, 1, \omega, \overline{\omega}\} \) is given by

\[
\begin{array}{cccc}
+ & 0 & \omega & \overline{\omega} \\
0 & 0 & \omega & \overline{\omega} \\
\omega & \overline{\omega} & 0 & \omega \\
\overline{\omega} & \omega & \overline{\omega} & 0
\end{array}
\]

Comparing the above to the addition table of \((\mathbb{Z}_2)^2\) establishes the isomorphism \( \gamma : GF(4) \rightarrow (\mathbb{Z}_2)^2 \), given by the table

<table>
<thead>
<tr>
<th>( GF(4) )</th>
<th>((\mathbb{Z}_2)^2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
</tr>
<tr>
<td>( \overline{\omega} )</td>
<td>01</td>
</tr>
<tr>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>\omega</td>
<td>10</td>
</tr>
</tbody>
</table>

\( \)
The multiplication table for GF(4) is defined as

\[
\begin{array}{c|cccc}
\times & 0 & \omega & 1 & \omega^2 \\
\hline
0 & 0 & 0 & 0 & 0 \\
\omega & 0 & \omega & \omega & 1 \\
1 & 0 & \omega & 1 & \omega \\
\omega & 0 & 1 & \omega & \omega \\
\end{array}
\]

Define the \textit{traces} (Tr) of the elements \{0, 1, \omega, \omega^2\} of GF(4) as \{0, 0, 1, 1\}, and their \textit{conjugates} (\( \omega^4 \)) as \{0, 1, \omega, \omega^2\}. Intuitively, \( \text{Tr} \, a \) measures the “\( \omega \)-ness” of \( a \in GF(4) \). Observe that \( a = 0 \) if and only if both \( \text{Tr} \, \omega \, a = 0 \) and \( \text{Tr} \, \omega^2 \, a = 0 \). The \textit{Hermitian inner product} of two elements \( a, b \in GF(4) \) is defined as \( \langle a, b \rangle = a^\dagger \, b \in GF(4) \). The \textit{trace product} is defined as \( \text{Tr} \langle a, b \rangle \in \mathbb{F}_2 \). The trace product table is readily found to be

\[
\begin{array}{c|cccc}
\text{Tr}(\cdot) & 0 & \omega & 1 & \omega \\
\hline
0 & 0 & 0 & 0 & 0 \\
\omega & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 \\
\omega & 0 & 1 & 1 & 0 \\
\end{array}
\]

Comparing the above to the \( \odot \) table of \((\mathbb{Z}_2)^2\) establishes the identity

\( \text{Tr} \langle a, b \rangle = \gamma(a) \odot \gamma(b) \).

These notions can be generalized to \( n \)-dimensional vector spaces over GF(4). Thus, for \( a, b \in (GF(4))^n \),

\[
\text{Tr}(a, b) = \gamma(a) \odot \gamma(b)^T. \tag{17}
\]

Let \( \text{wt}_4(a) \) be the number of non-zero bits in \( a \in GF(4)^n \). Then we have another identity

\[
\text{wt}(\gamma(a)) = \text{wt}_4(a), \tag{18}
\]

where \( \gamma(a) \in (\mathbb{Z}_2)^{2n} \).

**Proposition 0.3** If a classical \([n, k, d]_4\) code exists then an \([n, 2k - n, d, c]\) EAQEC code exists for some non-negative integer \( c \).

**Proof** Consider a classical \([n, k, d]_4\) code (the subscript 4 emphasizes that the code is over GF(4)) with an \((n-k) \times n\) quaternary parity check matrix \( H_4 \). By definition, for each nonzero \( a \in GF(4)^n \) such that \( \text{wt}_4(a) < d \),

\[
\langle H_4, a \rangle \neq 0^T.
\]

This is equivalent to the logical statement

\[
\text{Tr}(\omega \, H_4, a) \neq 0^T \lor \text{Tr}(\omega^2 \, H_4, a) \neq 0^T.
\]

This is further equivalent to

\[
\text{Tr}(\tilde{H}_4, a) \neq 0^T,
\]

where

\[
\tilde{H}_4 = \begin{pmatrix} \omega \, H_4 \\ \omega^2 \, H_4 \end{pmatrix}. \tag{19}
\]

Define the \((2n - 2k) \times 2n\) symplectic matrix \( H = \gamma(\tilde{H}_4) \). By the correspondences (17) and (18),

\[
H \odot u^T \neq 0^T,
\]
holds for each nonzero \( u \in (\mathbb{Z}_2)^{2n} \) with \( \text{wt}(u) < d \). Thus \( C = \text{rowspace}(H)\perp \) defines a non-degenerate \([n, 2k - n, d; c]\) EAQEC code, where

\[
c = \frac{1}{2} \dim \text{sym}(C).
\]

Any classical binary \([n, k, d]_2\) code may be viewed as an quaternary \([n, k, d]_4\). In this case, the above construction gives rise to a CSS-type code.

**Table of codes**

Below we show a table which includes the best known EAQEC codes, giving the distance \( d \) as a function of the block size \( n \) and number of encoded qubits \( k \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2</td>
<td>2*</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3*</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2*</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2*</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>4*</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2*</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>5*</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

The entries with an asterisk mark the improvements over the best standard QECC.