41076: Methods in Quantum Computing

'Quantum Error Correcting Codes' Module

Min-Hsiu Hsieh
Centre for Quantum Software & Information, Faculty of Engineering and Information Technology, University of Technology Sydney

Contents to be covered in this lecture are

1. Stabilizer Codes
2. Symplectic Codes
3. CSS Construction

Single qubit Pauli group

Recall the set of Pauli matrices over a two-dimensional Hilbert space $\mathcal{H}_2$:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

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

The multiplication table of these matrices is given by:

$\times$	I	X	Y	Z
I	I	X	Y	Z
X	X	I	iZ	$-iY$
Y	Y	$-iZ$	I	iX
Z	Z	iY	$-iX$	I

Observe that the Pauli matrices either commute or anticommute.

Let $[S] = \{\beta S \mid \beta \in \mathbb{C}, |\beta| = 1\}$ be the equivalence class of matrices equal to S up to a phase factor.[1] Let $\mathcal{G}$ be the group generated by the set of Pauli matrices $\{I, X, Y, Z\}$ with all possible phases, then the set $[\mathcal{G}] = \{[I], [X], [Y], [Z]\}$ is readily seen to form a commutative group under the multiplication operation defined by $[S][T] = [ST]$. We called $[\mathcal{G}]$ the Pauli group.

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

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:

$+$	00	01	11	10
00	00	01	11	10
01	01	00	10	11
11	11	10	00	01
10	10	11	01	00

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 product*[2] $\odot : (\mathbb{Z}_2)^2 \times (\mathbb{Z}_2)^2 \to \mathbb{Z}_2$, given by the table

$\odot$	00	01	11	10
00	0	0	0	0
01	0	0	1	1
11	0	1	0	1
10	0	1	1	0

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

$$u \odot v := zx' + z'x.$$

Define the map $N : (\mathbb{Z}_2)^2 \to \mathcal{G}$ by the following table:

$(\mathbb{Z}_2)^2$	$\mathcal{G}$
00	I
01	X
11	Y
10	Z

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 $[N] : (\mathbb{Z}_2)^2 \to [\mathcal{G}]$ 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.

[2]Strictly speaking it is not an inner product.

Multi-qubit Pauli group

Consider an n-qubit system corresponding to the tensor product Hilbert space $\mathcal{H}_2^{\otimes n}$. Define an n-qubit Pauli matrix $\mathbf{S}$ to be of the form $\mathbf{S} = S_1 \otimes S_2 \otimes \cdots \otimes S_n$, where $S_j \in \mathcal{G}$. Let $\mathcal{G}^n$ be the group of all 4^n n-qubit Pauli matrices with all possible phases. Define as before the equivalence class $[\mathbf{S}] = \{\beta\mathbf{S} \mid \beta \in \mathbb{C}, |\beta| = 1\}$. Then

$$[\mathbf{S}][\mathbf{T}] = [S_1T_1] \otimes [S_2T_2] \otimes \cdots \otimes [S_nT_n] = [\mathbf{ST}].$$

Thus the set $[\mathcal{G}^n] = \{[\mathbf{S}] : \mathbf{S} \in \mathcal{G}^n\}$ is a commutative multiplicative group, and is called the n-fold Pauli Group.

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

$$\mathbf{u} \odot \mathbf{v} := \mathbf{z} \cdot \mathbf{x}' + \mathbf{z}' \cdot \mathbf{x},$$

where '$\cdot$' represents the usual inner product of two bit strings in $\mathbb{Z}_2$. Equivalently,

$$\mathbf{u} \odot \mathbf{v} = \sum_i u_i \odot v_i$$

where $u_i = (z_i|x_i), v_i = (z_i'|x_i')$ are the i-th element of $\mathbf{u}, \mathbf{v}$, respectively, and this sum is Boolean addition. Observe that if $\mathbf{u} \odot \mathbf{v} = 0$, these two vectors are "orthogonal" to each other with respect to the symplectic inner product.

The map $N : (\mathbb{Z}_2)^{2n} \to \mathcal{G}^n$ is now defined as

$$N_{\mathbf{u}} = N_{u_1} \otimes \cdots \otimes N_{u_n}.$$

Denote

$$X^{\mathbf{x}} = X^{x_1} \otimes \cdots \otimes X^{x_n},$$
$$Z^{\mathbf{z}} = Z^{z_1} \otimes \cdots \otimes Z^{z_n},$$

as in the single qubit case, we have

$$[N_{(\mathbf{z}|\mathbf{x})}] = [Z^{\mathbf{z}}X^{\mathbf{x}}].$$

The two observations made for the single qubit case also hold:

1. The map $[N] : (\mathbb{Z}_2)^{2n} \to [\mathcal{G}^n]$ induced by N is an isomorphism:

$$[N_{\mathbf{u}}][N_{\mathbf{v}}] = [N_{\mathbf{u}+\mathbf{v}}]. \tag{1}$$

   Consequently, if $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ is a linearly independent set then the elements of the Pauli group subset $\{[N_{\mathbf{u}_1}], \ldots, [N_{\mathbf{u}_m}]\}$ 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

$$N_{\mathbf{u}}N_{\mathbf{v}} = (-1)^{\mathbf{u}\odot\mathbf{v}}N_{\mathbf{v}}N_{\mathbf{u}}. \tag{2}$$

We define the *weight* of a Pauli operator $N_{\mathbf{u}}$, $\mathrm{wt}(N_{\mathbf{u}})$, to be the number of single-qubit Pauli matrices in $N_{\mathbf{u}}$ not equal to the identity I. Define the *weight* of a vector $\mathbf{u} = (\mathbf{z}|\mathbf{x}) \in (\mathbb{Z}_2)^{2n}$ by $\mathrm{wt}_{\mathrm{sp}}(\mathbf{u}) = \mathrm{wt}_2(\mathbf{z} \vee \mathbf{x})$. Here $\vee$ denotes the bitwise logical "or", and $\mathrm{wt}_2(\mathbf{y})$ is the number of non-zero bits in $\mathbf{y} \in (\mathbb{Z}_2)^n$. It is easy to verify that

$$\mathrm{wt}(N_{\mathbf{u}}) = \mathrm{wt}_{\mathrm{sp}}(\mathbf{u}).$$

Structures of the symplectic subspaces

A subspace V of $(\mathbb{Z}_2)^{2n}$ is called *symplectic* [3] if there is no $\mathbf{v} \in V$ such that

$$\mathbf{v} \odot \mathbf{u} = 0, \ \ \forall \mathbf{u} \in V. \tag{3}$$

$(\mathbb{Z}_2)^{2n}$ is itself a symplectic subspace. Consider the standard basis for $(\mathbb{Z}_2)^{2n}$, consisting of $\mathbf{g}_i = (\boldsymbol{e}_i|\mathbf{0})$ and $\mathbf{h}_i = (\mathbf{0}|\boldsymbol{e}_i)$ for $i = 1, \ldots, n$, where $\{\boldsymbol{e}_i\}$ are the standard basis vectors of $(\mathbb{Z}_2)^n$ and $\mathbf{0}$ is a vector of zeros. Observe that

$$\mathbf{g}_i \odot \mathbf{g}_j = 0, \quad \text{for all } i, j \tag{4}$$
$$\mathbf{h}_i \odot \mathbf{h}_j = 0, \quad \text{for all } i, j \tag{5}$$
$$\mathbf{g}_i \odot \mathbf{h}_j = 0, \quad \text{for all } i \neq j \tag{6}$$
$$\mathbf{g}_i \odot \mathbf{h}_i = 1, \quad \text{for all } i. \tag{7}$$

Thus, the basis vectors come in n *hyperbolic pairs* $(\mathbf{g}_i, \mathbf{h}_i)$ such that only the symplectic product between hyperbolic partners is nonzero. The matrix $J = [\mathbf{g}_i \odot \mathbf{h}_j]$ defining the symplectic product with respect to this basis is given by

$$J = \begin{pmatrix} 0_{n\times n} & I_{n\times n} \\ I_{n\times n} & 0_{n\times n} \end{pmatrix}, \tag{8}$$

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 $(\mathbf{g}_i, \mathbf{h}_i)$ correspond to $(Z^{\mathbf{e}_i}, X^{\mathbf{e}_i})$, and are sometimes expressed as (Z_i, X_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* $\mathbf{v} \in V$. The largest isotropic subspace of $(\mathbb{Z}_2)^{2n}$ is n-dimensional. The span of the $\mathbf{g}_i$, $i = 1, \ldots, n$, 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, stated in [3] and rediscovered in Pauli language in [7], says that an arbitrary subspace V can be decomposed as a direct sum of a symplectic part and an isotropic part. Here, we prove this theorem constructively, using a version of the Gram-Schmidt procedure.

Theorem 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 $(\mathbf{u}_i, \mathbf{v}_i)$, $i = 1, \ldots, n$, such that $\{\mathbf{u}_1, \ldots, \mathbf{u}_{c+\ell}, \mathbf{v}_1, \ldots, \mathbf{v}_c\}$ is a basis for V, for some $c, \ell \geq 0$ with $2c + \ell = m$.*

Equivalently,

$$V = \mathrm{symp}(V) \oplus \mathrm{iso}(V)$$

where $\mathrm{symp}(V) = \mathrm{span}\{\mathbf{u}_1, \ldots, \mathbf{u}_c, \mathbf{v}_1, \ldots, \mathbf{v}_c\}$ *is symplectic and* $\mathrm{iso}(V) = \mathrm{span}\{\mathbf{u}_{c+1}, \ldots, \mathbf{u}_{c+\ell}\}$ *is isotropic.*

Proof. Pick an arbitrary basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$ for V and extend it to a basis $\{\mathbf{w}_1, \ldots, \mathbf{w}_{2n}\}$ for $(\mathbb{Z}_2)^{2n}$. The procedure consists of n rounds. In each round a new hyperbolic pair $(\mathbf{u}_i, \mathbf{v}_i)$ is generated; the index i is added to the set $\mathcal{U}$ (respectively, $\mathcal{V}$) if $\mathbf{u}_i \in V$ ($\mathbf{v}_i \in V$).

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

1. We start with vectors $\mathbf{w}_1, \ldots, \mathbf{w}_{2(n-i+1)}$, and $\mathbf{u}_1, \ldots \mathbf{u}_{i-1}, \mathbf{v}_1, \ldots \mathbf{v}_{i-1}$, such that

   (a) $\mathbf{w}_1, \ldots, \mathbf{w}_{2(n-i+1)}$, $\mathbf{u}_1, \ldots \mathbf{u}_{i-1}$,$\mathbf{v}_1, \ldots \mathbf{v}_{i-1}$ is a basis for $(\mathbb{Z}_2)^{2n}$,

   (b) each of $\mathbf{u}_1, \ldots \mathbf{u}_{i-1}, \mathbf{v}_1, \ldots \mathbf{v}_{i-1}$ has vanishing symplectic product with each of $\mathbf{w}_1, \ldots, \mathbf{w}_{2(n-i+1)}$,

   (c) $V = \mathrm{span}\{\mathbf{w}_j : 1 \le j \le m'\} \oplus \mathrm{span}\{\mathbf{u}_j : j \in \mathcal{U}\} \oplus \mathrm{span}\{\mathbf{v}_j : j \in \mathcal{V}\}$.

   These conditions are satisfied for $i = 1$ where we begin with vectors $\mathbf{w}_1, \ldots, \mathbf{w}_{2n}$. In this case, we implicitly assume that ($\mathbf{u}_0$, $\mathbf{v}_0$) is the empty set.

2. Define $\mathbf{u}_i = \mathbf{w}_1$. If $m' \ge 1$ then and add i to $\mathcal{U}$. Let $j \ge 2$ be the smallest index for which $\mathbf{w}_1 \odot \mathbf{w}_j = 1$. Such a j exists because of (a), (b) and the fact that there exists a $\mathbf{w} \in (\mathbb{Z}_2)^{2n}$ such that $\mathbf{u}_i \odot \mathbf{w} = 1$.

   Set $\mathbf{v}_i = \mathbf{w}_j$.

3. If $j \le m'$:

   This means that there is a hyperbolic partner of $\mathbf{u}_i$ in V. Add i to $\mathcal{V}$; swap $\mathbf{w}_j$ with $\mathbf{w}_2$; for $k = 3, \ldots, 2(n-i+1)$ perform

   $$\mathbf{w}'_{k-2} := \mathbf{w}_k - (\mathbf{v}_i \odot \mathbf{w}_k)\mathbf{u}_i - (\mathbf{u}_i \odot \mathbf{w}_k)\mathbf{v}_i,$$

   so that

   $$\mathbf{w}'_{k-2} \odot \mathbf{u}_i = \mathbf{w}'_{k-2} \odot \mathbf{v}_i = 0; \tag{9}$$

   set $m' := m' - 2$.

   If $j > m'$:

   This means that there is no hyperbolic partner of $\mathbf{u}_i$ in V. Swap $\mathbf{w}_j$ with $\mathbf{w}_{2(n-i+1)}$; for $k = 2, \ldots, 2(n-i)+1$ perform

   $$\mathbf{w}'_{k-1} := \mathbf{w}_k - (\mathbf{v}_i \odot \mathbf{w}_k)\mathbf{u}_i - (\mathbf{u}_i \odot \mathbf{w}_k)\mathbf{v}_i,$$

   so that

   $$\mathbf{w}'_{k-1} \odot \mathbf{u}_i = \mathbf{w}'_{k-1} \odot \mathbf{v}_i = 0; \tag{10}$$

   if $m' \ge 1$ then set $m' := m' - 1$.

4. Let $\mathbf{w}_k := \mathbf{w}'_k$ for $1 \le k \le 2(n-i)$. We need to show that the conditions from item 1 are satisfied for the next round ($i := i + 1$). Condition (a) holds because $\{\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}'_1, \ldots \mathbf{w}'_{2(n-i)}\}$ are related to the old $\{\mathbf{w}_1, \ldots \mathbf{w}_{2(n-i+1)}\}$ 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 $\mathcal{V}$ did not change from the previous round. Otherwise, consider the two cases in item 3. If $j \le m'$ then $\{\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}'_1, \ldots \mathbf{w}'_{m'-2}\}$ are related to the old $\{\mathbf{w}_1, \ldots \mathbf{w}_{m'}\}$ by an invertible linear transformation. If $j > m'$ then $\{\mathbf{u}_i, \mathbf{w}'_1, \ldots \mathbf{w}'_{m'-1}\}$ are related to the old $\{\mathbf{w}_1, \ldots \mathbf{w}_{m'}\}$ by an invertible linear transformation (the $(\mathbf{u}_i \odot \mathbf{w}_k)\mathbf{v}_i$ terms vanish for $1 \le k \le m'$ because there is no hyperbolic partner of $\mathbf{u}_i$ in V).

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

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

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

$$\Upsilon(\mathbf{u}) \odot \Upsilon(\mathbf{v}) = \mathbf{u} \odot \mathbf{v}. \tag{11}$$

The following theorem relates symplectomorphisms on $(\mathbb{Z}_2)^{2n}$ to unitary maps on $\mathcal{H}_2^{\otimes n}$. It appears, for instance, in [2]. For completeness, we give an independent proof here.

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

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

Remark. The unitary map U_Υ may be viewed as a map on $[\mathcal{G}_n]$ given by $[\mathbf{S}] \mapsto [U_\Upsilon \mathbf{S} U_\Upsilon^{-1}]$. The theorem says that the following diagram commutes

$$\begin{array}{ccc} (\mathbb{Z}_2)^{2n} & \xrightarrow{\Upsilon} & (\mathbb{Z}_2)^{2n} \\ {\scriptstyle [N]}\downarrow & & \downarrow{\scriptstyle [N]} \\ [\mathcal{G}_n] & \xrightarrow{U_\Upsilon} & [\mathcal{G}_n] \end{array}$$

Corollary 3. *Let $\mathcal{V}$ be an arbitrary subgroup of $\mathcal{G}_n$ with size 2^m. Then there exists a set of generators $\{\bar{Z}_1, \cdots, \bar{Z}_{p+q}, \bar{X}_{p+1}, \cdots, \bar{X}_{p+q}\}$ that generates $\mathcal{V}$ such that the $\bar{Z}$'s and $\bar{X}$'s obey the same commutation relations as in (12), for some $p, q \geq 0$ and $p + 2q = m$.*

$$\begin{aligned} [\bar{Z}_i, \bar{Z}_j] &= 0 \quad \forall i, j \\ [\bar{X}_i, \bar{X}_j] &= 0 \quad \forall i, j \\ [\bar{X}_i, \bar{Z}_j] &= 0 \quad \forall i \neq j \\ \{\bar{X}_i, \bar{Z}_i\} &= 0 \quad \forall i. \end{aligned} \tag{12}$$

Proof. Though the proof can be found in [7]; however, a new proof can be easily obtained by combining Theorem 1 and the isomorphic map $[N] : (\mathbb{Z}_2)^{2n} \to [\mathcal{G}_n]$. □

Symplectic codes

An $[n, k]$ symplectic code C_{sp} defined by an $(n-k) \times 2n$ parity check matrix H_{sp} is given by

$$C_{\text{sp}} = \text{rowspace}(H_{\text{sp}})^\perp$$

where

$$V^\perp = \{\mathbf{w} : \mathbf{w} \odot \mathbf{u} = 0, \ \forall \mathbf{u} \in V\}.$$

The subscript sp emphasizes that the code is defined with respect to the symplectic product. Note that $(V^\perp)^\perp = V$. We say that $C_{\rm sp}$ is *dual-containing* if

$$(C_{\rm sp})^\perp = \text{rowspace}(H_{\rm sp}) \subset C_{\rm sp}; \tag{13}$$

this is true if H_{sp} is *self-orthogonal* under the symplectic product. For simplicity, the term "self-orthogonal code" is often referred to a code with a self-orthogonal parity-check matrix.

The notion of *distance* provides a convenient way to characterize the error-correcting properties of a code. An $[n, k]$ symplectic code $C_{\rm sp}$ with a parity check matrix $H_{\rm sp}$ is said to have distance d if for each nonzero $\mathbf{u}$ of weight $< d$, $\mathbf{u} \notin C_{\rm sp}$, or equivalently, $H_{\rm sp} \odot \mathbf{u} \neq \mathbf{0}$.

Encoding classical information into quantum states

In this section we review two schemes for sending classical information over quantum channels: elementary coding and superdense coding. These will be used later in the context of quantum error correction to convey information to the decoder about which error happened.

Elementary coding

In the first scheme, Alice and Bob are connected by a perfect qubit channel. Alice can send an arbitrary bit $a \in \mathbb{Z}_2$ over the qubit channel in the following way:

- Alice locally prepares a state $|0\rangle$ in $\mathcal{H}_2$. This state is the $+1$ eigenstate of the Z operator. Based on her message a, she performs the encoding operation X^a, producing the state $|a\rangle = X^a|0\rangle$.
- Alice sends the encoded state to Bob through the qubit channel.
- Bob decodes by performing the von Neumann measurement in the $\{|0\rangle, |1\rangle\}$ basis. As this is the unique eigenbasis of the Z operator, this is equivalently called "measuring the Z observable".

We call this protocol "elementary coding" and write it symbolically as a *resource inequality* [4, 5] [3]

$$[q \to q] \geq [c \to c].$$

Here $[q \to q]$ represents a perfect qubit channel and $[c \to c]$ represents a perfect classical bit channel. The inequality $\geq$ signifies that the resource on the left hand side can be used in a protocol to simulate the resource on the right hand side.

Elementary coding immediately extends to m qubits. Alice prepares the simultaneous $+1$ eigenstate of the $Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m}$ operators $|\mathbf{0}\rangle$, and encodes the message $\mathbf{a} \in (\mathbb{Z}_2)^m$ by applying $X^{\mathbf{a}}$, producing the encoded state $|\mathbf{a}\rangle = X^{\mathbf{a}}|\mathbf{0}\rangle$. Bob decodes by simultaneously measuring the $Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m}$ observables. We could symbolically represent this protocol by

$$m\,[q \to q] \geq m\,[c \to c].$$

[3] In [4] resource inequalities were used in the asymptotic sense. Here they refer to finite protocols, and are thus slightly abusing their original intent.

Superdense coding

In the second scheme, Alice and Bob share the ebit state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \tag{14}$$

in addition to being connected by the qubit channel. In (14) Alice's state is to the left and Bob's is to the right of the $\otimes$ symbol.

The state $|\Phi\rangle$ is the simultaneous $(+1, +1)$ eigenstate of the commuting operators $Z \otimes Z$ and $X \otimes X$. Again, the operator to the left of the $\otimes$ symbol acts on Alice's system and the operator to the right of the $\otimes$ symbol acts on Bob's system. Alice can send a two-bit message $(a_1, a_2) \in (\mathbb{Z}_2)^2$ to Bob using "superdense coding" [1]:

- Based on her message (a_1, a_2), Alice performs the encoding operation $Z^{a_1} X^{a_2}$ on her part of the state $|\Phi\rangle$, producing the state $|a_1, a_2\rangle = (Z^{a_1} X^{a_2} \otimes I^B)|\Phi\rangle$.
- Alice sends her part of the encoded state to Bob through the perfect qubit channel.
- Bob decodes by performing the von Neumann measurement in the $\{(Z^{a_1} X^{a_2} \otimes I)|\Phi\rangle : (a_1, a_2) \in (\mathbb{Z}_2)^2\}$ basis, i.e., by simultaneously measuring the $Z \otimes Z$ and $X \otimes X$ observables.

The protocol is represented by the resource inequality

$$[q \to q] + [q\, q] \geq 2\, [c \to c], \tag{15}$$

where $[q\, q]$ now represents the shared ebit. It can also be extended to m copies. Alice and Bob share the state $|\Phi\rangle^{\otimes m}$ which is the simultaneous $+1$ eigenstate of the $Z^{\mathbf{e}_1} \otimes Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m} \otimes Z^{\mathbf{e}_m}$ and $X^{\mathbf{e}_1} \otimes X^{\mathbf{e}_1}, \ldots, X^{\mathbf{e}_m} \otimes X^{\mathbf{e}_m}$ operators. Alice encodes the message $(\mathbf{a}_1, \mathbf{a}_2) \in (\mathbb{Z}_2)^{2m}$ by applying $Z^{\mathbf{a}_1} X^{\mathbf{a}_2}$, producing the encoded state $|\mathbf{a}_1, \mathbf{a}_2\rangle = (Z^{\mathbf{a}_1} X^{\mathbf{a}_2} \otimes I)|\Phi\rangle$. Bob decodes by simultaneously measuring the $Z^{\mathbf{e}_1} \otimes Z^{\mathbf{e}_1}, \ldots, Z^{\mathbf{e}_m} \otimes Z^{\mathbf{e}_m}$ and $X^{\mathbf{e}_1} \otimes X^{\mathbf{e}_1}, \ldots, X^{\mathbf{e}_m} \otimes X^{\mathbf{e}_m}$ observables. The corresponding resource inequality is

$$m\, [q \to q] + m\, [q\, q] \geq 2m\, [c \to c].$$

Superdense coding provides the simplest illustration of how entanglement can increase the power of information processing.

Discretization of errors

It is well known that for standard quantum error correction (i.e., that unassisted by entanglement) it suffices to consider errors from the Pauli group (see e.g. [8].) We will review this result here.

Denote by $\mathcal{L}$ the space of linear operators defined on the qubit Hilbert space $\mathcal{H}_2$. In general, a noisy channel is defined by a completely positive, trace preserving (CPTP) map $\mathcal{N} : \mathcal{L}^{\otimes n} \to \mathcal{L}^{\otimes n}$ taking n-qubit density operators on Alice's system to density operators on Bob's system. We will often encounter isometric operators $U : \mathcal{H}_2^{\otimes n_1} \to \mathcal{H}_2^{\otimes n_2}$. The corresponding *superoperator*, or CPTP map, is marked by a hat $\hat{U} : \mathcal{L}^{\otimes n_1} \to \mathcal{L}^{\otimes n_2}$ and defined by

$$\hat{U}(\rho) = U \rho U^\dagger.$$

Observe that $\hat{U}$ is independent of any phases factors multiplying U. Thus, for a Pauli operator $N_{\mathbf{u}}$, $\hat{N}_{\mathbf{u}}$ only depends on the equivalence class $[N_{\mathbf{u}}]$.

Our communication scenario involves two spatially separated parties, Alice and Bob, connected by a noise channel $\mathcal{N}$. Alice wishes to send k qubits *perfectly* to Bob through $\mathcal{N}$. An $[[n, k]]$ QECC consists of

- An encoding isometry $\mathcal{E} = \hat{U}_{\text{enc}} : \mathcal{L}^{\otimes k} \to \mathcal{L}^{\otimes n}$
- A decoding CPTP map $\mathcal{D} : \mathcal{L}^{\otimes n} \to \mathcal{L}^{\otimes k}$

such that

$$\mathcal{D} \circ \mathcal{N} \circ \hat{U}_{\text{enc}} = \text{id}^{\otimes k},$$

where $\text{id} : \mathcal{L} \to \mathcal{L}$ is the identity map on a single qubit.

To make contact with classical error correction it is necessary to discretize the errors introduced by $\mathcal{N}$. This is done in two steps. First, the CPTP map $\mathcal{N}$ may be (non-uniquely) written in terms of its Kraus representation

$$\mathcal{N}(\rho) = \sum_i A_i \rho A_i^\dagger.$$

Second, each A_i may be expanded in the Pauli operators

$$A_i = \sum_{\mathbf{u} \in (\mathbb{Z}_2)^{2n}} \alpha_{i,\mathbf{u}} N_{\mathbf{u}}.$$

Define the support of $\mathcal{N}$ by $\text{supp}(\mathcal{N}) = \{\mathbf{u} \in (\mathbb{Z}_2)^{2n} : \exists i, \alpha_{i,\mathbf{u}} \neq 0\}$. The following theorem allows us to replace the continuous map $\mathcal{N}$ by the error set $S = \text{supp}(\mathcal{N})$.

Theorem 4. *If* $\mathcal{D} \circ \hat{N}_{\mathbf{u}} \circ \hat{U}_{\text{enc}} = \text{id}^{\otimes k}$ *for all* $\mathbf{u} \in \text{supp}(\mathcal{N})$*, then* $\mathcal{D} \circ \mathcal{N} \circ \hat{U}_{\text{enc}} = \text{id}^{\otimes k}$*.*

Proof. We may extend the map $\mathcal{D}$ to its Stinespring dilation – an isometric map $\hat{U}_{\text{dec}}$ with a larger target Hilbert space $\mathcal{L}^{\otimes n} \otimes \mathcal{L}'$, such that

$$\mathcal{D}(\rho) = \text{Tr}_{\mathcal{L}'} \hat{U}_{\text{dec}}(\rho).$$

If for all $\mathbf{u} \in \text{supp}(\mathcal{N})$ and all pure states $|\psi\rangle$ in $\mathcal{H}_2^{\otimes k}$, the following equation holds

$$U_{\text{dec}} N_{\mathbf{u}} U_{\text{enc}} |\psi\rangle = |\psi\rangle \otimes |\mathbf{u}\rangle$$

for some pure state $|\mathbf{u}\rangle\langle\mathbf{u}|$ on $\mathcal{L}'$, then by linearity, we have

$$U_{\text{dec}} A_i U_{\text{enc}} |\psi\rangle = |\psi\rangle \otimes |i\rangle,$$

with the unnormalized state $|i\rangle = \sum_{\mathbf{u}} \alpha_{i,\mathbf{u}} |\mathbf{u}\rangle$. Furthermore,

$$\begin{aligned} (\hat{U}_{\text{dec}} \circ \mathcal{N} \circ \hat{U}_{\text{enc}})(|\psi\rangle\langle\psi|) &= U_{\text{dec}} \left(\sum_i A_i U_{\text{enc}} |\psi\rangle\langle\psi| U_{\text{enc}}^\dagger A_i^\dagger \right) U_{\text{dec}}^\dagger \\ &= |\psi\rangle\langle\psi| \otimes \sum_i |i\rangle\langle i|, \end{aligned} \tag{16}$$

where the second subsystem corresponds to $\mathcal{L}'$. Tracing out the latter gives

$$(\mathcal{D} \circ \mathcal{N} \circ \hat{U}_{\text{enc}})(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|,$$

concluding the proof. □

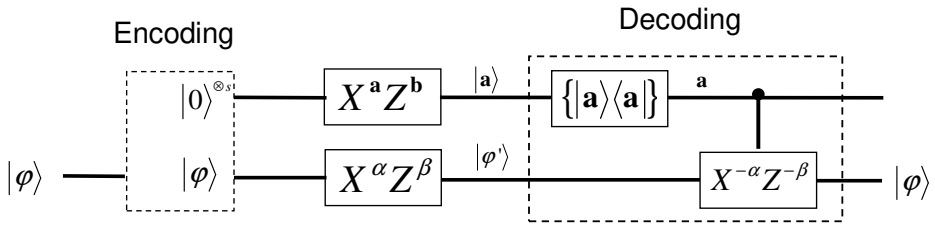

Figure 1: A canonical quantum error-correcting code.

Canonical codes

We first introduce the simplest form of standard quantum error-correcting codes (QECCs), the canonical codes. The canonical code $\mathcal{C}_0$ is defined by the following trivial encoding operation

$$U_0 : |\varphi\rangle \mapsto |\mathbf{0}\rangle|\varphi\rangle. \tag{17}$$

In other words, the register containing $|\mathbf{0}\rangle$ (of size $s = n - k$ qubits) is appended to the registers containing $|\varphi\rangle$ (of size k qubits). We call the encoded state in (17) a *codeword* of $\mathcal{C}_0$. We will denote $\mathcal{E}_0 = \hat{U}_0 \equiv U_0(\cdot)U_0^\dagger$. What errors can this canonical code $\mathcal{C}_0$ correct with such a simple-minded encoding?

Proposition 5. *The encoding given by $\mathcal{E}_0$ and a suitably-defined decoding map $\mathcal{D}_0$ can correct the error set*

$$\mathbf{E}_0 = \{X^{\mathbf{a}}Z^{\mathbf{b}} \otimes X^{\alpha(\mathbf{a})}Z^{\beta(\mathbf{a})} : \mathbf{a}, \mathbf{b} \in (\mathbb{Z}_2)^s\}, \tag{18}$$

for any fixed functions $\alpha, \beta : (\mathbb{Z}_2)^s \to (\mathbb{Z}_2)^k$.

Proof. The protocol is shown in Figure 1. After applying an error $E \in \mathbf{E}_0$, the channel output becomes (up to a phase factor):

$$E(|\mathbf{0}\rangle \otimes |\varphi\rangle) = (X^{\mathbf{a}}Z^{\mathbf{b}})|\mathbf{0}\rangle \otimes (X^{\alpha(\mathbf{a})}Z^{\beta(\mathbf{a})})|\varphi\rangle = |\mathbf{a}\rangle \otimes |\varphi'\rangle \tag{19}$$

where $|\mathbf{a}\rangle = X^{\mathbf{a}}|\mathbf{0}\rangle$, and $|\varphi'\rangle = (X^{\alpha(\mathbf{a})}Z^{\beta(\mathbf{a})})|\varphi\rangle$.

As the vector $(\mathbf{a}, \mathbf{b})$ completely specifies the error operator E, it is called the *error syndrome*. However, in order to correct this error, only the *reduced syndrome*, $\mathbf{a}$, matters. In effect, $\mathbf{a}$ has been encoded using elementary coding, and the receiver Bob can identify the reduced syndrome by simultaneously measuring the $Z^{\mathbf{e}_1}, \cdots, Z^{\mathbf{e}_s}$ observables. He then performs $X^{-\alpha(\mathbf{a})}Z^{-\beta(\mathbf{a})}$ on the remaining k-qubit system $|\varphi'\rangle$, returning it to the original state $|\varphi\rangle$.

Since the goal is the transmission of quantum information, no actual measurement is necessary. Instead, Bob can perform the CPTP decoding operation $\mathcal{D}_0$ consisting of the controlled unitary

$$U_{0,\text{dec}} = \sum_{\mathbf{a}} |\mathbf{a}\rangle\langle\mathbf{a}| \otimes X^{-\alpha(\mathbf{a})}Z^{-\beta(\mathbf{a})}, \tag{20}$$

which is constructed based on the reduced syndrome, and is also known as *collective measurement*, followed by discarding the unwanted systems. □

We can rephrase the above error-correcting procedure in terms of the stabilizer formalism. Let $\mathcal{S}_0 = \langle Z_1, \cdots, Z_s \rangle$ be an Abelian group of size 2^s. Group $\mathcal{S}_0$ is called the stabilizer for $\mathcal{C}_0$, since every element of $\mathcal{S}_0$ fixes the codewords of $\mathcal{C}_0$. Notice that we have used Z_i to represent $Z^{\mathbf{e}_i}$ here for simplicity.

Proposition 6. *The QECC $\mathcal{C}_0$ defined by $\mathcal{S}_0$ can correct an error set $\mathbf{E}_0$ if for all $E_1, E_2 \in \mathbf{E}_0$, $E_2^\dagger E_1 \in \mathcal{S}_0 \bigcup (\mathcal{G}_n - \mathcal{Z}(\mathcal{S}_0))$, where $\mathcal{Z}(\mathcal{S})$ is the normalizer of group $\mathcal{S}$.*

Proof. Since the vector $(\mathbf{a}, \mathbf{b})$ completely specifies the error operator E, we consider the following two different cases:

- If two error operators E_1 and E_2 have the same reduced syndrome $\mathbf{a}$, then the error operator $E_2^\dagger E_1$ gives us the all-zero reduced syndrome. Therefore, $E_2^\dagger E_1 \in \mathcal{S}_0$. This error $E_2^\dagger E_1$ has no effect on the codeword.
- If two error operators E_1 and E_2 have different reduced syndromes, and let $\mathbf{a}$ be the reduced syndrome of $E_2^\dagger E_1$, then $E_2^\dagger E_1 \notin \mathcal{Z}(\mathcal{S}_0)$. This error $E_2^\dagger E_1$ can be corrected by the decoding operation given in (20).

□

The general case

We will need some lemmas to transform the canonical codes into practical/useful quantum codes.

The following lemma is a simply result from group theory, and a new proof can be obtained from Theorem 2 and $[N] : (\mathbb{Z}_2)^{2n} \to [\mathcal{G}_n]$.

Lemma 7. *If there is a one-to-one map between $\mathcal{V}$ and $\mathcal{S}$ which preserves their commutation relations, which we denote $\mathcal{V} \sim \mathcal{S}$, then there exists a unitary U such that for each $V_i \in \mathcal{V}$, there is a corresponding $S_i \in \mathcal{S}$ such that $V_i = U S_i U^{-1}$, up to a phase which can differ for each generator.*

Lemma 8. *Performing U followed by measuring the operator $\mathbf{A}$ is equivalent to measuring the operator $U^{-1}\mathbf{A}U$ followed by performing U.*

Proof. Let Π_i be a projector onto the eigenspace corresponding to eigenvalue λ_i of $\mathbf{A}$. Performing U followed by measuring the operator $\mathbf{A}$ is equivalent to the instrument (generalized measurement) given by the set of operators $\{\Pi_i U\}$. The operator $U^{-1}\mathbf{A}U$ has the same eigenvalues as $\mathbf{A}$, and the projector onto the eigenspace corresponding to eigenvalue λ_i is $U^{-1}\Pi_i U$. Measuring the operator $U^{-1}\mathbf{A}U$ followed by performing U is equivalent to the instrument $\{U(U^{-1}\Pi_i U)\} = \{\Pi_i U\}$. □

Lemma 9. *If $\mathcal{C}_0$ is a simultaneous eigenspace of Pauli operators from the set $\mathcal{S}_0'$, then $\mathcal{C} = U^{-1}(\mathcal{C}_0)$ is a simultaneous eigenspace of Pauli operators from the set $\mathcal{S} = \{U^{-1}\mathbf{A}U : \mathbf{A} \in \mathcal{S}_0'\}$.*

Proof. Observe that if

$$\mathbf{A}|\psi\rangle = \alpha|\psi\rangle,$$

then

$$(U^{-1}\mathbf{A}U)U^{-1}|\psi\rangle = \alpha U^{-1}|\psi\rangle.$$

□

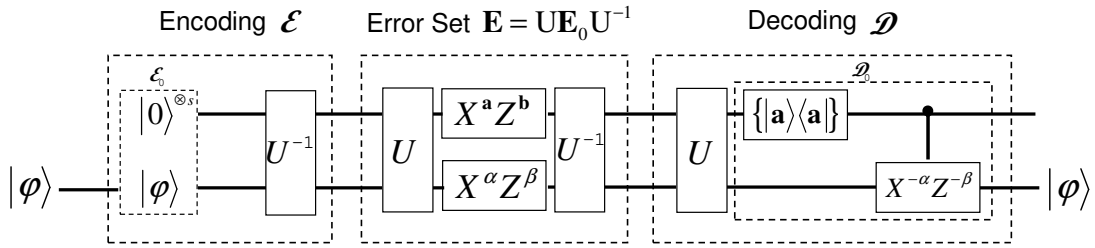

Figure 2: A standard quantum error-correcting code.

Theorem 10. *Given an Abelian group $\mathcal{S}_I$ of size 2^{n-k} that does not contain $-I$, there exists an $[[n,k]]$ quantum error-correcting code $\mathcal{C}$ defined by the encoding and decoding pair $(\mathcal{E},\mathcal{D})$ with the following properties:*

1. *The code $\mathcal{C}$ can correct the error set $\mathbf{E}$ if for all $E_1, E_2 \in \mathbf{E}$, $E_2^\dagger E_1 \in \mathcal{S}_I \bigcup (\mathcal{G}_n - \mathcal{Z}(\mathcal{S}_I))$.*
2. *The codespace $\mathcal{C}$ is a simultaneous eigenspace of the $\mathcal{S}_I$.*
3. *To decode, the reduced error syndrome is obtained by simultaneously measuring the observables from $\mathcal{S}_I$.*

Proof. The protocol is shown in Figure 2. Since $\mathcal{S}_I$ has the same commutation relations with the stabilizer $\mathcal{S}_0$ of the canonical code $\mathcal{C}_0$ given in the previous section, by Lemma 8, there exists an unitary matrix U such that $\mathcal{S}_0 = U\mathcal{S}_I U^{-1}$. Define $\mathcal{E} = U^{-1} \circ \mathcal{E}_0$ and $\mathcal{D} = \mathcal{D}_0 \circ U$, where $\mathcal{E}_0$ and $\mathcal{D}_0$ are given in (17) and (20), respectively.

1. Let $\mathbf{E}_0$ be the error set that can be corrected by $\mathcal{C}_0$. Then by Proposition 6,

   $$\mathcal{D}_0 \circ E_0 \circ \mathcal{E}_0 = \mathrm{id}^{\otimes k}$$

   for any $E_0 \in \mathbf{E}_0$. Let $\mathbf{E} = \{U^{-1}E_0U : \forall E_0 \in \mathbf{E}_0\}$. It follows that, for any $E \in \mathbf{E}$,

   $$\mathcal{D} \circ E \circ \mathcal{E} = \mathrm{id}^{\otimes k}.$$

   Thus, the encoding and decoding pair $(\mathcal{E},\mathcal{D})$ corrects $\mathbf{E}$. Following Proposition 7, the correctable error set $\mathbf{E}$ contains all E_1, E_2 such that $E_2^\dagger E_1 \in \mathcal{S}_I \bigcup (\mathcal{G}_n - \mathcal{Z}(\mathcal{S}_I))$.

2. Since $\mathcal{C}_0$ is the simultaneous $+1$ eigenspace of $\mathcal{S}_0$, and $\mathcal{S}_I = U^{-1}\mathcal{S}_0U$, Lemma 10 guarantees that the codespace $\mathcal{C}$ after encoding $\mathcal{E}$ is a simultaneous eigenspace of $\mathcal{S}_I$.

3. The decoding operation $\mathcal{D}_0$ involves

   (a) measuring the set of generators of $\mathcal{S}_0$, yielding the error syndrome according to the error E_0.

   (b) performing a recovering operation E_0 again to undo the error.

   By Lemma 9, performing $\mathcal{D} = \mathcal{D}_0 \circ U$ is equivalent to measuring $\mathcal{S}_I = U^{-1}\mathcal{S}_0U$, followed by performing the recovering operation $U^{-1}E_0U$, followed by U to undo the encoding.

□

We said an $[[n, k]]$ QECC defined by $\mathcal{S}_I$ to have distance d, if for all operators E_1 and E_2 with weigh $< d$ and $E_1 \neq E_2$, either

1. $E_2^\dagger E_1 \notin \mathcal{G}_n - \mathcal{Z}(\mathcal{S}_I)$, or
2. $E_2^\dagger E_1 \in \mathcal{S}_I$.

The code is called *non-degenerate* if the second condition is not invoked. A QECC with distance d can correct up to t-qubit errors, where $t = \lfloor (d-1)/2 \rfloor$. Such code is called an $[[n, k, d]]$ QECC.

Relation to symplectic codes

Proposition 11. *Consider an $[n, k, d]$ symplectic code C_{sp} defined by H_{sp}. If C_{sp} is dual-containing, then C_{sp} defines a non-degenerate $[[n, k, d]]$ QECC.*

Proof. Since H_{sp} is self-orthogonal, that means the group $\mathcal{S}_I$ generated by the operator $g_i = N_{\mathbf{r}_i}$, where $\mathbf{r}_i$ is the i-th row of H_{sp}, is an Abelian group with size 2^{n-k}. From Theorem 11, $\mathcal{S}_I$ defines an $[[n, k]]$ QECC $\mathcal{C}$.

For all vectors $\mathbf{u}_1, \mathbf{u}_2$ with weight $< t$, where $t = \lfloor (d-1)/2 \rfloor$, we have

$$H_{sp} \odot (\mathbf{u}_1 - \mathbf{u}_2) \neq \mathbf{0},$$

or, equivalently,

$$N_{\mathbf{u}_2}^\dagger N_{\mathbf{u}_1} \notin \mathcal{G}_n - \mathcal{Z}(\mathcal{S}_I).$$

Therefore $\mathcal{C}$ is a non-degenerate QECC with distance d.

□

The CSS construction

Proposition 12. *Given a dual-containing classical binary codes $[n, k, d]$ C, there exists an $[[n, 2k-n, d]]$ QECC.*

Proof. Let H be the parity check matrix of C. Since

$$\text{rowspace}(H) = C^\perp \subset C = \text{rowspace}(H)^\perp,$$

therefore

$$H_{sp} = \left(\begin{array}{c|c} H & \mathbf{0} \\ \mathbf{0} & H \end{array} \right), \tag{21}$$

is dual-containing, and defines an $[n, 2k-n]$ symplectic code C_{sp}. By definition of classical linear codes, for each nonzero $\mathbf{a} \in (\mathbb{Z}_2)^n$ such that $\text{wt}(\mathbf{a}) < d$,

$$\langle H, \mathbf{a} \rangle \neq \mathbf{0}^T,$$

Then

$$H_{sp} \odot \mathbf{u} \neq \mathbf{0},$$

holds for each nonzero $\mathbf{u} \in (\mathbb{Z}_2)^{2n}$ with $\text{wt}(\mathbf{u}) < d$. Thus C_{sp} defines a non-degenerate $[[n, 2k-n, d]]$ QECC by Proposition 12. □

Actually, instead of using the same code C, one can use two codes C_1 and C_2, such that $C_1 \subset C_2$, in the CSS construction [8]. Furthermore, the CSS code have one interesting property that its generators contain all X's and protect against phase flips and generators contain all Z's and protect against bit flips.

Examples

The first quantum error-correcting code constructed by Shor [9] was a quantum analog of the classical repetition code, which stores information redundantly by duplicating each bit several times. We list the stabilizer generators for the $[[9, 1, 3]]$ Shor code in Table 1. It is easy to verify that it can correct arbitrary single-qubit error.

S_1	Z	Z	I	I	I	I	I	I	I
S_2	I	Z	Z	I	I	I	I	I	I
S_3	I	I	I	Z	Z	I	I	I	I
S_4	I	I	I	I	Z	Z	I	I	I
S_5	I	I	I	I	I	I	Z	Z	I
S_6	I	I	I	I	I	I	I	Z	Z
S_7	X	X	X	I	I	I	X	X	X
S_8	X	X	X	X	X	X	I	I	I
$\bar{Z}$	Z	Z	Z	Z	Z	Z	Z	Z	Z
$\bar{X}$	X	X	X	X	X	X	X	X	X

Table 1: The [[9,1,3]] Shor code.

The second example, the $[[7, 1, 3]]$ Steane code, is constructed using the CSS construction from dual-containing $[7, 4, 3]$ Hamming code with the parity check matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{22}$$

We list the stabilizer generators in Table 2.

S_1	I	I	I	Z	Z	Z	Z
S_2	I	Z	Z	I	I	Z	Z
S_3	Z	I	Z	I	Z	I	Z
S_4	I	I	I	X	X	X	X
S_5	I	X	X	I	I	X	X
S_6	X	I	X	I	X	I	X
$\bar{Z}$	Z	Z	Z	Z	Z	Z	Z
$\bar{X}$	X	X	X	X	X	X	X

Table 2: The [[7,1,3]] Steane code.

Fault-tolerant quantum computation

We have introduced the theory of quantum error correction to protect raw quantum states in previous sections. However, the error correction procedure itself could be error-prone. As a result,

these errors that occur during the encoding or decoding circuits can introduced more errors because errors can propagate through entangling gates, such as CNOT.

Exercise 13. *An operator M can be transformed by a unitary U to $UMU^\dagger$. Show that CNOT induces the following transformations:*

$$\begin{aligned} X \otimes I &\rightarrow X \otimes X && (23)\\ Z \otimes I &\rightarrow Z \otimes I && (24)\\ I \otimes X &\rightarrow I \otimes X && (25)\\ I \otimes Z &\rightarrow Z \otimes Z. && (26) \end{aligned}$$

Exercise 14 demonstrated that the quantum gate CNOT will cause significant harm to QECC when the errors occur before it. Specifically, the bit-flip error X on the controlled qubit will propagate forwards while the phase-flip error Z on the data qubit will propagate backwards. Therefore, the encoding and decoding circuits for QECCs have to be designed very carefully so that an error occurs during the procedure will only propagate to a small number of qubits and the error correction can effectively removes these errors. Moreover, the cost of quantum error correction is huge due to the requirement of encoding and decoding (syndrome measurement). To mitigate this overhead and the error propagation issue, the concept of fault-tolerant quantum computation, namely to compute directly on the *encoded* quantum states, is proposed.

Fault-tolerant logic operations

Let's take the $[[7, 1, 3]]$ Steane code as an example. The Steane code can protect one qubit with an encoded space of $\mathcal{H}_2^{\otimes 7}$. Denote the encoded logic states by $|0_L\rangle$ and $|1_L\rangle$. Then we have, for any S in the stablizer group $\mathcal{S}$ of the Steane code,

$$S|\Psi\rangle = |\Psi\rangle \tag{27}$$

for any $|\Psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$. The logic phase-flip and bit-flip operation $\bar{Z}$ and $\bar{X}$ are given in Table 2:

$$\begin{aligned} \bar{Z}(\alpha|0_L\rangle + \beta|1_L\rangle) &= \alpha|0_L\rangle - \beta|1_L\rangle && (28)\\ \bar{X}(\alpha|0_L\rangle + \beta|1_L\rangle) &= \alpha|1_L\rangle + \beta|0_L\rangle. && (29) \end{aligned}$$

In the following, we will show that the Hadamard, phase, and CNOT gates can be implemented transversally.

Note that the logical Hadamard gate $\bar{H}$ should convert

$$\begin{aligned} \bar{H}\bar{Z}\bar{H}^\dagger &= \bar{X} && (30)\\ \bar{H}\bar{X}\bar{H}^\dagger &= \bar{Z}. && (31) \end{aligned}$$

It is quite easy to verify that $\bar{H} = H^{\otimes 7}$ can achieve the above transformations.

Secondly, we can implement the logical phase gate $\bar{S}$ transversally as follows. Note that the phase gate S

$$\begin{aligned} SZS^\dagger &= Z && (32)\\ SXS^\dagger &= iXZ. && (33) \end{aligned}$$

Note that application of $S^{\otimes 7}$ can only transform $\bar{X}$ to $-\bar{Y}$. Hence the logical phase operation for the Steane code should be $\bar{S} = (ZS)^{\otimes 7}$.

Finally, the logical CNOT operation can be implemented transversally by $\overline{\text{CNOT}} = \text{CNOT}^{\otimes 7}$. Even if the error could propagate to the other block either forwards or backwards, it will only cause one additional error in the other block—hence it is still correctable.

Since $\{S, CNOT, H, \frac{\pi}{8}\}$ is a universal gate set, if we can implement the logical $\frac{\pi}{8}$ gate transversally, we can implement any logical operations transversally. However, we have the following no-go theorem:

Theorem 14 ([6])**.** *No quantum error correcting code can have a continuous symmetry which acts transversely on physical qubits.*

Exercise 15. *How could one implement a fault-tolerant $\frac{\pi}{8}$ gate?*

Threshold Theorem

Suppose that we have a rate C quantum error correcting code, i.e., one qubit is protected by C number of physical qubits, and total of D time steps are required for the error correcting procedure. Let the occurrence probability of a single qubit error be p. Then we will have CD locations for a single error to occur, and the probability that more than one single qubit error occurs is

$$p' = \sum_{i=2}^{CD} \binom{CD}{i} p^i (1-p)^{CD-i} \approx (CD)^2 p^2 \tag{34}$$

when p is small. If p is well below $\frac{1}{(CD)^2}$, $p' < p$; namely, each level of error correction could reduce the error rate. This could then allow us to perform quantum computation for a longer time.

Specifically, assume that we concatenate the same code k times—a single qubit is protected by C^k number of qubits and the overall time steps for the error correction procedure to complete is D^k. Similar to Eq. (34), the probability that more than one single qubit error occurs is $O((CDp)^{2^k})$. It is easy to see that if we want the raw data to survive for T number of logic operations without accumulating errors, i.e., the error rate $p' \ll \frac{1}{T}$, we can choose $k = O(\log \log T)$.

References

[1] Charles H. Bennett and Stephen J. Wiesner, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Physical Review Letters **69** (1992), 2881–2884.

[2] S. Bravyi, D. Fattal, and D. Gottesman, *GHZ extraction yield for multipartite stabilizer states*, J. Math. Phys. **47** (2006), 062106.

[3] A. C. da Silva, *Lectures on symplectic geometry*, Springer-Verlag, Berlin, 2001.

[4] Igor Devetak, Aram W. Harrow, and Andreas Winter, *A resource framework for quantum shannon theory*, IEEE Transactions on Information Theory **54** (2008October), no. 10, 4587–4618.

[5] Igor Devetak, Aram W. Harrow, and Andreas J. Winter, *A family of quantum protocols*, Physical Review Letters **93** (2004), 239503.

[6] Bryan Eastin and Emanuel Knill, *Restrictions on transversal encoded quantum gate sets*, Phys. Rev. Lett. **102** (2009Mar), 110502.

[7] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, *Entanglement in the stabilizer formalism*, 2004. quant-ph/0406168.

[8] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, New York, 2000.

[9] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Physical Review A **52** (1995), 2493–2496.