Topological Quantum Error Correcting Codes Parts I

Isaac Smith

July 18, 2019

Brief Revision of Classical Linear Codes

The following definitions have been lifted verbatim from James Clift's talk two weeks ago. We recall them now to motivate, and allow us to draw comparisons to, the initial theory regarding quantum error correcting codes.

Definition 0.1. A **linear code** C of length n and rank k is a k-dimensional subspace of $\mathbb{F}_2^n$.

Definition 0.2. The **code generator matrix** G is an $n \times k$ matrix such that if $v \in \mathbb{F}_2^k$ is an unencoded word, then $Gv \in \mathbb{F}_2^n$ is the corresponding encoded word.

Definition 0.3. A **parity-check matrix** H is an $(n-k) \times n$ matrix with $\ker H = C$.

Definition 0.4. Let $x \in \mathbb{F}_2^n$. The **Hamming weight** of x is the number of non-zero entries; we denote this by $||x||$. If $x, y \in \mathbb{F}_2^n$, we define the **Hamming distance** between x and y as $||x - y||$.

1 General Theory of Quantum Error-Correcting Codes and Quantum Operations

These notes are based heavily on "Quantum Computing and Quantum Information" by M. A. Nielsen and I. L. Chuang (see references).

Definition 1.1. A **quantum error correcting code** is a subspace $\mathcal{C}$ of the Hilbert space (state space) $\mathcal{H}$ of the quantum system.

It is often useful to consider a code $\mathcal{C}$ along with a projector $P_{\mathcal{C}}$ onto the code space.

Encoding in the setting of quantum error correcting codes also parallels that of classical linear codes: a state $|\psi\rangle \in \mathcal{H}$ is encoded as a state $|\psi'\rangle \in \mathcal{C}$ via a unitary transformation U. This encoding unitary is typically

written as a quantum circuit rather than an explicit matrix, since even simple codes are encoded by large matrices.

The nature of quantum mechanics is such that quantum error correcting codes are required to deal with more complicated types of errors than classical codes. There are many different error models related to quantum systems, often called **error channels** (we'll discuss some examples later), so we would like to develop a general theory of quantum error-correction that makes as few assumptions regarding the specific error models as possible. To do this, we first need the following definition.

Definition 1.2. A **quantum operation** is a map $\mathcal{E}$ from the input space $\mathcal{H}_1$ to the output space $\mathcal{H}_2$ such that for all $|\psi\rangle \in \mathcal{H}_1$

$$\mathcal{E}(|\psi\rangle) = \sum_i E_i|\psi\rangle$$

for some set of operators E_i, called **operation elements**, that map $\mathcal{H}_1$ to $\mathcal{H}_2$ and satisfy

$$\sum_i E_i^\dagger E_i \leq I$$

Definition 1.3. A quantum operation is **trace-preserving** if $\sum_i E_i^\dagger E_i = I$.

Theorem 1.1. ***(Unitary freedom of quantum operations)*** *Suppose $\{E_1, ..., E_m\}$ and $\{F_1, ..., F_n\}$ are operation elements defining quantum operations $\mathcal{E}$ and $\mathcal{F}$ respectively. We can assume that $m = n$ (otherwise append some 0 operators to the smaller of the two sets). Then $\mathcal{E} = \mathcal{F}$ if and only if there exist complex numbers u_{ij} such that $E_i = \sum_j u_{ij} F_j$ and (u_{ij}) is an $m \times m$ unitary matrix.*

Before we prove the theorem, we need the following lemma.

Lemma 1.2. *The set $|\psi_i\rangle$ and $|\phi_i\rangle$ generate the same density matrix if and only if*

$$|\psi_i\rangle = \sum_j u_{ij}|\phi_j\rangle$$

where (u_{ij}) is a unitary matrix over $\mathbb{C}$, and the sizes of the two sets can be taken to be equal by appending 0 vectors to the smaller of the two sets.

Proof. Suppose $|\psi_i\rangle = \sum_j u_{ij}|\phi_j\rangle$ for some unitary u_{ij}. Then

$$\begin{aligned}
\sum_i |\psi_i\rangle\langle\psi_i| &= \sum_{ijk} u_{ij} u_{ik}^* |\phi_j\rangle\langle\phi_k| \\
&= \sum_{jk} \big(\sum_i u_{kj}^\dagger u_{ij} \big) |\phi_j\rangle\langle\phi_k| \\
&= \sum_{jk} \delta_{kj} |\phi_j\rangle\langle\phi_k| \\
&= \sum_j |\phi_j\rangle\langle\phi_j|
\end{aligned}$$

which proves one direction. For the other direction, suppose that

$$A = \sum_i |\psi_i\rangle\langle\psi_i| = \sum_j |\phi_j\rangle\langle\phi_j|$$

Let $A = \sum_k \lambda_k |k\rangle\langle k|$ where the $|k\rangle$ are othronormal and the λ_k are strictly positive (that is, consider the spectral decomposition for the density operator A). Define $|k'\rangle = \sqrt{\lambda_k}|k\rangle$ and let $|\psi'\rangle$ be any vector orthonormal to the space spanned by the $|k'\rangle$. This means that $\langle\psi'|k'\rangle\langle k'|\psi'\rangle = 0$ and moreover

$$0 = \langle\psi'|A|\psi'\rangle = \sum_i \langle\psi'|\psi_i\rangle\langle\psi_i|\psi'\rangle = \sum_i |\langle\psi'|\psi_i\rangle|^2$$

Therefore, $\langle\psi'|\psi_i\rangle = 0$ for all i and all $|\psi'\rangle$, meaning that for each i we can write $|\psi_i\rangle = \sum_k c_{ik}|k'\rangle$. Therefore

$$A = \sum_k |k'\rangle\langle k'| = \sum_{kl} \big(\sum_i c_{ik}c_{il}^*\big)|k'\rangle\langle l'|$$

The operators $|k'\rangle\langle l'|$ are linearly independent and so

$$\sum_i c_{ik}c_{il}^* = \delta_{kl}$$

We then can append columns to the matrix c to obtain a unitary matrix v such that $|\psi_i\rangle = \sum_k v_{ik}|k'\rangle$, where some 0 vectors may have been appended to the list of $|k'\rangle$. The same process can be repeated for $|\phi_j\rangle$ to find a unitary matrix w such that $|\phi_j\rangle = \sum_k w_{jk}|k'\rangle$. Taking $u = vw^\dagger$ gives the desired result. □

Now to prove the theorem.

Proof. Suppose $\mathcal{E}$ and $\mathcal{F}$ act on $\mathcal{H}$ and are generated by $\{E_1, ..., E_n\}$ and $\{F_1, ..., F_m\}$ respectively. Without loss of generality, we can assume $n = m$.

Suppose $\mathcal{E} = \mathcal{F}$, that is,

$$\sum_i E_i|\psi\rangle = \sum_j F_j|\psi\rangle$$

for all $|\psi\rangle \in \mathcal{H}$. Let us denote the basis for $\mathcal{H}$ by $|i\rangle$. Define the following state in $\mathcal{H}$

$$|\phi\rangle = N\sum_i |i\rangle$$

where N is a normalisation constant. Let us also define the following

$$|e_k\rangle = \sum_i E_k(|i\rangle)$$
$$|f_l\rangle = \sum_i F_l(|i\rangle)$$

Since $\mathcal{E}(|\phi\rangle) = \mathcal{F}(|\phi\rangle)$, get that $\sum_k |e_k\rangle\langle e_k| = \sum_l |f_l\rangle\langle f_k|$ and let us denote this operator by σ. By 1.2, the two sets of vectors $\{|e_k\rangle\}$ and $\{|f_l\rangle\}$ generate the same operator if and only if $|e_k\rangle = \sum_l u_{kl}|f_l\rangle$ for some unitary (u_{kl}). Since these two sets generate σ, such a unitary exists. Now, we can write an arbitrary $|\psi\rangle \in \mathcal{H}$ as follows

$$|\psi\rangle = \sum_i \alpha_i |i\rangle$$

and let us define $|\psi'\rangle$ by

$$|\psi'\rangle = \sum_i \alpha_i^* |i\rangle$$

Then we get

$$\begin{aligned} E_i|\psi\rangle &= \langle\psi'|e_i\rangle \\ &= \sum_j u_{ij}\langle\psi'|f_j\rangle \\ &= \sum_j u_{ij} F_j|\psi\rangle \end{aligned}$$

for all $|\psi\rangle$ and for all i. Thus, we get $E_i = \sum_j u_{ij} F_j$ as required.

Now suppose that $E_i = \sum_j u_{ij} F_j$ for some unitary (u_{ij}). Then for any $|\psi\rangle$, we have

$$\begin{aligned} \mathcal{E}(|\psi\rangle) &= \sum_i E_i|\psi\rangle \\ &= \sum_i \sum_j u_{ij} F_j|\psi\rangle \\ &= \sum_j F_j\big(\sum_i u_{ij}\big)|\psi\rangle \\ &= \sum_j F_j(e^{i\theta})|\psi\rangle \\ &= \sum_j F_j|\psi\rangle \qquad \text{up to a global phase} \\ &= \mathcal{F}(|\psi\rangle) \end{aligned}$$

Thus $\mathcal{E} = \mathcal{F}$. □

Proposition 1.3. *Let $\mathcal{E}$ and $\mathcal{F}$ be quantum operations from $\mathcal{H}_1$ to $\mathcal{H}_2$ and from $\mathcal{H}_2$ to $\mathcal{H}_3$ respectively. Then $\mathcal{F} \circ \mathcal{E}$ is a quantum operation from $\mathcal{H}_1$ to $\mathcal{H}_3$.*

Proof. Let $\mathcal{E}$ and $\mathcal{F}$ be quantum operations defined by $\{E_i\}$ and $\{F_j\}$ respectively. Thus, we can write

$$\begin{aligned}\mathcal{F}(\mathcal{E}(|\psi\rangle)) &= \mathcal{F}(\sum_i E_i|\psi\rangle) \\ &= \sum_i \mathcal{F}(E_i|\psi\rangle) \\ &= \sum_i \sum_j F_j(E_i|\psi\rangle)\end{aligned}$$

where the second equality follows by the linearity of quantum operations. So, $\mathcal{F} \circ \mathcal{E}$ can be described by the set of operators $\{F_j E_i\}_{i,j}$ that map $\mathcal{H}_1$ to $\mathcal{H}_3$. We also note that

$$\begin{aligned}\sum_{i,j}(F_j E_i)^\dagger F_j E_i &= \sum_{i,j} E_i^\dagger F_j^\dagger F_j E_i \\ &\leq \sum_i E_i^\dagger I E_i \\ &\leq I\end{aligned}$$

Therefore $\mathcal{F} \circ \mathcal{E}$ is a quantum operation. □

Proposition 1.4. *Measurement is a quantum operation.*

Proof. This proposition follows directly by definition. The third postulate of quantum mechanics defines quantum measurements to be described by a collection of operators $\{M_m\}$ that act on the state space being measured, with the subscript m referring to the measurement outcome [1]. The measurement operation on $|\psi\rangle$ is given by

$$\mathcal{E}(|\psi\rangle) = \sum_m \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

and the operators M_m satisfy

$$\sum_m M_m^\dagger M_m = I$$

Thus quantum measurement is a quantum operation. □

We are now in a position to describe our minimal set of assumptions on which to base our general theory of quantum error correction.

Definition 1.4. For a given error channel effected by a quantum operation $\mathcal{E}$, an **error-correction procedure** is a trace-preserving quantum operation $\mathcal{R}$ such that

$$(\mathcal{R} \circ \mathcal{E})(|\psi\rangle) \propto |\psi\rangle \tag{1}$$

Remark. We say that error-correction can occur for a given error channel $\mathcal{E}$ if an error-correction procedure exists for $\mathcal{E}$. The usual two-stage error detection then error correction procees is all bundled up inside the definition given above. The above equation does not contain equality since we haven't made any assumptions preventing the error channel including measurement of the system. Equality would occur if the error channel is also trace-preserving. The requirement that the error-correction procedure $\mathcal{R}$ is trace-preserving amounts to requiring that the process $\mathcal{R}$ succeeds with certainty since the trace is closely related to probability.

The following theorem provides criteria for an error channel to be correctable.

Theorem 1.5. ***(Quantum error-correcting conditions)*** *Let $\mathcal{C}$ be a quantum code and let $P_{\mathcal{C}}$ be the projector onto $\mathcal{C}$. Suppose $\mathcal{E}$ is a quantum operation with elements $\{E_i\}$. There exists an error-correction procedure $\mathcal{R}$ that satisfies (1) if and only if*

$$P_{\mathcal{C}} E_i^\dagger E_j P_{\mathcal{C}} = \alpha_{ij} P_{\mathcal{C}}$$

where (α_{ij}) is a Hermitian matrix over $\mathbb{C}$.

The proof of the theorem makes use of the following

Lemma 1.6. ***(Polar decomposition of a linear operator)*** *Let A be a linear operator on a vector space V. Then there exists a unitary U and positive operators J and K such that*

$$A = UJ = KU$$

where the unique operators J and K satisfying the above equation are defined by $J = \sqrt{A^\dagger A}$ and $K = \sqrt{AA^\dagger}$.

Proof. J is a positive operator so, by taking its spectral decomposition, we can write $J = \sum_i \lambda_i |i\rangle\langle i|$ with all λ_i non-negative. Define $|\psi_i\rangle = A|i\rangle$ for all i. Consider the set of $|\psi_i\rangle$ such that $\lambda_i \neq 0$. For each of these i, define $|e_i\rangle = |\psi_i\rangle/\lambda_i$. The set of these $|e_i\rangle$ are orthonormal. This set can be extended to an orthonormal basis via the Gram-Schmidt procedure. Also label this set $|e_i\rangle$. If we define $U = \sum_i |e_i\rangle\langle i|$, we see that for $\lambda_i \neq 0$, $UJ|i\rangle = \lambda_i|e_i\rangle = |\psi_i\rangle = A|i\rangle$, and for $\lambda_i = 0$, $UJ|i\rangle = 0 = |\psi_i\rangle$. Thus A and UJ agree on the basis $|i\rangle$ which proves equality.

Suppose $J' \neq J$ is another positive operator that satisfies $A = UJ'$. But then, we have

$$\begin{aligned} A^\dagger A &= J' U^\dagger U J' \\ &= J'^2 \end{aligned}$$

so either $J' = -\sqrt{A^\dagger A}$ which contradicts the assumption that J' is positive, or $J' = \sqrt{A^\dagger A} = J$ which contradicts the other assumption. Thus $J = \sqrt{A^\dagger A}$ is the unique positve operator satisfying $A = UJ$. The proof for K follows by defining $K = UJU^\dagger$. □

Now to the proof of 1.5.

Proof. Suppose $\{E_i\}$ is a set of operation elements for a quantum operation $\mathcal{E}$ satisfying

$$PE_i^\dagger E_j P = \alpha_{ij} P$$

for some Hermitian matrix $\alpha = (\alpha)_{ij}$. It follows that α can be diagonalised to some diagonal matrix $d = u^\dagger \alpha u$, with u unitary. Let $F_k = \sum_i u_{ik} E_i$. By 1.1, the set $\{F_k\}$ also describes $\mathcal{E}$. We can then write

$$\begin{aligned} PF_k^\dagger F_l P &= \sum_{ij} u_{ki}^\dagger u_{jl} P E_i^\dagger E_j P \\ &= \sum_{ij} u_{ki}^\dagger \alpha_{ij} u_{jl} P \\ &= d_{kl} P \end{aligned}$$

Now let us consider the polar decomposition of the operator $F_k P$. By 1.6 we can write

$$\begin{aligned} F_k P &= U_k \sqrt{P F_k^\dagger F_k P} \\ &= \sqrt{d_{kk}} U_k P \end{aligned}$$

for some unitary U_k. We then define the projectors

$$\begin{aligned} P_k &= U_k P U_k^\dagger \\ &= \frac{F_k P U_k^\dagger}{\sqrt{d_{kk}}} \end{aligned}$$

and note that these projectors define orthogonal subspaces, that is, for $l \neq k$, we see that

$$\begin{aligned} P_l P_k &= P_l^\dagger P_k \\ &= \frac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll}}\sqrt{d_{kk}}} \\ &= \frac{U_l d_{lk} P U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} \\ &= 0 \qquad\qquad \text{since } d_{lk} = 0 \text{ for } l \neq k \end{aligned}$$

Defining the correction procedure $\mathcal{R}$ by the set of operators $\{U_k^\dagger P_k\}$, we see that, for any $|\psi\rangle$ in the codespace

$$\begin{aligned}
\mathcal{R}(\mathcal{E}(|\psi\rangle)) &= \sum_{kl} U_k^\dagger P_k F_l |\psi\rangle \\
&= \sum_{kl} U_k^\dagger P_k^\dagger F_l P|\psi\rangle && \text{since } |\psi\rangle \text{ is in the codespace} \\
&= \sum_{kl} \frac{U_k^\dagger U_k P F_k^\dagger F_l P|\psi\rangle}{\sqrt{d_{kk}}} \\
&= \sum_{kl} \delta_{kl}\sqrt{d_{kk}}|\psi\rangle \\
&= \sum_{k} \sqrt{d_{kk}}|\psi\rangle \\
&\propto |\psi\rangle
\end{aligned}$$

This finishes the first half of the proof, once we note that we can append additional projectors to the set $\{P_k\}$, in order to have a set of operation elements $\{U_k^\dagger P_k\}$ that satisfies

$$\sum_k P_k U_k U_k^\dagger P_k = \sum_k P_k = I$$

Now, for the other direction, suppsoe $\{E_i\}$ is a set of errors (describing a quantum operation $\mathcal{E}$) that is correctable by a trace-preserving error-correction operation $\mathcal{R}$ described by operation elements $\{R_j\}$. Define a quantum operation $\mathcal{E}_C$ such that

$$\mathcal{E}_C(|\psi\rangle) = \mathcal{E}(P|\psi\rangle)$$

Since $P|\psi\rangle$ is in the codespace for any $|\psi\rangle$, we get that

$$\mathcal{R}(\mathcal{E}_C(|\psi\rangle)) \propto P|\psi\rangle$$

In fact, we can show that the proportionality is constant and indpendent of $|\psi\rangle$ via the following argument. Let $|\psi\rangle$ and $|\phi\rangle$ be arbitrary. Then consider

$$\begin{aligned}
\mathcal{R}(\mathcal{E}_C(a|\psi\rangle + b|\phi\rangle)) &= \alpha(a|\psi\rangle + b|\phi\rangle)P(a|\psi\rangle + b|\phi\rangle) \\
&= a\alpha(a|\psi\rangle + b|\phi\rangle)P|\psi\rangle + b\alpha(a|\psi\rangle + b|\phi\rangle)P|\phi\rangle
\end{aligned}$$

where $\alpha(\cdot)$ denotes the proportionality as a function of vectors. But quantum operations are linear, so

$$\begin{aligned}
\mathcal{R}(\mathcal{E}_C(a|\psi\rangle + b|\phi\rangle)) &= a\mathcal{R}(\mathcal{E}_C(|\psi\rangle)) + b\mathcal{R}(\mathcal{E}_C(|\phi\rangle)) \\
&= a\alpha(|\psi\rangle)P|\psi\rangle + b\alpha(|\phi\rangle)P|\phi\rangle
\end{aligned}$$

Thus

$$a\alpha(a|\psi\rangle + b|\phi\rangle)P|\psi\rangle + b\alpha(a|\psi\rangle + b|\phi\rangle)P|\phi\rangle = a\alpha(|\psi\rangle)P|\psi\rangle + b\alpha(|\phi\rangle)P|\phi\rangle$$

which implies that α is constant.

It follows from 1.1 that the operation elements $\{R_j E_i\}$ are equivalent to the quantum operation with the operation elements αP. Thus we have

$$R_j E_i P = \beta_{ji} P$$

for $\beta_{ji} \in \mathbb{C}$. We then get

$$\begin{aligned} P E_i^\dagger R_k^\dagger R_k E_j^\dagger P &= \beta_{ki}^* \beta_{kj} P \\ \implies \sum_k P E_i^\dagger R_k^\dagger R_k E_j^\dagger P &= \sum_k \beta_{ki}^* \beta_{kj} P \\ \implies P E_i^\dagger (\sum_k R_k^\dagger R_k) E_j^\dagger P &= \sum_k \beta_{ki}^* \beta_{kj} P \\ \implies P E_i^\dagger E_j P &= \gamma_{ij} P \qquad \text{since } \sum_k R_k^\dagger R_k = I \text{ by trace-preservation} \end{aligned}$$

where $\gamma_{ij} = \sum_k \beta_{ki}^* \beta_{kj}$ which is Hermitian. □

We often refer to the set of operation elements for an error channel $\mathcal{E}$ as **errors** and if an operation $\mathcal{R}$ exists that satisfies (1), then we refer to them as **correctable errors**.

We have the following important theorem.

Theorem 1.7. ***(Discretisation of Errors)*** *Let $\mathcal{C}$ be a quantum code and $\mathcal{R}$ be the error-correction procedure that corrects the set of errors $\{E_i\}$ describing the error operation $\mathcal{E}$. Suppose $\mathcal{F}$ is a quantum operation with operation elements $\{F_j\}$ such that $F_j = \sum_i m_{ji} E_i$ for some matrix (m_{ji}) over $\mathbb{C}$. Then $\mathcal{R}$ also corrects $\mathcal{F}$ on $\mathcal{C}$.*

Proof. Similar to the proof of 1.5, we can assume without loss of generality that the set of errors $\{E_i\}$ is such that

$$P E_j^\dagger E_i P = d_{ij} P$$

where d_{ij} is diagonal. We again take the operation elements of the error-correction procedure $\mathcal{R}$ to be $U_k^\dagger P_k$, defined as before, such that

$$U_k^\dagger P_k E_i |\psi\rangle = \delta_{ik} \sqrt{d_{kk}} |\psi\rangle$$

for all $|\psi\rangle$ in the codespace. Now, we get that

$$\begin{aligned} U_k^\dagger P_k F_j |\psi\rangle &= \sum_i m_{ji} \delta_{ki} \sqrt{d_{kk}} |\psi\rangle \\ &= m_{jk} \sqrt{d_{kk}} |\psi\rangle \end{aligned}$$

which shows that $\mathcal{R}$ corrects the set of errors $\{F_j\}$ since

$$\begin{aligned}\mathcal{R}(\mathcal{F}(|\psi\rangle)) &= \sum_j \mathcal{R}(F_j|\psi\rangle) \\ &= \sum_{jk} U_k^\dagger P_k F_j |\psi\rangle \\ &= \big(\sum_{kj} m_{jk}\sqrt{d_{kk}}\big)|\psi\rangle \\ &\propto |\psi\rangle\end{aligned}$$

□

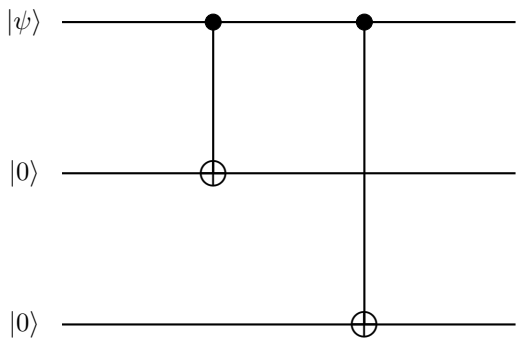
1.1 Examples of Error Channels and Quantum Error-Correcting Codes

Let us now see some examples of different error channels written in the quantum operation formalism, and codes that correct these channels.

Example 1.1. (**Bit-flip channel and bit-flip code**) We can specify the bit-flip error channel $\mathcal{E}_{bit}$ by writing down it's operation elements $\{E_0, E_1\}$:

$$E_0 = \sqrt{p}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$
$$E_1 = \sqrt{1-p}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

where $1-p$ is the probability that a bit flip occurs when a state $|\psi\rangle$ is transmitted through the channel $\mathcal{E}_{bit}$. Now let us consider the three-qubit bit flip error-correcting code $\mathcal{C}_{3,bit}$. This code is the subspace of the 2^3-dimensional state space $\mathcal{H}$ spanned by $\{|000\rangle, |111\rangle\}$. A state of a single qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ is encoded into the state $|\psi'\rangle = a|000\rangle + b|111\rangle$ via the following circuit (unitary transformation)



Suppose the state $|\psi\rangle$ is successfully encoded as $|\psi'\rangle$. Then suppose $|\psi'\rangle$ is passed through the error channel $\mathcal{E}$ which is actually three independent bit-flip error channels (the independence of error channels is crucial

for error correction to work), one for each qubit, that is

$$\begin{aligned}\mathcal{E}(|\psi'\rangle) &= (\mathcal{E}_{3,bit} \circ \mathcal{E}_{2,bit} \circ \mathcal{E}_{1,bit})(|\psi'\rangle) \\ &= (\mathcal{E}_{3,bit} \circ \mathcal{E}_{2,bit})(\sqrt{p_1}|\psi'\rangle + \sqrt{1-p_1}X_1|\psi'\rangle) \\ &= \mathcal{E}_{3,bit}(\sqrt{p_1}\mathcal{E}_{2,bit}(|\psi'\rangle) + \sqrt{1-p_1}\mathcal{E}_{2,bit}(X_1|\psi'\rangle)) \\ &= ...\end{aligned}$$

We will take $p_1 = p_2 = p_3$ to make things simpler. This gives

$$\begin{aligned}\mathcal{E}(|\psi'\rangle) = p^{3/2}|\psi'\rangle + p\sqrt{1-p}(X_3|\psi'\rangle + X_2|\psi'\rangle + X_1|\psi'\rangle) + (1-p)\sqrt{p}(X_3X_2|\psi'\rangle + X_3X_1|\psi'\rangle + X_2X_1|\psi'\rangle) \\ + (1-p)^{3/2}X_3X_2X_1|\psi'\rangle\end{aligned}$$

Now let us define the following four projection operators

$$\begin{aligned}P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|\end{aligned}$$

and let us define our error-correction procedure $\mathcal{R}$ as the quantum operation described by the elements $\{P_0, X_1P_1, X_2P_2, X_3P_3\}$. If we let $|\psi"\rangle$ denote $\mathcal{E}(|\psi'\rangle)$ and if we assume that at most one error has occurred, then we get

$$\mathcal{R}(|\psi"\rangle) = |\psi'\rangle$$

since it is easy to see that the $+1$-eigenstates of each of the four projectors correspond to no error, a single error on first qubit, a single error on the second qubit and a single error on the third qubit respectively. So if, say, $|\psi''\rangle = a|010\rangle + b|101\rangle$, we get

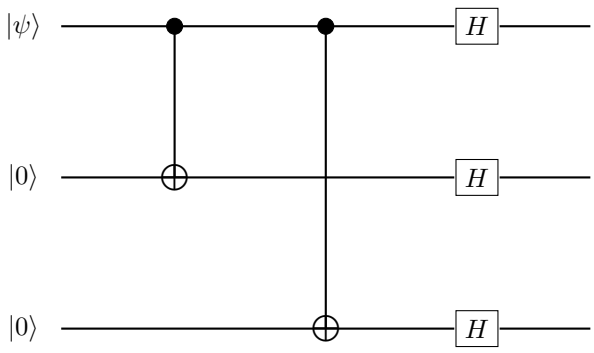
$$\begin{aligned}\mathcal{R}(a|010\rangle + b|101\rangle) &= P_0(a|010\rangle + b|101\rangle) + X_1P_1(a|010\rangle + b|101\rangle) + X_2P_2(a|010\rangle + b|101\rangle) + X_3P_3(a|010\rangle + b|101\rangle) \\ &= 0 + 0 + X_2(a|010\rangle + b|101\rangle) + 0 \\ &= a|000\rangle + b|111\rangle \\ &= |\psi'\rangle\end{aligned}$$

So if at most one error occurs, then this procedure works with certainty.

Example 1.2. (**Phase-flip channel and phase flip code**) The phase-flip channel and phase-flip code are very similar to the bit-flip channel and bit-flip code, so the details in this example are similar to above. The phase-flip channel $\mathcal{E}_{phase}$ can be described by $\{E'_0, E'_1\}$ where

$$\begin{aligned}E'_0 &= E_0 = \sqrt{p}I \\ E'_1 &= \sqrt{1-p}\begin{bmatrix}1 & 0 \\ 0 & -1\end{bmatrix}\end{aligned}$$

The phase-flip code, just like the bit-flip code above, can correct against single errors. A state $|\psi\rangle$ is encoded via the following unitary transformation



which encodes $a|0\rangle + b|1\rangle$ as $a|{+}{+}{+}\rangle + b|{-}{-}{-}\rangle$. Error detection and correction occurs via a very similar process to that outlined above. In fact, these bit-flip and phase-flip error channels (and corresponding the bit-flip and phase-flip codes) are **unitarily equivalent** (recall **??**).

Example 1.3. (**Depolarising channel and the Shor code**) An important error channel is the depolarising channel,

$$\mathcal{E}_{depol}(|\psi\rangle) = \frac{pI}{2} + (1-p)|\psi\rangle$$

which can be written in two other equivalent ways: via the operation elements $\{\sqrt{1-3p/4}I, \sqrt{p}X/2, \sqrt{p}Y/2, \sqrt{p}Z/2\}$, and via the following

$$\mathcal{E}_{depol}(|\psi\rangle) = (1-p)|\psi\rangle + \frac{p}{3}(X|\psi\rangle + Y|\psi\rangle + Z|\psi\rangle)$$

Now let us consider for a moment the following

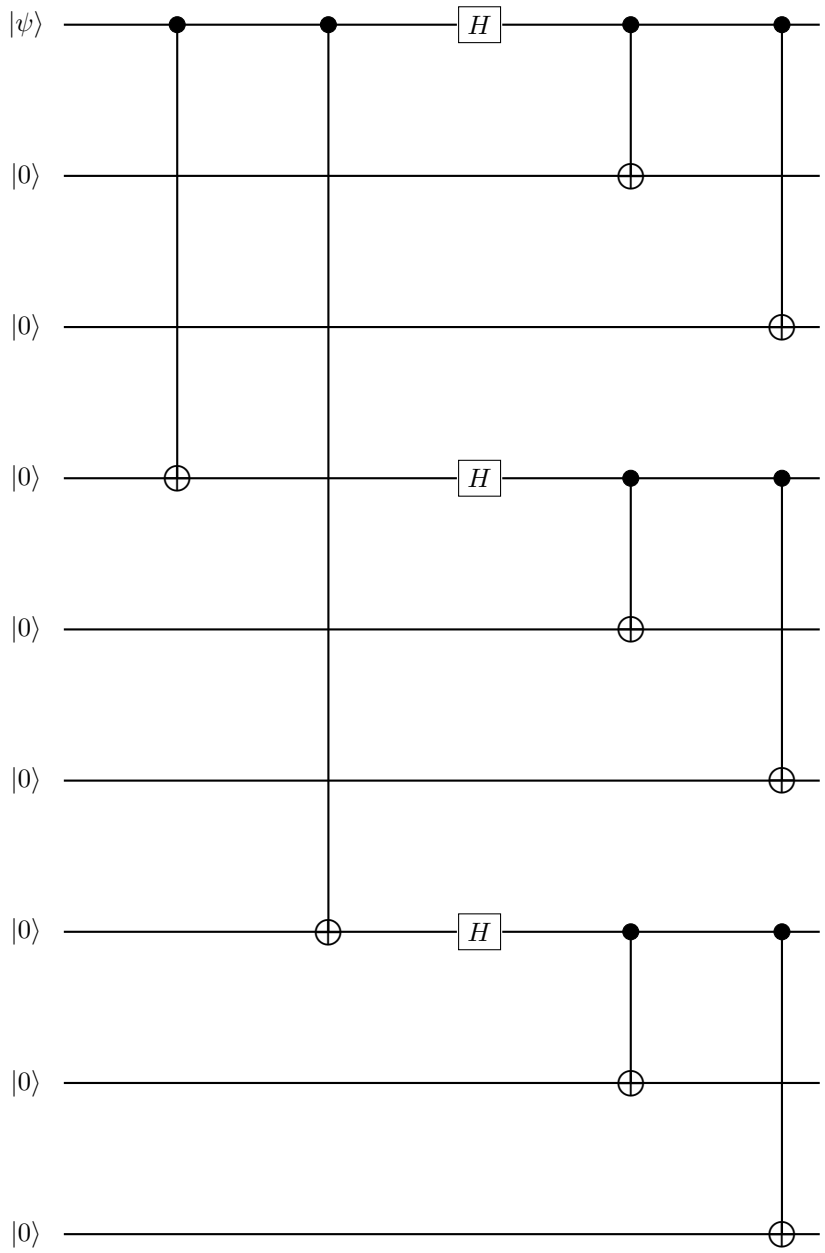
$$\begin{aligned}\mathcal{E}_{bit}(\mathcal{E}_{phase}(|\psi\rangle)) &= \mathcal{E}_{bit}(\sqrt{r}|\psi\rangle + \sqrt{1-r}Z|\psi\rangle) \\ &= \sqrt{r}(\sqrt{t}|\psi\rangle + \sqrt{1-t}X|\psi\rangle) + \sqrt{1-r}(\sqrt{t}Z|\psi\rangle + \sqrt{1-t}XZ|\psi\rangle)\end{aligned}$$

So $\mathcal{E}_{bit} \circ \mathcal{E}_{phase}$ has operatation elements $\{\sqrt{r}\sqrt{t}I, \sqrt{r}\sqrt{1-t}X, \sqrt{1-r}\sqrt{t}Z, \sqrt{1-r}\sqrt{1-t}XZ\}$. By 1.7 that means if we can find an error-correction procedure $\mathcal{R}$ that corrects for $\mathcal{E}_{bit} \circ \mathcal{E}_{phase}$ then $\mathcal{R}$ also corrects the set of operations

$$\begin{aligned}&\{\frac{(1-p)}{\sqrt{r}\sqrt{t}}\sqrt{r}\sqrt{t}I, \frac{p}{3\sqrt{r}\sqrt{1-t}}\sqrt{r}\sqrt{1-t}X, \frac{p}{3\sqrt{1-r}\sqrt{t}}\sqrt{1-r}\sqrt{t}Z, \frac{ip}{3\sqrt{1-r}\sqrt{1-t}}\sqrt{1-r}\sqrt{1-t}XZ\} \\ &= \{(1-p)I, \frac{p}{3}X, \frac{p}{3}Z, \frac{p}{3}Y\}\end{aligned}$$

Thus, correcting for bit and phase flips is sufficient to correct for the depolarising channel. Moreover, if an error-correction procedure can correct for the depolarising channel, by another application of the same theorem, we can correct for any arbitrary single qubit error.

Let us now define the Shor code. This is defined as the concatenation of the three qubit bit-flip code with the three qubit phase-flip code (which intuitively makes sense since we want it to correct for the concatenation of bit-flip and phase-flip channels). A state $|\psi\rangle$ is encoded into the Shor code via



which is encoding into the phase-flip code first, followed by encoding the result into the bit-flip code. That

is

$$|0\rangle \xrightarrow{phase} |++\!+\rangle \xrightarrow{bit} \frac{(|000\rangle + |111\rangle)}{\sqrt{2}} \frac{(|000\rangle + |111\rangle)}{\sqrt{2}} \frac{(|000\rangle + |111\rangle)}{\sqrt{2}} = |0\rangle_L$$
$$|1\rangle \xrightarrow{phase} |--\!-\rangle \xrightarrow{bit} \frac{(|000\rangle - |111\rangle)}{\sqrt{2}} \frac{(|000\rangle - |111\rangle)}{\sqrt{2}} \frac{(|000\rangle - |111\rangle)}{\sqrt{2}} = |1\rangle_L$$

Without going into the details (we'll come back to them later on), we can perform correction via $\mathcal{R}_{phase} \circ \mathcal{R}_{bit}$, that is, the concatenation of the error correction procedures of the two codes we've seen previously.

The notion of concatenation seen above leads to some natural ways of constructing new codes from known codes. In particular, there is a class of quantum error-correcting codes that can be constructed from classical linear codes, called **Calderbank-Shor-Steane codes**.

References

[1] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.