Lecture 16: Quantum Error Correction

Scribed by: Dah-Yoh Lim

October 30, 2003

1 Introduction

Today we are going to look at how one can do error correction in the quantum world. In the PreShannon days, simple repetition codes were used: to transmit bit 0, it is first encoded into a string of zeros, say 0000. Similarly, 1 gets encoded into 1111. One can prove that if you want to reduce the error rate to $1/n$, and the channel flips bits with probability $1/\epsilon$, then you need roughly $\frac{\log n}{\log(1/\epsilon)}$ repetitions.

2 Quantum Analog to Repetition Code

The analog to the repetition code is to say encode $|0\rangle$ as $|000\rangle$ and $|1\rangle$ as $|111\rangle$. Note that this is not the same as copying/cloning the bit, since in the quantum world we know that cloning is not possible.

So for instance, under this encoding E the EPR state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ would be encoded as $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

2.1 Bit Errors

Suppose there is a bit error σ_X at the third qubit.

$$\sigma_X^{(3)} E(|0\rangle) = \sigma_X^{(3)}(|000\rangle) = |001\rangle.$$

Similarly,

$$\sigma_X^{(3)} E(|1\rangle) = \sigma_X^{(3)}(|111\rangle) = |110\rangle.$$

To correct bit errors, simply project onto the subspaces $\{|000\rangle, |111\rangle\}$, $\{|001\rangle, |110\rangle\}$, $\{|010\rangle, |100\rangle\}$, $\{|100\rangle, |011\rangle\}$.

2.2 Phase Errors

Suppose there is a phase error σ_Z.

$$\sigma_Z^{(j)} E(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \sigma_Z^{(j)} \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = E(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)),$$

for $j = 1, 2, 3$. Therefore, if we use this code, single bit errors can be corrected but phase errors will be come 3 times more likely!

Recall that

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

This takes bit errors to phase errors. If we apply H to the 3-qubit protection code, we get:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle + ... + |111\rangle),$$

and

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle - |001\rangle + ... - |111\rangle),$$

with a negative sign iff the string contains an odd number of 1s.

Now consider the following 3-qubit phase error correcting code:

$$|0\rangle \rightarrow \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle),$$

and

$$|1\rangle \rightarrow \frac{1}{2}(|011\rangle + |100\rangle + |010\rangle + |001\rangle).$$

Now if there is a phase error on the first qubit:

$$\begin{aligned} \sigma_Z^{(1)} E(|0\rangle) &= \frac{\sigma_Z^{(1)}}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ &= \frac{1}{2}(|000\rangle + |011\rangle - |101\rangle - |110\rangle). \end{aligned}$$

Next, note that $\sigma_Z^{(i)} E(|0\rangle)$ and $\sigma_Z^{(i)} E(|1\rangle)$ are orthogonal, for $i = 1, 2, 3$. Therefore, to correct phase errors we can project onto the four subspaces $\{\sigma_Z^{(i)} E(|0\rangle), \sigma_Z^{(i)} E(|1\rangle)\}$ and $\{E(|0\rangle), E(|1\rangle)\}$. Now we have a code that corrects phase error but not bit errors.

2.3 Bit and Phase Errors

If we concatenate the codes that corrected bit and phase errors respectively, then we can get a code that corrects both errors. Consider:

$$E(|0\rangle) = \frac{1}{2}(|000000000\rangle + |000111111\rangle + |111000111\rangle + |111111000\rangle)$$

$$E(|1\rangle) = \frac{1}{2}(|111111111\rangle + |111000000\rangle + |000111000\rangle + |000000111\rangle).$$

It is easy to see that this corrects bit errors. Note that the error correcting procedure does not collapse the superposition, so it can be applied to superpositions as well. There is a continuum of $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ that one can apply to the 1st qubit.

In general, phase errors can be expressed as $\begin{bmatrix} 1 & 0 \\ 0 & e^{2i\theta} \end{bmatrix} = e^{i\theta} \begin{bmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{bmatrix} \equiv R_\theta.$

$$
\begin{aligned}
&R_\theta(\frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)) \\
&\quad = \frac{1}{2}(e^{-i\theta}|000\rangle + e^{-i\theta}|011\rangle + e^{i\theta}|101\rangle + e^{i\theta}|110\rangle) \\
&\quad = \frac{1}{2}\frac{e^{i\theta}+e^{-i\theta}}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) + \frac{1}{2}\frac{-e^{i\theta}+e^{-i\theta}}{2}(|000\rangle + |011\rangle - |101\rangle - |110\rangle) \\
&\quad = \cos\theta E(|0\rangle) - i\sin\theta\sigma_Z^{(1)}E(|0\rangle),
\end{aligned}
$$

i.e. phase error on the 1st qubit.

With our 9-qubit code, let's say we apply $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ to some qubit. Since

$$
\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \frac{\alpha+\delta}{2}I + \frac{\alpha-\delta}{2}\sigma_Z + \frac{\beta+\gamma}{2}\sigma_X + i\frac{\beta-\gamma}{2}\sigma_Y,
$$

we can separate its operation on $\eta E|0\rangle + \mu E|1\rangle$ as follows:

$$
\begin{aligned}
&\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}(\eta E|0\rangle + \mu E|1\rangle) \\
&\qquad = \frac{\alpha+\delta}{2}(\eta E|0\rangle + \mu E|1\rangle) + \frac{\alpha-\delta}{2}\sigma_Z(\eta E|0\rangle + \mu E|1\rangle) \\
&\qquad\quad + \frac{\beta+\gamma}{2}\sigma_X(\eta E|0\rangle + \mu E|1\rangle) + i\frac{\beta-\gamma}{2}\sigma_Y(\eta E|0\rangle + \mu E|1\rangle).
\end{aligned}
$$

However, we know that projection onto $|\phi\rangle$ is equivalent to applying the projection matrix $|\phi\rangle\langle\phi|$; therefore, we see that the code corrects phase errors too.

3 7 bit Hamming Code

The Hamming code encodes 4 bits into 7 bits. The 2^4 codewords are:

S_0	S_1
0000000	1111111
1110100	1011000
0111010	0101100
0011101	0010110
1001110	0001011
0100111	1000101
1010011	1100010
1101001	0110001

Recall that a linear code is a code where the sum of two codewords (mod 2) is another codeword. The Hamming code is a linear code, i.e. one can chose 4 basis elements generated by $G_C = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$, where the rowspace of this matrix gives all the codewords. The parity check matrix is $H_C = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$, which is exactly the generator matrix for the dual code (the set of vectors orthogonal to every vector in the code C).

3.1 Quantum Hamming Code

The quantum analog of the Hamming Code is as follows:

$$|0\rangle \to \frac{1}{2^{3/2}} \sum_{v \in H_C} |v\rangle; \qquad |1\rangle \to \frac{1}{2^{3/2}} \sum_{v \in H_C} |v + e\rangle,$$

where e is the string of all 1s.

Note that this corrects σ_X on any qubit (because of the properties of the Hamming code). Also, if we apply the Hadamard transformation to the quantum Hamming code, we can correct phase errors as well:

$$\begin{aligned}
H^{\otimes 7} E|0\rangle &= \frac{1}{2^{3/2}} \sum_{v \in H_C} H^{\otimes 7} |v\rangle \\
&= \frac{1}{2^{3/2}} \frac{1}{2^{7/2}} \sum_{x=0}^{2^7-1} \sum_{v \in H_C} (-1)^{x \cdot v} |x\rangle \\
&= \frac{1}{2^{7/2}} 2^3 \sum_{x \in G_C} |x\rangle \\
&= \frac{1}{\sqrt{2}} (E|0\rangle + E|1\rangle). \\
H^{\otimes 7} E|1\rangle &= \frac{1}{2^{3/2}} \sum_{v \in H_C} H^{\otimes 7} |v + e\rangle \\
&= \frac{1}{2^{3/2}} \frac{1}{2^{7/2}} \sum_{x=0}^{2^7-1} \sum_{v \in H_C} (-1)^{x \cdot (v+e)} |x\rangle \\
&= \frac{1}{2^{7/2}} 2^3 \sum_{x \in G_C} (-1)^{x \cdot e} |x\rangle \\
&= \frac{1}{\sqrt{2}} (E|0\rangle - E|1\rangle) \\
&= EH|1\rangle.
\end{aligned}$$

So, the σ_X and σ_Z errors are "independent", and therefore this code can correct σ_X error in any qubit and σ_Z error in any other qubit.