Notes 8.370/18.435 Fall 2022

Lecture 28 Prof. Peter Shor

We continue our discussion of the nine-qubit code.

Recall that last time, we started our discussion with the three-qubit bit flip correcting code. This was based on the classical repetition code, that just repeats every bit three times. This code takes

$$\begin{aligned} |\,0\rangle &\rightarrow |\,000\rangle\,, \\ |\,1\rangle &\rightarrow |\,111\rangle\,. \end{aligned}$$

This is not a cloning transformation, because $\alpha\,|\,0\rangle + \beta\,|\,1\rangle \rightarrow \alpha\,|\,000\rangle + \beta\,|\,111\rangle$. This code corrected one bit-flip error, but made phase-flip errors more likely. We then used the fact that $H\sigma_x H = \sigma_z$ to get a three-qubit phase-flip correcting code. This code is

$$\begin{aligned} |\,0\rangle &\rightarrow |\,+++\rangle\,, \\ |\,1\rangle &\rightarrow |\,---\rangle\,. \end{aligned}$$

or in the $\{|\,0\rangle\,, |\,1\rangle\}$ basis,

$$\begin{aligned} |\,0\rangle &\rightarrow \frac{1}{\sqrt{8}}(|\,0\rangle + |\,1\rangle)^{\otimes 3}, \\ |\,1\rangle &\rightarrow \frac{1}{\sqrt{8}}(|\,0\rangle - |\,1\rangle)^{\otimes 3}. \end{aligned}$$

A bit-flip error (σ_x) on any qubit results in a phase flip error on the encoded state: It will change one of the $(|\,0\rangle - |\,1\rangle)$ terms to $(|\,1\rangle - |\,0\rangle)$, which changes a $|\,1\rangle_L$ to a $-|\,1\rangle_L$, and leaves an encoded $|\,0\rangle$ the same.

On the other hand, this will correct any phase-flip (σ_z) error on a single qubit. Why is this true? It's because the eight states

$$\begin{array}{cccc} |\,0\rangle_L\,, & \sigma_z^{(1)}\,|\,0\rangle_L\,, & \sigma_z^{(2)}\,|\,0\rangle_L\,, & \sigma_z^{(3)}\,|\,0\rangle_L \\ |\,1\rangle_L\,, & \sigma_z^{(1)}\,|\,1\rangle_L\,, & \sigma_z^{(2)}\,|\,1\rangle_L\,, & \sigma_z^{(3)}\,|\,1\rangle_L \end{array}$$

are all orthogonal, where $\sigma_z^{(j)}$ denotes a σ_z error on qubit j.

To correct the state, we project it onto one of the four subspaces:

$$|\,0_L\rangle\langle 0_L\,| + |\,1_L\rangle\langle 1_L\,|$$

and

$$\sigma_z^{(j)}\big(\,|\,0_L\rangle\langle 0_L\,| + |\,1_L\rangle\langle 1_L\,|\,\big)\sigma_z^j,$$

for $j = 1, 2, 3$.

We combined these two codes by *concatenating* them. This means first encoding by using the phase-flip code (it would work just as well if we used the bit-flip code first, but this is the standard way to do it) and then encoding each of the qubits in the resulting three-qubit code by the bit-flip code:

$$\begin{aligned}
|\,0\rangle &\rightarrow |\,+\rangle^{\otimes 3} \rightarrow \frac{1}{\sqrt{8}}\big(\,|\,000\rangle + |\,111\rangle\,\big)^{\otimes 3},\\
|\,1\rangle &\rightarrow |\,-\rangle^{\otimes 3} \rightarrow \frac{1}{\sqrt{8}}\big(\,|\,000\rangle - |\,111\rangle\,\big)^{\otimes 3}.
\end{aligned}$$

This results in a nine-qubit code. It corrects both bit and phase errors. This nine-qubit code can correct one Pauli error on any qubit. One σ_x error is corrected by the bit-flip correcting code. One σ_z error passes through the bit-flip correcting code to apply a σ_z error to one of the groups of three qubits, which then gets corrected by the phase-error correcting code. And a σ_y error can be thought of as both a σ_x and a σ_z error on the same qubit, since $\sigma_y = i\sigma_x\sigma_z$, so the bit-flip correcting code corrects the σ_x error and the phase-flip correcting code corrects the σ_z error..

But what about arbitrary errors? You can have arbitrary unitary errors, or you can have a measurement on qubits, or you can have a more general type of quantum transformation that we haven't covered in this class (but which you will see if you take 8.371/18.436). It turns out that this code will correct them, as well. This is because of the following theorem:

Theorem 1 *Any quantum error-correcting code, which corrects t or fewer Pauli errors (σ_x, σ_y, and σ_z errors) on a subset of t or fewer qubits will also correct an arbitrary quantum operation which is applied to at most t qubits.*

That the 9-qubit code will correct any arbitrary single-qubit error follows from the above theorem with $t = 1$.

How do we prove this theorem? We will first show why it works by looking at an example on the three-qubit phase-flip error–correcting code, and then prove it.

Let's consider a qubit $\alpha\,|\,0\rangle + \beta\,|\,1\rangle$ encoded in the three -qubit phase-flip correcting code:

$$\alpha\,|\,0\rangle + \beta\,|\,1\rangle \rightarrow \alpha\,|\,0\rangle_L + \beta\,|\,1\rangle_L$$

What happens when we apply the phase error $\begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}$ to the second qubit of it? We have

$$\begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} \cos\theta - i\sin\theta & 0 \\ 0 & \cos\theta + i\sin\theta \end{pmatrix} = \cos\theta I - i\sin\theta\sigma_z$$

So we get the state

$$\cos\theta\big(\alpha\,|\,0_L\rangle + \beta\,|\,1_L\rangle\,\big) - i\sin\theta\,\sigma_z^{(2)}\big(\alpha\,|\,0_L\rangle + \beta\,|\,1_L\rangle\,\big)$$

When we measure which qubit is in error, we get that there is no error with probability $\cos^2\theta$ and that there is a σ_z in qubit 2 with probability $\sin^2\theta$. And in fact, we collapse the state, so after the measurement, this will indeed be the case. When we correct the σ_z error on qubit 2, this restores the original state.

Why did this happen? The reason is that the error matrix has a decomposition in I and σ_z:

$$\begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = (\cos\theta)I - i(\sin\theta)\sigma_z\,.$$

When you apply it, you get a superposition of applying the identity matrix with amplitude $\cos\theta$ and the σ_z matrix with amplitude $-i\sin\theta$. Now, when you perform the error correction protocol, you measure the error, and find out that there was no error with probability $\cos^2\theta$ and a $\sigma_z^{(2)}$ error with probability $\sin^2\theta$. However, after the quantum state has collapsed, this is indeed the situation.

So how do we prove Theorem 1? We prove that if an error-correcting code can correct errors described by matrices M_1, M_2, M_3, $\ldots$, M_k, then it can correct errors described by any linear combination of these. Then we show that any error on t qubits is a linear combination of Pauli errors on t qubits.

The first step is just an application of the linearity of quantum mechanics. Consider an error correcting circuit. Then we can apply the principle of delayed measurement to postpone any measurements until the end. Here, instead of measuring the error classically and applying Pauli matrices (say) to correct it, you measure the error coherently and then use controlled Pauli gates to correct the error. This gives us a unitary which takes

$$M_i \,|\, \psi \rangle \,\big|\, 0^l \big\rangle \longrightarrow |\, \psi \rangle \,|\, D_i \rangle$$

where $|\, D_i \rangle$ is essentially a description of the error. Then, for an error F, if we have $F = \sum_i M_i$, we can correct it. This is because the error correction circuit takes

$$F \,|\, \psi \rangle \,\big|\, 0^k \big\rangle = \sum_i \alpha_i M_i \,|\, \psi \rangle \,\big|\, 0^k \big\rangle \longrightarrow |\, \psi \rangle \sum_i \alpha_i \,|\, D_i \rangle\,.$$

This calculation also shows how error correction gets around the Heisenberg Uncertainty Principle, which says that if you measure a quantum state, you disturb it. What error correction does is measure the error without measuring the encoded quantum state. This lets you correct the error without measuring the quantum state.

Finally, let me address the question of what happens if you have a small error on every qubit. For example, suppose you have n qubits, and each qubit has an independent error where the error on the ith qubit is

$$F_i = (1-\epsilon_i)I + \delta_{x,i}\sigma_x^{(i)} + \delta_{y,i}\sigma_y^{(i)} + \delta_{z,i}\sigma_z^{(i)}.$$

What you do is expand the tensor product $\bigotimes_i F_i$. If the δ's are small enough, then most of the amplitude of this product will be in terms which have relatively few Pauli errors, so if you can correct (say) any tensor product of fewer than $n/100$ Pauli errors, then if the δ's are small enough, nearly all the time, when you measure the error there will be Pauli errors on fewer than $n/100$ qubits, and the probability that you make an error that is too large to be corrected will be exponentially small.