Quantum Coding Theory **(UC Berkeley CS294, Spring 2024)**

Lecture 2: Shor 9-Qubit Code

Jan 26 2024

Lecturer: John Wright *Scribe: Malvika Raj*

1 Recap of last lecture

These are the important quantum errors to correct

1. $X : |0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$. Also known as "bit flip".
2. $Z : |0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto -|1\rangle$. Also known as "phase flip". Its action is interesting in the Hadamard basis, $|+\rangle \mapsto |-\rangle$ and $|-\rangle \mapsto |+\rangle$, which is a bit flip.
3. $Y = iXZ$: First applies Z and then X. This describes an error model where both X and Z errors.

We want to construct codes resilient against these errors. Last time we saw the 3-qubit bit flip code that encodes $a|0\rangle + b|1\rangle \to a|000\rangle + b|111\rangle$. In quantum we have no cloning, this only clones in the standard basis and can correct a single bit flip but no phase flips at all.

The natural next question is, can we defend against phase flips?

2 3-qubit phase flip code

A phase flip is just a bit flip in the H basis. So we just take the bit flip code and do it in H basis.

$$|0\rangle \mapsto |0_L\rangle \equiv |+++\rangle \tag{1}$$
$$|1\rangle \mapsto |1_L\rangle \equiv |---\rangle \tag{2}$$

This is encoding the standard basis and it extends by linearity to a general state.

$$|\psi\rangle = a|0\rangle + b|1\rangle \mapsto a|+++\rangle + b|---\rangle$$

Question: Why do we describe the encoding in standard basis and not Hadamard basis?
The other way also probably works but we'll see later that there's a reason to do it this way.

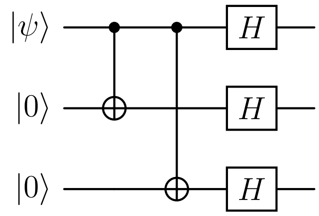

Figure 1: Encoding circuit for the 3 qubit phase flip code.

There was a question last time about the CNOT gate. For $a, b \in \{0,1\}$, it takes $|a\rangle|b\rangle \to |a\rangle|a \oplus b\rangle$.

2.1 Errors

It detects errors the same way as last time but in a different basis. For example, we have our encoded state $|\psi_L\rangle = a|000\rangle + b|111\rangle$ and it encounters a Z error on the third qubit, i.e, the error flips the $+$ and $-$ in the third qubit,

$$\left|\tilde{\psi}_L\right\rangle = IIZ|\psi_L\rangle = a|{+}{+}{-}\rangle + b|{-}{-}{+}\rangle$$

To correct the error, if we measure the state, it will collapse. So we'll only measure the error syndrome, the relative parity: for every two qubits, whether they are different. Last time we did this in the std basis, now we do it in the H basis.

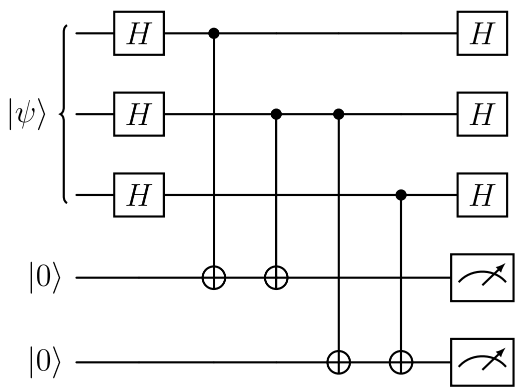

Figure 2: Circuit for phase flip detection.

Question: If we add the circuit for creating the logical state before this, won't the H gates cancel out?
We are assuming that the error happens in between. Right now, we're also assuming that

our measurement is error free.

For example, on $\left|\tilde{\psi}_L\right\rangle$, the circuit will first take,

$$a\left|++-\right\rangle + b\left|--+\right\rangle \mapsto a\left|001\right\rangle + b\left|110\right\rangle$$

Then it applies the exact same circuit as last time on this state after appending the syndrome qubits.

$$(a\left|001\right\rangle + b\left|110\right\rangle) \otimes \left|00\right\rangle \mapsto (a\left|001\right\rangle + b\left|110\right\rangle) \otimes \left|10\right\rangle$$

The syndrome bits are actually telling us the location of the errors. So $\left|10\right\rangle$ tells us that a Z error occurd on the 3 qubit. Sometimes it is written as $\left|Z \text{ on } 3\right\rangle$.

Now we can measure the syndrome and know the error location without changing the state. Then, we can apply the Z back to correct it.

2.1.1 Bit flip error

In the $+/-$ basis, it negates the $-$.

$$IXI\left|\psi_L\right\rangle = a\left|+++\right\rangle - b\left|---\right\rangle$$

This is not an error you can detect, just like the bit flip code, it is a valid encoding of another state $\left|\varphi\right\rangle = a\left|0\right\rangle - b\left|1\right\rangle$:

$$\left|\varphi_L\right\rangle = a\left|+++\right\rangle - b\left|---\right\rangle$$

We have the same issues with these errors, they get 3 time worse because the code is 3 times as likely to bit flip.

3 Shor's 9 qubit code

This is an example of code concatenation. First we encode using the bit flip code and then encode using the phase flip code.

$$\begin{aligned}
\left|0\right\rangle &\to \left|+++\right\rangle && (3)\\
&\to (\left|000\right\rangle + \left|111\right\rangle) \otimes (\left|000\right\rangle + \left|111\right\rangle) \otimes (\left|000\right\rangle + \left|111\right\rangle) && (4)\\
&= \left|0_L\right\rangle && (5)\\
\left|1\right\rangle &\to \left|---\right\rangle && (6)\\
&\to (\left|000\right\rangle - \left|111\right\rangle) \otimes (\left|000\right\rangle - \left|111\right\rangle) \otimes (\left|000\right\rangle - \left|111\right\rangle) && (7)\\
&= \left|1_L\right\rangle && (8)
\end{aligned}$$

This extends to a general $\left|\psi\right\rangle$ by superposition,

$$\left|\psi\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle \mapsto a\left|0_L\right\rangle + b\left|1_L\right\rangle$$

3.1 Bit flip errors

Suppose the bit flip happens on the first qubit of $|\psi\rangle_L$,

$$X_1 |\psi_L\rangle = a(|100\rangle + |011\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) + \\ b(|100\rangle - |011\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \quad (9)$$

To detect this error, for each group of 3 qubits, calculate the parity of every pair of qubits. For the first group, we will see an error. The parities in the other groups should be 0. Correcting the error is exactly the same as the bit flip code.

3.2 Phase flip

Suppose the phase flip happens on the first qubit,

$$Z_1 |\psi_L\rangle = a(|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle) + (|000\rangle + |111\rangle) \\ +b(|000\rangle + |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \quad (10)$$

We can defend against a phase error by comparing the signs of the three blocks, i.e the parity of signs. Here is one way to implement this. The circuit for a single block looks like this,

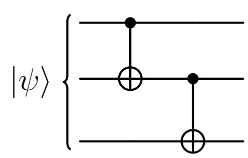

Figure 3: Detecting phase flips in Shor 9-qubit code.

After applying it to all three blocks we get,

$$a|-\rangle|00\rangle \otimes |+\rangle|00\rangle \otimes |+\rangle|00\rangle + b|+\rangle|00\rangle \otimes |-\rangle|00\rangle \otimes |-\rangle|00\rangle$$

Ignoring the $|00\rangle$ we have something that looks the same as a phase flip error, $a|-++\rangle + b|+--\rangle$, which we know how to correct for.

Observe that $Z_1|\psi_L\rangle = Z_2|\psi_L\rangle = Z_3|\psi_L\rangle$. This means our code is a degenerate code. This is a property specific to quantum codes that classical codes do not have. Multiple errors can achieve the same effect on the encoded state, and we can take advantage of this sometimes.

3.3 Bit flip and phase flip

$$\begin{aligned}
Y_1 |\psi_L\rangle &= iX_1 Z_1 |\psi_L\rangle && (11)\\
&= ia\,(|100\rangle - |011\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)\\
&+ ib\,(|100\rangle + |011\rangle) \otimes (|000\rangle - |111\rangle) \otimes |000\rangle - |111\rangle && (12)
\end{aligned}$$

First we undo the bit flip, we can detect this by measuring the parities of the first two qubits. Then we apply the phase flip correction. The order in which errors occur doesn't matter but the order in which we correct them does matter.

3.4 Distance of code

Definition 3.1 (Quantum code)**.** An $[[n, k, d]]$ code uses n qubits to encode k logical qubits and has distance d. The double brackets distinguish it from classical codes.

Shor's 9-qubit code is a $[[9, 1, 3]]$ code.

Question: Why don't the errors get worse when we increase the number of qubits?
Suppose the probability of an error on 1 qubit is p, then with 9 qubits, the probability of one error is $\approx 9p$ and the probability of two erros is $\approx 9^2p^2$. So, this works in the case when $9^2p^2 < p$.

4 Noise

ρ denotes a general mixed quantum state. A natural way of viewing noise is the interaction of ρ with the environment.

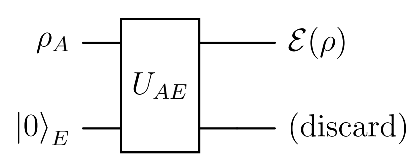

Figure 4: A quantum noise channel.

ρ_A is our state and $|0\rangle_E$ is the starting state of the environment. At some point, they interact and U_{AE} is the unitary describing this. Then, we discard the environment and are left with $\mathcal{E}(\rho)$.

$\rho \mapsto \mathcal{E}(\rho)$ is a quantum channel, also known as a CPTP map or a superoperator. The properties it satisfies are natural, it takes mixed states to mixed states. A mixed state is PSD and trace 1.

1. **(Trace preserving)** $\operatorname{tr} \mathcal{E}(\rho) = \operatorname{tr} \rho$
2. **(Positive)** If the input is PSD then the output will also be PSD,

$$\rho \geq 0 \Rightarrow \mathcal{E}(\rho) \geq 0$$

Actually (2.) is not strong enough. There is a stronger condition,

3. **(Completely positive)** This models the case when ρ has subsystems A, B and the environment only interacts with A. The result should still be a positive.

$$\rho_{AB} \geq 0 \Rightarrow (\mathcal{E}_A \otimes I_B)(\rho_{AB}) \geq 0$$

There are maps that satisfy (2.) but not (3.), they cannot be a result of a process like this. Thus, a quantum channel is defined by properties (1.) and (3.).

Definition 4.1 (Steinspring representation)**.** The Steinspring representation of a quantum channel is defined as discarding the environment after applying a unitary on the system and environment, as in Fig. 4. Any quantum channel has such a representation.

4.1 Kraus representation

Another way to think about channels is to treat discarding the environment as a partial trace operation on the E register. We can calculate the partial trace by summing over the basis for the E register.

$$\begin{aligned}
\mathcal{E}(\rho) &= \operatorname{tr}_E \left(U_{AE}\ \rho_A \otimes |0\rangle\langle 0|_E \, U_{AE}^\dagger \right) &(13)\\
&= \sum_i \langle i|_E \, U\rho \otimes |0\rangle\langle 0| \, U^\dagger \, |i\rangle_E &(14)\\
&= \sum_i \underbrace{\langle i|_E \, U \, |0\rangle}_{K_i} \rho \underbrace{\langle 0|_E \, U^\dagger \, |i\rangle_E}_{K_i^\dagger} &(15)
\end{aligned}$$

This expression gives matrices that acts just on the A register. The unitary acting on A and E can be written as a block with rows and columns indexed by $|0\rangle_E, |1\rangle_E \ldots$ and $\langle 0|_E, \langle 1|_E \ldots$. Then,

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger \tag{16}$$

Definition 4.2 (Kraus operators)**.** The operators on A given by $K_i = \langle 0|_E \, U \, |i\rangle_E$ are the Kraus operators of the channel $\mathcal{E}$. They satisfy,

$$\sum_i K_i^\dagger K_i = I \tag{17}$$

We can verify that they sum to the identity, because $U^\dagger U = I_{AE}$.

$$\sum_i K_i^\dagger K_i = \sum_i \langle 0|_E U^\dagger |i\rangle_E \langle i|_E U |0\rangle_E \tag{18}$$

$$= \langle 0|_E U^\dagger \left(\sum_i |i\rangle\langle i| \right) U |0\rangle_E \tag{19}$$

$$= \langle 0|_E U^\dagger U |0\rangle_E \tag{20}$$

$$= I_A \tag{21}$$

The channel can be thought of as taking a mixed state ρ and selecting one of the K_i's to act on it with some probability. i.e, with probability $\operatorname{tr}\left(K_i \rho K_i^\dagger\right)$, it takes,

$$\rho \mapsto \frac{K_i \rho K_i^\dagger}{\operatorname{tr} K_i \rho K_i^\dagger}$$

Thus, the output is a mixture over these terms for every i.

Note that these probabilities add up to 1. This is because, from the cyclic property of trace, $\operatorname{tr}\left(K_i \rho K_i^\dagger\right) = \operatorname{tr}\left(\rho K_i^\dagger K_i\right)$ and $\sum_i K_i^\dagger K_i = I$. So, we can think of each K_i as a different error that the channel may apply with some probability.

Question: Are the K_i's orthogonal?
They can be orthogonal sometimes but not in general. These K_i's are just general matrices.

4.2 Example noise channels

These are some of the noise channels we might see.

4.2.1 Unitary channel

$$\mathcal{E}(\rho) = U \rho U^\dagger$$

This has a single Kraus operator $K_1 = U$. Examples so far are the Pauli X, Y, Z channels. We will also see the channel that rotates by an angle θ,

$$R_\theta = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{22}$$

When θ is small, it doesn't affect the state much.

4.2.2 Dephasing channel

This channel changes the state with some probability p.

$$\mathcal{E}(\rho) = (1-p)\rho + pZ\rho Z \tag{23}$$

The Kraus operators are $K_1 = \sqrt{(1-p)}I, K_2 = \sqrt{p}Z$. This is an error you can see in a real world. When p is small, it leaves the state alone. You might think that it gets worse when p gets large, but not quite.

Consider $p = \frac{1}{2}$, on the state $|\psi\rangle = a|0\rangle + b|1\rangle$,

$$\mathcal{E}(|\psi\rangle\langle\psi|) = a|0\rangle\langle 0| + b|1\rangle\langle 1|$$

This channel completely destroys the superposition. Meanwhile, when $p = 1$, we can just apply Z to undo it.

4.2.3 Depolarizing channel

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3} \cdot X\rho X + \frac{p}{3} \cdot Y\rho Y + \frac{p}{3} \cdot Z\rho Z \tag{24}$$

$$= \left(1 - \frac{4p}{3}\right)\rho + \frac{4p}{3} \cdot \frac{I}{2} \tag{25}$$

$I/2$ is the maximally mixed state, which we can think of as garbage because it contains no information about our state.

The Kraus representation is not unique, this is one example of that. Another set of Kraus operators for the same channel is,

$$\left\{ \sqrt{1 - \frac{4p}{3}} \cdot I, \quad \sqrt{\frac{2p}{3}}\,|0\rangle\langle 0|\,, \quad \sqrt{\frac{2p}{3}}\,|0\rangle\langle 1|\,, \quad \sqrt{\frac{2p}{3}}\,|1\rangle\langle 0|\,, \quad \sqrt{\frac{2p}{3}}\,|1\rangle\langle 1| \right\}.$$

Next time we will cover more channels and general error correcting codes.