Lecture 12 Quantum error correction

Xiao Yuan

November 20, 2021

In this lecture, we study quantum error correction, including the Shor code, the stabilizer formalism, and fault-tolerance.

1 The Shor code

1.1 Classical repetition code

Consider a classical bit $x \in \{0, 1\}$ and suppose bit flip error, i.e., $x \to x \oplus 1$, happens with probability $p < 0.5$. Can we protect x? The answer is yes and a simple strategy is to use redundant information. In particular, we can use $2n + 1$ bits to encode x as

$$0_L := 00\ldots0, \quad 1_L := 11\ldots1. \tag{1}$$

Then we can use majority vote to decide whether it is 0_L or 1_L. Suppose that error happens independently, then the failure probability is

$$p_{\text{fail}} = \sum_{k=n+1}^{2n+1} \binom{2n+1}{k} p^k (1-p)^{2n+1-k} \leq \sum_{k=n+1}^{2n+1} \left(\frac{e(2n+1)p}{n+1}\right)^k = \left(\frac{e(2n+1)p}{n+1}\right)^{n+1} \frac{1 - \left(\frac{e(2n+1)p}{n+1}\right)^{n+1}}{1 - \frac{e(2n+1)p}{n+1}}. \tag{2}$$

Here we used $\binom{2n+1}{k} \leq \left(\frac{e(2n+1)}{n+1}\right)^k$ for $k \geq n+1$. Therefore, as long as $\frac{e(2n+1)p}{n+1} \leq 1$ or equivalently $p \leq \frac{e(n+1)}{2n+1}$, we can exponentially suppress the failure probability[1].

1.2 Quantum repetition code — bit flip error

There are several challenges to construct a quantum error correcting code.

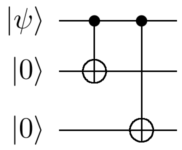
- Quantum states are continuous and cannot be cloned — a quantum state is $|\psi\rangle = a|0\rangle + b|1\rangle$ with continuous a and b, and we cannot clone it to have $|\psi\rangle^{\otimes n}$.
- Errors are also continuous — a general error channel is $\mathcal{E}(\rho) = \sum_j K_j \rho K_j^\dagger$ where each $K_j = a_0 I + a_1 X + a_2 Y + a_3 Z$ with continuous a_i.
- Measurement destroys quantum states — the state collapses if we measure the state or extract information.

For quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$, the quantum repetition code is defined as

$$|\psi\rangle_L = a|0\rangle_L + b|1\rangle_L = a|000\rangle + b|111\rangle. \tag{3}$$

[1] In fact, the bound here is quite loose. We only need $p < 1/2$ to have exponentially small error.

We can realize it with the following quantum circuit.



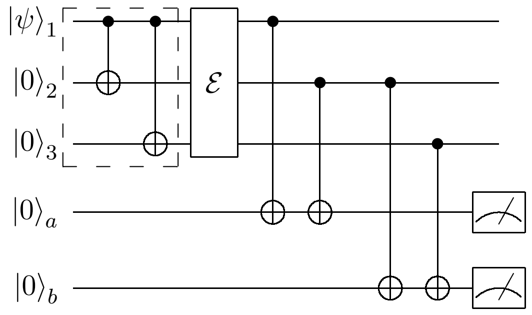
What can we do with this code? Suppose independent bit flip error happens to every qubit, i.e., $\mathcal{E}(\rho) = (1-p)\rho + pX\rho X$, then

$$\mathcal{E}_1 \circ \mathcal{E}_2 \circ \mathcal{E}_3(\psi_L) = (1-p)^3\psi_L + p(1-p)^2\big[X_1\psi_L X_1 + X_2\psi_L X_2 + X_3\psi_L X_3\big] + \mathcal{O}(p^2). \tag{4}$$

Now the leading order errors are $X_1\psi_L X_1 + X_2\psi_L X_2 + X_3\psi_L X_3$, which are independent bit flip errors on each qubit. We can detect these errors by majority vote, or using the nondestructive measurement

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111|, \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011|, \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101|, \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|, \end{aligned} \tag{5}$$

which can be realize using the following circuit



Specifically, the ancillary qubit a is 0 iff qubit 1 and 2 are the same and it is 1 otherwise, the ancillary qubit b is 0 iff qubit 2 and 3 are the same and it is 1 otherwise. Note that the two ancillary qubits effectively measures an eigenstate of Z_1Z_2 and Z_2Z_3. Specifically, when $a = 0$ (1) we have $Z_1Z_2 = 1$ (-1).

Therefore, the there are four cases of the two ancillary qubit measurement corresponds to four eigenstates of Z_1Z_2 and Z_2Z_3, that is the four nondestructive measurement

$$\begin{aligned} &a = 0,\ b = 0 \leftrightarrow Z_1Z_2 = 1,\ Z_2Z_3 = 1 \leftrightarrow P_0, \\ &a = 0,\ b = 1 \leftrightarrow Z_1Z_2 = 1,\ Z_2Z_3 = -1 \leftrightarrow P_3, \\ &a = 1,\ b = 0 \leftrightarrow Z_1Z_2 = -1,\ Z_2Z_3 = 1 \leftrightarrow P_1, \\ &a = 1,\ b = 1 \leftrightarrow Z_1Z_2 = -1,\ Z_2Z_3 = -1 \leftrightarrow P_2, \end{aligned} \tag{6}$$

The ZZ or P measurements are called the syndrome measurements.

To see the equivalence between the ZZ operators and the projectors P, we first define the projector of $Z_iZ_k = \pm 1$ as $\Pi_{Z_iZ_k=\pm 1} = (\mathbb{I} \pm Z_iZ_k)/2$. For example, $\Pi_{Z_1Z_2=1} = (\mathbb{I} + Z_1Z_2)/2 = (|00\rangle\langle 00| + |11\rangle\langle 11|)_{12} \otimes \mathbb{I}_3$ and $\Pi_{Z_2Z_3=-1} = (\mathbb{I} - Z_2Z_3)/2 = \mathbb{I}_1 \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|)_{23}$. Then the projector with both $Z_1Z_2 = 1$ and $Z_2Z_3 = -1$ is $\Pi_{Z_1Z_2=1\&Z_2Z_3=-1} = \Pi_{Z_1Z_2=1}\Pi_{Z_2Z_3=-1} = |001\rangle\langle 001| + |110\rangle\langle 110| = P_3$.

Using the four measurements in Eq. (5), we can therefore detect which error happens. That is, P_i corresponds to the case of bit flip error on the ith qubit ($i \in [1,3]$). Then we can apply a recovery operation to correct single qubit errors. The above discussion ignores the case with more than one errors and it is not hard to see that we cannot detect or correct more those cases. Now we study whether error correction is useful at all. Without error correction, the state is $\mathcal{E}(\psi)$ whose fidelity to ψ is

$$F(\mathcal{E}(\psi),\psi) = \sqrt{\langle\psi|\mathcal{E}(\psi)|\psi\rangle} = \sqrt{(1-p) + p\,\langle\psi|X\,|\psi\rangle\,\langle\psi|\,X|\psi\rangle}, \tag{7}$$

with a minimal value of $\sqrt{1-p}$. With error correction, we have the ideal encoded state $|\psi\rangle_L$ and the corrected noisy state $\rho = [(1-p)^3 + 3p(1-p)^2]\psi_L + \dots$. The fidelity of the corrected state is

$$F(\rho,\psi_L) = \sqrt{\mathrm{Tr}[\psi_L\rho]} \geq \sqrt{(1-p)^3 + 3p(1-p)^2} = \sqrt{1-3p^2+2p^3}. \tag{8}$$

To have $F(\rho,\psi_L) > F(\mathcal{E}(\psi),\psi)$, we need $1-3p^2+2p^3 \geq 1-p$ or equivalently $p < 1/2$. Therefore, as long as $p < 1/2$, we can decrease the error or increase the state fidelity.

1.3 Quantum repetition code — phase flip error

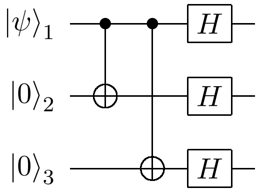
Now suppose the error channel is $\mathcal{E}(\rho) = (1-p)\rho + pZ\rho Z$, can we still detect and correct those errors? Lets see how phase flip affects the state. For state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, we have

$$Z\,|\psi\rangle = a\,|0\rangle - b\,|1\rangle\,, \tag{9}$$

which flips the phase instead of the value, just as the name of the error indicates. While this error seems quite different from the bit flip error, they are actually very related. Remember the transformation between X and Z with $Z = HXH$, a phase flip error could thus be understood as a bit flip error in a different basis. Remember that a transformation of operator is equivalent to a corresponding transformation of the state, i.e., $\langle\psi|[U^\dagger OU]|\psi\rangle = \langle\tilde{\psi}|O|\tilde{\psi}\rangle$ with $|\tilde{\psi}\rangle = U\,|\psi\rangle$. Therefore, we can apply the $H_L = H^{\otimes 3}$ on the encoded state to have

$$|\psi\rangle_L = H_L(a\,|0\rangle_L + b\,|1\rangle_L) = a\,|+\rangle_L + b\,|-\rangle_L = a\,|+++\rangle + b\,|---\rangle\,, \tag{10}$$

with the circuit



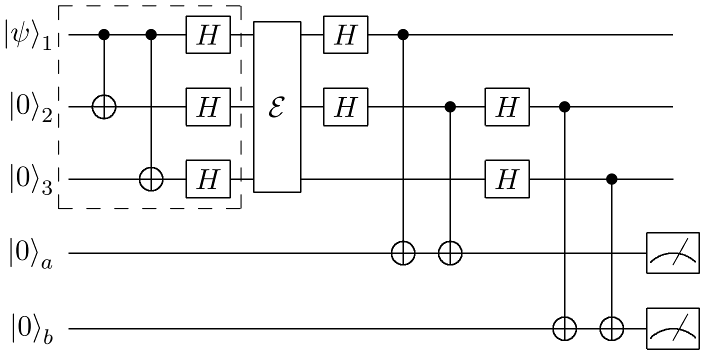
Now suppose Z_1 error happens on qubit 1, we have

$$Z_1\,|\psi\rangle_L = a\,|-++\rangle + b\,|+--\rangle\,, \tag{11}$$

which is analog to the effect of a X_1 error on $a\,|0\rangle_L + b\,|1\rangle_L$. Focusing on the cases with zero and one error, we can apply a transformed nondestructive measurements of Eq. (5),

$$\{H_L P_i H_L\}, \tag{12}$$

to detect phase errors. Specifically, the measurement $H_L P_i H_L$ detects the error Z_i on the ith qubit with $i \in \{1,2,3\}$. The circuit to detect errors is



The relation between the a, b measurement outcomes and the nondestructive measurements $H_L P_i H_L$ is

$$\begin{aligned}
&a = 0,\, b = 0 \leftrightarrow X_1X_2 = 1,\, X_2X_3 = 1 \leftrightarrow H_L P_0 H_L, \\
&a = 0,\, b = 1 \leftrightarrow X_1X_2 = 1,\, X_2X_3 = -1 \leftrightarrow H_L P_3 H_L, \\
&a = 1,\, b = 0 \leftrightarrow X_1X_2 = -1,\, X_2X_3 = 1 \leftrightarrow H_L P_1 H_L, \\
&a = 1,\, b = 1 \leftrightarrow X_1X_2 = -1,\, X_2X_3 = -1 \leftrightarrow H_L P_2 H_L,
\end{aligned} \tag{13}$$

Here we can similarly understand the a and b measurement as X_1X_2 and X_2X_3, respectively.

1.4 The Shor code

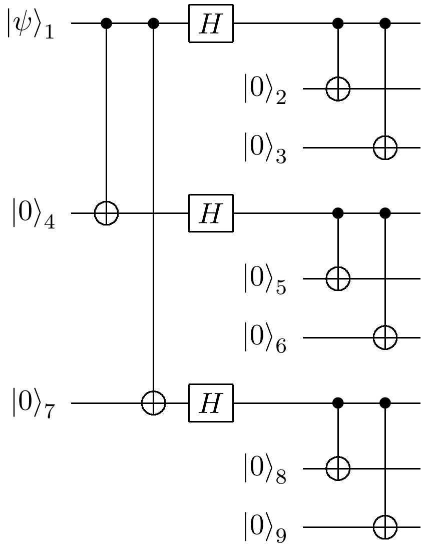
Since the encoding circuits are different for bit and phase flip errors, can we combine them to correct both of them? The answer is yes with the Shor code. The basic idea is to use code concatenation. We first apply the phase flip code to have

$$|0\rangle_L = |+++\rangle = \frac{(|0\rangle + |1\rangle)^{\otimes 3}}{2\sqrt{2}},\ |1\rangle_L = |---\rangle = \frac{(|0\rangle - |1\rangle)^{\otimes 3}}{2\sqrt{2}}. \tag{14}$$

Then for each of $|0\rangle$ and $|1\rangle$, we apply the bit flip code with $|0\rangle \to |000\rangle$ and $|1\rangle \to |111\rangle$. Then we have the Shor code

$$|0\rangle_L = \frac{(|000\rangle + |111\rangle)^{\otimes 3}}{2\sqrt{2}},\ |1\rangle_L = \frac{(|000\rangle - |111\rangle)^{\otimes 3}}{2\sqrt{2}}. \tag{15}$$

The encoding circuit is



We can now detect any single qubit phase or bit flip error. For example, suppose a bit flip error happens to the first qubit, we can then measure Z_1Z_2 and Z_2Z_3 to detect it. Any other bit flip error could be detected similarly. On the other hand, suppose a phase flip error happen to the first qubit, then we can measure $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$ to detect it. To summarize, we can measure the following observables

$$\begin{aligned}
&Z_1Z_2,\ Z_2Z_3,\ Z_4Z_5,\ Z_5Z_6,\ Z_7Z_8,\ Z_8Z_9, \\
&X_1X_2X_3X_4X_5X_6,\ X_4X_5X_6X_7X_8X_9,
\end{aligned} \tag{16}$$

and any single qubit bit or phase flip error could be detected using those measurement outcomes.

Can we do more than this? Suppose both bit and phase flip errors happen to the first qubit, we can actually still detect it using the measurement results of Z_1Z_2, Z_2Z_3, $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$. This works for simultaneous bit and phase flip errors on any qubit.

However, a practical error may be like $\mathcal{E}(\rho) = \sum_j K_j \rho K_j^\dagger$ with $K_j = a_0 I + a_1 X + a_2 Y + a_3 Z$, which is a superposition of the bit, phase, bit+phase errors. Can we still correct them. For simplicity, we assume that an error $K_j \rho K_j^\dagger$ happens to the first qubit of state $|\psi\rangle_L$. Then we have

$$K_j |\psi\rangle_L = a_0 |\psi\rangle_L + a_1 X_1 |\psi\rangle_L + a_2 Y_1 |\psi\rangle_L + a_3 Z_1 |\psi\rangle_L . \tag{17}$$

Now we measure Z_1Z_2, Z_2Z_3, $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$, or equivalently applying one of the 16 projectors $\Pi_{Z_1Z_2=\pm1}$, $\Pi_{Z_2Z_3=\pm1}$, $\Pi_{X_1X_2X_3X_4X_5X_6=\pm1}$, and $\Pi_{X_4X_5X_6X_7X_8X_9=\pm1}$. Suppose we have obtained $Z_1Z_2 = -1$, $Z_2Z_3 = -1$, $X_1X_2X_3X_4X_5X_6 = -1$ and $X_4X_5X_6X_7X_8X_9 = -1$, then the state is projected to

$$\Pi_{Z_1Z_2=-1}\Pi_{Z_2Z_3=-1}\Pi_{X_1X_2X_3X_4X_5X_6=-1}\Pi_{X_4X_5X_6X_7X_8X_9=-1} K_j |\psi\rangle_L = a_2 Y_1 |\psi\rangle_L . \tag{18}$$

Therefore, when we apply the non-destructive syndrome measurements, we also project the state to either $|\psi\rangle_L$, $X_1 |\psi\rangle_L$, $Y_1 |\psi\rangle_L$, or $Z_1 |\psi\rangle_L$, i.e., one of the state with single qubit I, X, Y, Z errors. So as long as we can correct discrete single qubit I, X, Y, Z errors, we can also correct continuous errors!

Now we analyze whether the state fidelity is improved with the Shor code. Consider the depolarizing channel $\mathcal{E}(\rho) = (1-p)\rho + p/3(X\rho X + Y\rho Y + Z\rho Z)$ as a special case, the fidelity without error correction is

$$F(\psi, \mathcal{E}(\psi)) = \sqrt{\mathrm{Tr}[\psi \mathcal{E} \psi]} = \sqrt{\mathrm{Tr}[\psi[(1-4p/3)\psi + 2p/3]]} = \sqrt{1-2p/3} = 1 - p/3 + \mathcal{O}(p^2). \tag{19}$$

On the other hand, suppose we encode the state using the Shor code with logical state ψ_L and independent depolarizing channel happens to every qubit. Since we can correct all single qubit errors, the corrected state is $\rho = \left[(1-p)^9 + 9p(1-p)^8\right]\psi_L + \ldots$, and the fidelity is

$$F(\psi_L, \rho) \geq \sqrt{(1-p)^8(1+8p)} = 1 - 18p^2 + \mathcal{O}(p^3) \tag{20}$$

Consider infidelity as a measure of error, the infidelity is then quadratically improved from $p/3$ to $18p^2$. In practice, we can apply code concatenation to further decrease errors.

Revisiting the aforementioned three challenges, we overcome them using the following ideas.

- Quantum states are continuous and cannot be cloned — we can encode the state into a subspace of a larger entangled state.
- Errors are also continuous — errors become effectively discrete when we apply syndrome measurements.
- Measurement destroys quantum states — we apply non-destructive syndrome measurements.

2 A general theory of QEC

The theory of error correction could be understood abstractly as follows. We first encode the state, say a qubit, into a multi-qubit entangled state $|\psi_L\rangle = a|0\rangle_L + b|1\rangle_L$. The logical state space $\{|0\rangle_L, |1\rangle_L\}$ is only a subspace of the physical state space and we denote the projection from the physical space to the logical space as Π. For example, the projection of the Shor code is

$$\Pi = \Pi_{Z_1Z_2=1}\Pi_{Z_2Z_3=1}\Pi_{Z_4Z_5=1}\Pi_{Z_5Z_6=1}\Pi_{Z_7Z_8=1}\Pi_{Z_8Z_9=1}\Pi_{X_1X_2X_3X_4X_5X_6=1}\Pi_{X_4X_5X_6X_7X_8X_9=1}. \tag{21}$$

That is, for any 9-qubit state $|\psi\rangle$, applying the projection $\Pi|\psi\rangle$ projects it into the code space. Now, suppose an error channel $\mathcal{E}(\psi_L) = \sum_j K_j \psi_L K_j^\dagger$ happens to the logical state ψ_L, it now becomes a mixture of states $\rho_j = K_j \psi_L K_j^\dagger$. We denote the state space with K_j error as $\mathcal{S}_j = \{K_j |\psi_L\rangle, \forall \psi_L\}$. Then error correction works if S_j forms orthogonal subspaces so that there exist a projective measurement $\{\Pi_j\}$ to distinguish them, as shown in Fig. 1(b). Specifically, we need

$$\langle\psi|_L K_j^\dagger K_k |\psi\rangle_L = d_{jk}, \ \forall |\psi\rangle_L , \tag{22}$$

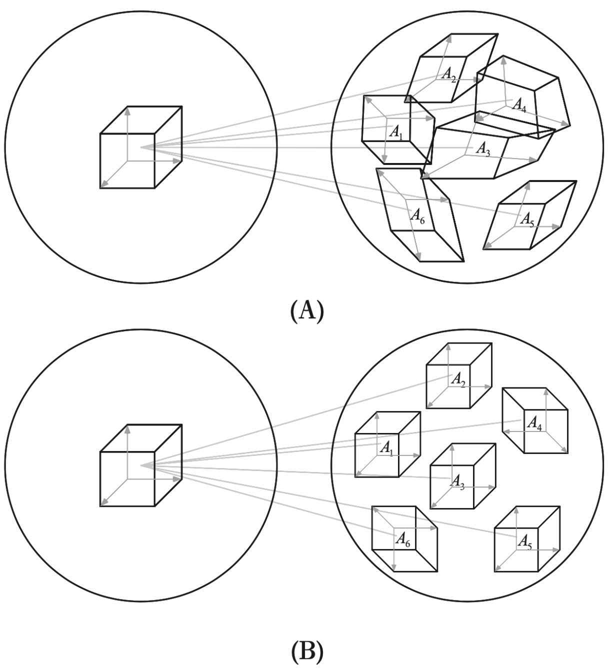


Figure 1: Illustration of quantum error correction. From Nielsen & Chuang's book.

for diagonal d_{jk}. Note that $|\psi\rangle_L = \Pi |\psi\rangle_L$, the above equation is equivalent to

$$\langle\psi|_L \Pi K_j^\dagger K_k \Pi |\psi\rangle_L = d_{jk},\ \forall |\psi\rangle_L , \tag{23}$$

or

$$\Pi K_j^\dagger K_k \Pi = d_{jk} \Pi. \tag{24}$$

Here we thus proved the necessary condition of error correction (not strictly, see discussion below). We can further prove that the above equation is sufficient for error correction. When we have $\Pi K_j^\dagger K_k \Pi = d_{jk}\Pi$, we can explicitly construct the projective measurement $\{\Pi_j\}$ to distinguish between S_j. Consider the polar decomposition of $K_k\Pi = U_k\sqrt{\Pi K_k^\dagger K_k \Pi} = \sqrt{d_{kk}} U_k \Pi$ with some unitary U_k, the effect of K_k on the logical space is thus equivalent to a unitary U_k. Now define projectors $\{\Pi_k = U_k \Pi U_k^\dagger\}$, we have

$$\Pi_k K_k |\psi\rangle_L = U_k \Pi U_k^\dagger K_k |\psi\rangle_L = K_k |\psi\rangle_L , \tag{25}$$

and $\Pi_k \Pi_j = \delta_{k,j}$. Therefore, we can apply a projective measurement $\{\Pi_k\}$, which distinguishes S_j or K_j. Then we can apply the inverse map of U_j to rotate the space S_j or state $K_j |\psi\rangle_L$ back to $\{|\psi\rangle_L\}$.

In the above analysis, we assumed that we need to perfectly distinguish the errors K_j. However, we have seen that even if K_j is a sum of Pauli errors (in this case, we cannot distinguish them), we can still correct them. Actually, we can prove that

Theorem 1. *If error correction works for channel with Kraus operators $\{E_j\}$, it also works for channels with Kraus operators $\{K_k = \sum_k c_{jk} E_j\}$, which is a linear combination of E_j.*

The idea is very similar to our analysis of the Shor code. Basically, since $\{\Pi_k\}$ project the state to the subspace $\mathcal{S}_j = \{K_j |\psi_L\rangle, \forall \psi_L\}$, applying the projection $\{\Pi_k\}$ also project $\{K_k = \sum_k c_{jk} E_j\}$ into a mixture of $\{E_j\}$, which becomes correctable.

Taking the above theorem into account, we thus arrive at the final result for the condition of error correction.

Theorem 2. *Suppose the logical state is defined by a projector P and consider errors with Kraus operator $\{K_j\}$, a necessary and sufficient condition for the existence of an error-correction protocol is*

$$PK_j^\dagger K_k P = \alpha_{jk} P, \tag{26}$$

for any hermitian matrix α_{jk}.

We refer to Nielsen & Chuang's book for the detailed and rigourous proof.