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

Lecture 4: Knill-Laflamme Conditions

Feburary 2, 2024

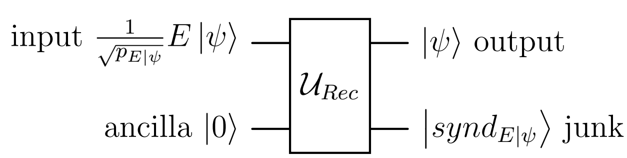
Lecturer: John Wright *Scribe: Shilun Li*

1 Necessary Condition for Correctable Errors

Knill-Laflamme conditions specify what kinds of error can a quantum error correcting code correct. Last lecture, we ended with the definition of a quantum error correcting code. A QECC C is a subspace which is contained in some larger Hilbert space $C \subseteq \mathcal{H}_{phisical}$. Typically $\mathcal{H}_{phisical}$ will be the state of all n-qbit states. Given you code C, we say that it corrects a set of errors $\mathcal{E}$ if there exists a recovery algorithm Rec such that for all $|\psi\rangle \in C$ and $E \in \mathcal{E}$:

$$\text{Rec}(\frac{1}{\sqrt{p_{E|\psi}}} E |\psi\rangle) = |\psi\rangle$$

where $p_{E|\psi} = \langle\psi| E^\dagger E |\psi\rangle$. We can think of $p_{E|\psi}$ as a probability value that the quantum channel decides to apply error E. In general, the probability that a quantum channel applies a given error might actually depend on the state $|\psi\rangle$. We can mathematically model this as a quantum circuit:



$\mathcal{U}_{Rec}$ is called the recovery unitary, it takes in $\frac{1}{\sqrt{p_{E|\psi}}} E |\psi\rangle$ as input and recovers the original codeword $|\psi\rangle$. Last lecture we said that the junk register of the output can be interpreted as a syndrome register, which records what error was applied to the state $|\psi\rangle$. Here we will allow $|synd_{E|\psi}\rangle$ to depend on both E and ψ. Mathematically, we can write this as

$$\mathcal{U}_{Rec}\big(\frac{1}{\sqrt{p_{E|\psi}}} E |\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |synd_{E|\psi}\rangle,$$

which can be rewritten as

$$\mathcal{U}_{Rec} E |\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes \big(\sqrt{p_{E|\psi}}\, |synd_{E|\psi}\rangle\big).$$

Because the expression on the left is a linear function of $|\psi\rangle$, the right hand side must also be a linear function of $|\psi\rangle$. So $\sqrt{p_{E|\psi}}\, |synd_{E|\psi}\rangle$ should be a constant independent of $|\psi\rangle$.

We will denote the constant $\sqrt{p_{E|\psi}}\left|synd_{E|\psi}\right\rangle = \sqrt{p_E}\left|synd_E\right\rangle$. This means that as long as $|\psi\rangle \in C$ and $E \in \mathcal{E}$, the probability of applying errors does not depend on the state $|\psi\rangle$. Intuitively, suppose there is a quantum channel that where the error probability is dependent on the state $|\psi\rangle$, then by learning what error occurred, we would actually learn something about the state $|\psi\rangle$. But if we learn something about $|\psi\rangle$, the state would collapse. Therefore the error being independent of $|\psi\rangle$ is a general property that we want. In addition, this also shows that the syndrome state is independent of $|\psi\rangle$. We saw an example last lecture that in the Shor 9-qbit code [Sho95], the syndrome only records the error applied to the code and does not depend on $|\psi\rangle$.

Let us consider applying the process 2 times and take the dot product, then

$$\big(\left\langle\psi_2\right| E_2^\dagger \otimes \langle 0|\big)\mathcal{U}_{Rec}^\dagger \mathcal{U}_{Rec}\big(E_1\left|\psi_1\right\rangle \otimes |0\rangle\big) = \big(\left\langle\psi_2\right| \otimes \sqrt{p_{E_2}}\left\langle synd_{E_2}\right|\big)\big(\left|\psi_1\right\rangle \otimes \sqrt{p_{E_1}}\left|synd_{E_1}\right\rangle\big)$$

Simplifying the equaiton above, we obtain

$$\left\langle\psi_2\right| E_2^\dagger E_1 \left|\psi_1\right\rangle = \langle\psi_2|\psi_1\rangle \sqrt{p_{E_1} p_{E_2}}\,\langle synd_{E_2}|synd_{E_1}\rangle$$

for all $\psi_1, \psi_2 \in C$ and $E_1, E_2 \in \mathcal{E}$. Here $\sqrt{p_{E_1} p_{E_2}}\,\langle synd_{E_2}|synd_{E_1}\rangle$ measures overlap between E_1 and E_2. Let us consider two special cases:

- Case 1 ($|\psi_1\rangle \perp |\psi_2\rangle$): Then we would have $\langle\psi_2|\psi_1\rangle = 0$ so $\left\langle\psi_2\right| E_2^\dagger E_1 \left|\psi_1\right\rangle = 0$. This is a necessary property for any error correcting code to satisfy. Suppose we apply E_1 to $|\psi_1\rangle$ and E_2 to $|\psi_2\rangle$. Since $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal, we would need $E_1|\psi_1\rangle$ and $E_2|\psi_2\rangle$ to be orthogonal as well. If they were not orthogonal, then no recovery process can turn them into orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, therefore the code would not be reliable.
- Case 2 ($E_1 = E_2$): Then we have $\frac{1}{\sqrt{p_{E_1} p_{E_2}}}\left\langle\psi_2\right| E_2^\dagger E_1 \left|\psi_1\right\rangle = \langle\psi_2|\psi_1\rangle$. This says that if we have two different states $|\psi_1\rangle$ and $|\psi_2\rangle$, and then we apply the same error to them, then the resulting states will have the same inner product as what we started with, which is exactly what we need. Intuitively, the errors act on the states as rotations. And all we have to do to correct the errors is to undo the rotation.

2 Knill-Laflamme Theorem

Theorem 2.1 (Knill-Laflamme [KLV00]). *The set of errors $\mathcal{E}$ that are correctable on a code C if and only if*

$$\left\langle\psi_1\right| E_1^\dagger E_2 \left|\psi_2\right\rangle = \langle\psi_1|\psi_2\rangle \cdot O_{E_1,E_2} \tag{1}$$

holds for all $|\psi_1\rangle, |\psi_2\rangle \in C$ and $E_1, E_2 \in \mathcal{E}$, where O_{E_1,E_2} is a constant depending on E_1, E_2.

Remark 2.2. Although Knill-Laflamme theorem states that if condition (1) is satisfied, then a recovery algorithm exists, we might not be able to construct it if we don't know exactly what the errors are. In addition, the recovery algorithm may be inefficient.

We've already shown one direction of the theorem: if the set of errors are correctable on the code C then this condition is implied. We will now prove the other direction. First, we will state several equivalent ways of writing condition (1).

Proposition 2.3. *Condition (1) in Theorem 2.1 is equivalent to:*

- *Let $\{|\overline{x}\rangle\}_{x\in\{0,1\}^k}$ be an orthonormal basis of C. Then*

$$\langle\overline{x}|\, E_1^\dagger E_2 \,|\overline{y}\rangle = \delta_{x,y} \cdot O_{E_1,E_2} \tag{2}$$

  holds for all basis vector $\overline{x}, \overline{y} \in \{|\overline{x}\rangle\}_{x\in\{0,1\}^k}$.

- *Let $\{|x\rangle\}_{x\in\{0,1\}^k}$ be an orthonormal basis of C and $\{E_1, ..., E_m\}$ be a basis for $\mathcal{E}$. Then*

$$\langle\overline{x}|\, E_a^\dagger E_b \,|\overline{y}\rangle = \delta_{x,y} \cdot O_{E_a,E_b} \tag{3}$$

  holds for all basis vector $\overline{x}, \overline{y} \in \{|\overline{x}\rangle\}_{x\in\{0,1\}^k}$ and $E_a, E_b \in \{E_1, ..., E_m\}$.

- *For all $|\psi\rangle \in C, E \in \mathcal{E}$,*

$$p_{E|\psi} = p_E = \text{constant}. \tag{4}$$

  where $p_{E|\psi} = \langle\psi|\, E^\dagger E \,|\psi\rangle = O_{E,E}$.

The proof can be easily completed using that fact that $\langle\psi_1|\, E_1^\dagger E_2 \,|\psi_2\rangle$ is a multilinear map with respect to $\psi_1,\ \psi_2,\ E_1,\ E_2$. Note that a sufficient condition for equation (2) is:

$$\langle\overline{x}|\, E_a^\dagger E_b \,|\overline{y}\rangle = \delta_{x,y}\delta_{a,b} \tag{5}$$

for all basis vectors $\overline{x}, \overline{y}$ and basis operators E_a, E_b. Now in this special case, we can construct a recovery map by

$$\mathcal{U}_{Rec} : \frac{1}{\sqrt{p_{E_a}}} E_a \,|\overline{x}\rangle \mapsto |\overline{x}\rangle \otimes |a\rangle \tag{6}$$

where $|a\rangle$ is the syndrome. However, the sufficient condition given by Eq. (5) is not satisfied when there is degeneracy. For example in the Shor 9-qbit code:

$$Z_1 \,|\psi\rangle_L = Z_2 \,|\psi\rangle_L$$

so

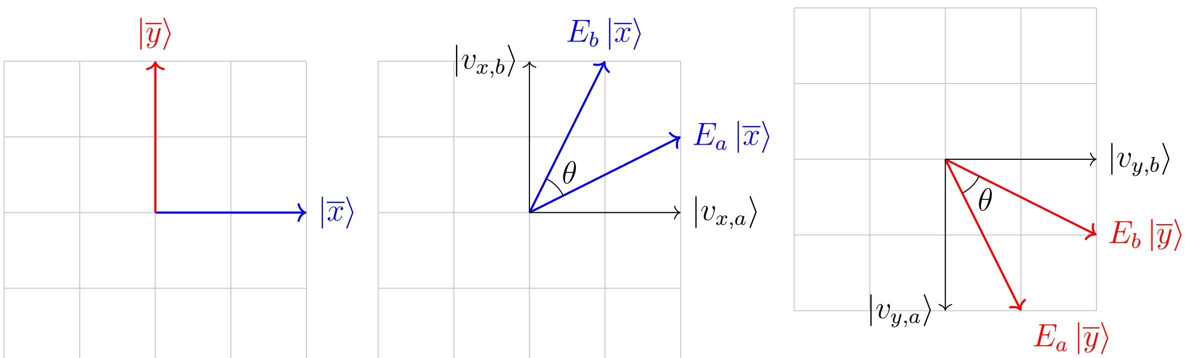
$$\langle\psi|_L \, Z_1^\dagger Z_2 \,|\psi\rangle_L = 1$$

which does not satisfy condition (5).

3 Proof of Knill-Laflamme Theorem

We will now complete the proof of the Knill-Laflamme Theorem by showing that a recovery algorithm $\mathcal{U}_{Rec}$ exists if the Knill-Laflamme condition is satisfied.

Proof. (Theorem 2.1) Using the equivalent condition given by Eq. (3), let us show that condition (3) implies the existence of a correction algorithm $\mathcal{U}_{Rec}$. Condition (3) implies that $\{E_i |\overline{x}\rangle\}_{1\le i\le m}$ is orthogonal to $\{E_i |\overline{y}\rangle\}_{1\le i\le m}$. Let $S_x = \text{span}\{E_i |\overline{x}\rangle\}_{1\le i\le m}$ and $S_y = \text{span}\{E_i |\overline{y}\rangle\}_{1\le i\le m}$. Since $\langle\overline{x}| E_a^\dagger E_b |\overline{x}\rangle = O_{a,b}$. The angle between $E_a |\overline{x}\rangle$ and $E_b |\overline{x}\rangle$ is equal to the angle between $E_a |\overline{y}\rangle$ and $E_b |\overline{y}\rangle$ as illustrated by the figure below:



Therefore, there exists an orthonormal basis $\{|v_{x,i}\rangle\}_{1\le i\le m}$ of S_x such that $E_a |\overline{x}\rangle = \sum_i C_{a,i} |v_{x,i}\rangle$ where $C_{a,i}$ does not depend on x. We can now define $\mathcal{U}_{Rec}$ on the basis $\{|v_{x,i}\rangle\}$.

$$\mathcal{U}_{Rec} |v_{x,i}\rangle = |\overline{x}\rangle \otimes |i\rangle .$$

Then

$$\mathcal{U}_{Rec} E_a |\overline{x}\rangle = \sum_i C_{a,i} \mathcal{U}_{Rec} |v_{x,i}\rangle = \sum_i C_{a,i} |\overline{x}\rangle \otimes |i\rangle = |\overline{x}\rangle \otimes \left(\sum_i C_{a_i} |i\rangle \right)$$

holds for all basis vector $|\overline{x}\rangle$ and E_a, where $\sum_i C_{a_i} |i\rangle$ is the syndrome $|synd_{E_a}\rangle$. Then by linearity, $\mathcal{U}_{Rec}$ is a recovery algorithm for all $E \in \mathcal{E}$ and $|\psi\rangle \in C$ which completes the proof. □

Let us take a closer look at this proof. Intuitively, we can also express $|v_{x,i}\rangle$ using coordinates in the basis S_x:

$$|v_{x,i}\rangle = \sum_a C'_{a,i} E_a |\overline{x}\rangle = F_i |\overline{x}\rangle ,$$

where $F_i = \sum_a C'_{a,i} E_a$. Notice that $\{F_i\}_{1\le i\le m}$ is also a basis of $\mathcal{E}$. So equivalently, we can replace the errors $\{E_i\}_{1\le i\le m}$ with $\{F_i\}_{1\le i\le m}$. Then we would have

$$\langle\overline{x}| F_i^\dagger F_j |\overline{y}\rangle = \langle v_{x,i}|v_{y,i}\rangle = \delta_{x,y}\delta_{i,j}$$

which is the special case of the Knill-Laflamme conditions given by Eq. (5) with a recovery map given by Eq. (6).

Let us consider a channel Φ which acts by

$$\Phi(|\psi\rangle\langle\psi|) = \sum_i E_i |\psi\rangle\langle\psi| E_i^\dagger$$

for all E_i. Then

$$U|\psi\rangle|0\rangle = \sum_i (E_i|\psi\rangle)_A \otimes (|i\rangle)_E,$$

where U is the unitary corresponding to the noise channel Φ. Here $|i\rangle$ is the environment resister and we can obtain the action of the channel by tracing out the environment register. However, let us trace out the register corresponding to the noisy codeword

$$\begin{aligned}
&\mathrm{Tr}_A\left(\sum_i E_i|\psi\rangle \otimes |i\rangle \cdot \sum_j \langle\psi| E_j^\dagger \otimes \langle j|\right) \\
=&\sum_{i,j} \mathrm{Tr}_A\left(E_i|\psi\rangle\langle\psi| E_j^\dagger \otimes |i\rangle\langle j|\right) \\
=&\sum_{i,j} \mathrm{Tr}\left(E_i|\psi\rangle\langle\psi| E_j^\dagger\right) \cdot |i\rangle\langle j| \\
=&\sum_{i,j} \langle\psi| E_j^\dagger E_i |\psi\rangle \cdot |i\rangle\langle j| \\
=&\sum_{i,j} O_{i,j} \cdot |i\rangle\langle j|
\end{aligned}$$

We would notice that the result is independent of the codeword $|\psi\rangle$. So the state that the environment gets after applying a noise is independent of the codestate. This means that the environment does not learn anything about your state and information is not lost.

References

[KLV00] Emanuel Knill, Raymond Laflamme, and Lorenza Viola. Theory of quantum error correction for general noise. *Physical Review Letters*, 84(11):2525–2528, March 2000. 2.1

[Sho95] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, 1995. 1