CMSC 657: Introduction to Quantum Information Processing
Lecture 18

Instructor: Daniel Gottesman

Fall 2024

1 Quantum Error Correction

1.1 The Idea of Error Correction

Alice wants to send qubits to Bob over a noisy quantum channel. Her plan is to use a *quantum error-correcting code (QECC)*: By encoding the logical qubits she wants to send in a larger number of physical qubits, she hopes to protect the information against errors. Note that quantum error correction is also useful for memory: Alice wants to store qubits for a long time despite the possibility of errors that may occur in storage. In this case, "Bob" is really just Alice's future self.

Later, we will briefly discuss fault-tolerant quantum computation, which is a protocol we can put on top of QECCs to perform gates on qubits while they are encoded in a QECC. For now, though, we will assume that the quantum gates being used are perfect and the only time errors occur is during transmission through the channel (or during storage).

Let us begin by thinking about the same problem for classical information. The simplest thing to do is encode the information in a *repetition code*:

$$0 \mapsto 000 \tag{1}$$

$$1 \mapsto 111. \tag{2}$$

To decode, Bob looks at the three bits and take the majority. For instance, if he sees 010, he concludes that Alice's original bit was 0. If there is an error on only 1 bit during the transmission (or no errors at all), Bob will correctly deduce Alice's bit. Of course, if there are 2 or 3 bit errors, Bob will get the wrong answer.

If the probability of error per bit transmitted is p, then the probability of having errors is as follows:

- 0 errors: $(1-p)^3$
- 1 error: $3p(1-p)^2$
- 2 errors: $3p^2(1-p)$
- 3 errors: p^3

That is, the chance of two or more errors is $O(p^2)$, which is thus the probability that Bob will deduce the wrong value for Alice's bit. In contrast, if Alice sends a single bit unencoded, the probability of having an error is p. When p is small enough (because of the constant factor in $O(p^2)$, which is about 3 in this case), Bob's probability of error will be lower in the encoded case than in the unencoded case.

Rather than repeating this calculation every time, we often make the simplifying assumption that there is only 1 error (or t errors for codes that correct more errors), and neglect the possibility of more errors. This should be read as shorthand for the above argument — if the error rate is low enough, then using an error-correcting code will reduce the logical error rate.

1.2 Barriers to Quantum Error Correction

Let us start to think about how to make a quantum error-correcting code. For instance, we might imagine making a quantum repetition code by encoding $|\psi\rangle \mapsto |\psi\rangle^{\otimes 3}$. This is not possible; indeed, there are a number of problems that appear.

1. No-Cloning Theorem prohibits repetition of quantum information.
2. Measuring to learn about the error collapses superpositions.
3. We must correct phase errors as well as bit flip errors.
4. We must correct dephasing errors, decoherence, continuous rotations, etc.

Quantum error correction looks hopeless, but of course it's not or the lecture would have to end here. In fact, the prospect of building a quantum computer without error correction would be fairly hopeless, and a lot of what we've done up to now in the class would be pointless. (Although some of it, and some of what we'll do later, still has applications either to small quantum devices or to simply our conceptual understanding of quantum mechanics.)

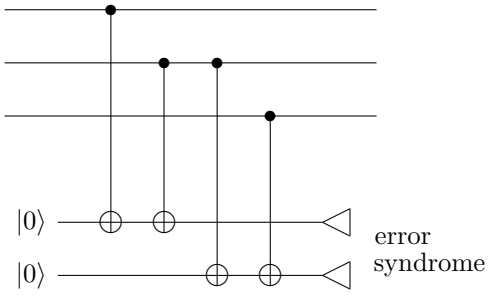
1.3 Three-Qubit Code(s)

Let us try to attack the first two problems first and leave the last two for later. First of all, while we can't repeat general quantum states, we can repeat in a basis. We know the classical repetition code corrects bit flip errors, so why can't we use it to protect quantum information from bit flip errors too?

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle. \tag{3}$$

This does not violate the No-Cloning Theorem, since the encoding of a superposition is an entangled state and not three copies of the original superposition. We are spreading the information out, but not really repeating it.

How can we learn the error without collapsing the superposition? The trick is to measure only the error and not the encoded state. In the case of the repetition code, we only need to know if one of the bits is different and if so, which one. We can learn that without finding out what the actual encoded state is if we measure whether the first two qubits are the same or different (in the computational basis), and then whether the last two qubits are the same or different:



The *error syndrome*, which we get by measuring the ancillas in this circuit, tells us information about the error. In this case, we have the following correspondence between error syndromes and errors:

00	no error
01	3rd qubit
10	1st qubit
11	2nd qubit

Note that this table does not depend on whether the encoded bit is 0 or 1. Thus, measuring the error syndrome does not collapse superpositions, solving problem 2.

But a code to correct bit flip errors is not enough. Recall that a common sort of error is dephasing, which randomizes the phase. We can represent it as a CP map which does Z with some probability, as opposed to the X errors representing bit flips. How can we make a code correcting phase errors? Well, if we *only* want to correct phase errors, we can recall that the Hadamard switches the eigenbases of X and Z:

$$|0\rangle \longleftrightarrow |+\rangle = |0\rangle + |1\rangle \tag{4}$$
$$|1\rangle \longleftrightarrow |-\rangle = |0\rangle - |1\rangle \tag{5}$$

In particular, Z in the $|+\rangle, |-\rangle$ basis acts like a bit flip. Thus, if we do the repetition code in the Hadamard-rotated basis, we can correct a single phase error:

$$|0\rangle \mapsto |+\rangle|+\rangle|+\rangle \tag{6}$$
$$|1\rangle \mapsto |-\rangle|-\rangle|-\rangle \tag{7}$$
$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|+++\rangle + \beta|---\rangle. \tag{8}$$

We can measure the error syndrome by doing the same circuit in the Hadamard-rotated basis (and recall that that basically means doing the CNOTs backwards; also the ancilla initial states become $|+\rangle$ instead of $|0\rangle$).

1.4 9-Qubit Code

However, we'd like to correct both bit and phase flip errors at the same time. We can do so by increasing to 9 qubits and repeating in both bases:

$$|0\rangle \mapsto (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \tag{9}$$
$$|1\rangle \mapsto (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \tag{10}$$

Within each set of 3 qubits, we can correct a bit flip error as before, by comparing to see which qubit is different from the other two. We can also compare the phases between the sets of three in order to see which phase is different from the other two. This is a bit more involved, but can be done as well, and lets us correct a phase error. This solves problem 3.

Indeed, we've gotten something for free. Since the bit flip and phase flip error correction procedures are independent from each other, we can correct both a bit flip and a phase flip simultaneously. In particular, we can correct a $Y = iXZ$ error.

If we want to correct general 1-qubit errors, though (problem 4), what do we do? Let us do something very naive: Pretend that the actual error was a Pauli error X, Y, or Z and just try to correct it under that assumption.

Let us take a concrete example of over-rotation:

$$R_\theta = \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \cos\theta I - i\sin\theta Z. \tag{11}$$

Suppose we have an error which does this on qubit j:

$$R_{2\theta}^{(j)}|\psi\rangle|0\rangle_{syn} = (\cos\theta|\psi\rangle - i\sin\theta Z^{(j)}|\psi\rangle)|0\rangle_{syn}. \tag{12}$$

(The $|0\rangle$ is the ancilla that we will be using for the error syndrome.) When we interact the QECC with the ancilla qubits, we have that in any given branch of the superposition, the ancilla records the Pauli error that occurred. By linearity, the state as a whole is the superposition of those possibilities with the same amplitudes as before the interaction:

$$\mapsto \cos\theta|\psi\rangle|\text{no error}\rangle_{syn} - i\sin\theta Z^{(j)}|\psi\rangle|Z^{(j)}\rangle_{syn}. \tag{13}$$

When we measure the ancilla to learn the error syndrome, the superposition collapses to one of two probabilities:

$$\text{Prob. } \cos^2\theta: \qquad |\psi\rangle|\text{no error}\rangle_{syn} \tag{14}$$

$$\text{Prob. } \sin^2\theta: \qquad Z^{(j)}|\psi\rangle|Z^{(j)}\rangle_{syn} \tag{15}$$

In either case, the error given by the error syndrome matches the actual error remaining. In either case, correcting the measured Pauli error returns the original codeword.

We can generalize this statement:

Theorem 1. *If a QECC corrects errors A and B, it also corrects $\alpha A + \beta B$. It follows that if a QECC corrects I, X, Y, and Z on all single qubits, it corrects all single-qubit errors. If the QECC corrects $\leq t$-qubit tensor products of X, Y, and Z, it corrects all t-qubit errors.*

The last statements follow because I, X, Y, and Z form a basis for the space of 2×2 matrices. Certainly any unitary error on a single qubit can be written as a sum of I, X, Y, and Z, so can be corrected by the first statement of the theorem. Indeed, any non-unitary 2×2 matrix can also be written in this way, so the code corrects non-unitary errors as well. Thus, we can correct general single-qubit CP maps. Under the error,

$$|\psi\rangle\langle\psi| \mapsto \sum_k A_k|\psi\rangle\langle\psi|A_k^\dagger. \tag{16}$$

That is, we have a mixture of $A_k|\psi\rangle$ with different probabilities. Each A_k can be corrected by the code, so the whole superoperator can be corrected.

There are two ways to have a "small" error in quantum mechanics: One is to have a small probability of error, leading to only a few qubits that have errors while all the others are perfect. The other possiblity is to have an action close to the identity on every qubit. For instance, suppose we have $U_\epsilon = I + \epsilon U'$. Then

$$U_\epsilon^{\otimes n} = I + \epsilon[U^{'(1)} + U^{'(2)} + \ldots + U^{'(n)}] + O(\epsilon^2). \tag{17}$$

The $O(\epsilon)$ term consists of a sum of 1-qubit errors, so given a code (like the 9-qubit code) that corrects all 1-qubit errors, by the theorem, it also corrects the $O(\epsilon)$ term here. (A QECC corrects a sum of correctable errors even if they act on different qubits.) Thus, the state after error correction only has errors of size $O(\epsilon^2)$, which includes two-qubit and larger errors.

1.5 Pauli Group

The Pauli group P_n consists of the tensor products of I, X, Y, and Z on n qubits, with overall phase ± 1, $\pm i$.

- It is a *group* — closed under multiplication.
- Any element of P_n squares to $\pm I$.
- Any two elements of P_n either commute or anticommute.

We will be using the Pauli group a lot in the next lecture.