Week 9 : Quantum Error Correction and Fault Tolerance

Contents

Mathematical models of computation such as Turing machines and Quantum Turing machines are idealised abstractions which execute algorithms precisely and without any error. Physical devices that implement such abstract models are imperfect and are subject to electrical noise which result in errors causing computed values to be different from expected values.

While it is impossible to entirely eliminate the source of these errors, we can design schemes which would allow us to recover from these errors with a reasonable amount of additional memory and computation.

1 Classical Error Correction

While the aim of this text is to discuss quantum error correction, it is necessary that we first understand the fundamentals of error correction in general by studying error correction in a classical setting.

The error correction process can be broken down into:

1. Characterising the error model.
2. Introducing redundancy through encoding.
3. Error recovery process.

1.1 The Error Model

The first step to correct the errors our bits are being subjected to we must first understand the nature of these errors and characterise them through an *error model*.

When are bits are being stored or transported, the transformations that affect them are called a *channel*. One of the simplest error model is a *bit-flip channel*. In this model, each bit is independently flipped with probability p and remains unflipped with probability $1-p$. A more general error model would also account for the correlation between the flipping of individual bits.

The errors model, $\mathcal{E}$, may consist of different operations $\mathcal{E}_i$, each occurring with different probabilities p_i.

1.2 Encoding

Upon describing our error model, we must encode our information in a way that is robust against the errors we described.

This is typically done by adding a number of of extra bits (called the *ancilla*) to a logical bit, b, we wish to protect. The string corresponding to encoded bit is called a codeword, b_{enc}. The set of all such codewords is called the code.

The idea behind adding the ancilla is to introduce redundancy, so that even when errors corrupt some of the bits in a codeword, the remaining bits contain enough information to recover the logical bit.

1.3 Error Recovery

After a codeword, b_{enc} is subjected to some errors the resulting string is b'_{enc}. The procedure for recovering the logical bit, b from b'_{enc} is called the *recovery operation*.

A recovery operation must be able to unambiguously distinguish between codewords after errors have acted on them. Given a code for a set of errors to be classically correctable by that code, we must have,

$$\mathcal{E}_i(k_{enc}) \neq \mathcal{E}_j(l_{enc}), \quad \forall k \neq j.$$

1.4 Fault Tolerance

Intuitively, the way one would assume computation would be carried in tandem with error correction is, a logical bit would operated upon to store the result of an earlier computation, the bit would be encoded before being stored or transported, the bit would be decoded upon arrival and the process would be repeated.

However, this strategy leaves the logical bit unprotected between the decoding and re-encoding. Moreover, the encoding and decoding processes themselves aren't free from errors.

The theory of *fault-tolerant* computing attempts to provide a solution by describing procedures to compute directly on the codewords.

2 Quantum Error Correction

It is possible to generalise classical error correction to the quantum case despite the fact that:

1. Quantum evolution is continuous, as opposed to the classical case which is discrete,
2. Encoding cannot make copies of an arbitrary quantum state,
3. Corruption of encoded quantum state cannot be detected through measurement of the qubits.

2.1 Error Models for Quantum Computation

Just like in the classical case we shall be assuming that, transformations occur on one bit independently from others, due to the simplicity of the analysis.

Errors occur on a qubit when its evolution differs from the desired one. This difference can occur due to imprecise control over the qubits or by interaction of the qubits with an environment.

Let us see how qubits evolve when they interact with their environment $|E\rangle$:

$$|0\rangle|E\rangle \mapsto \beta_1|0\rangle|E_1\rangle + \beta_2|1\rangle|E_2\rangle,$$

$$|1\rangle|E\rangle \mapsto \beta_3|1\rangle|E_3\rangle + \beta_4|0\rangle|E_4\rangle.$$

More generally,

$$(\alpha_0|0\rangle + \alpha_1|1\rangle)|E\rangle \mapsto \alpha_0\beta_1|0\rangle|E_1\rangle + \alpha_0\beta_2|1\rangle|E_2\rangle + \alpha_1\beta_3|1\rangle|E_3\rangle + \alpha_1\beta_4|0\rangle|E_4\rangle.$$

Therefore, post interaction we may write,

$$\begin{aligned}\alpha_0\beta_1|0\rangle|E_1\rangle + \alpha_0\beta_2|1\rangle|E_2\rangle + \alpha_1\beta_3|1\rangle|E_3\rangle + \alpha_1\beta_4|0\rangle|E_4\rangle \\ = \frac{1}{2}(\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_1|E_1\rangle + \beta_3|E_3\rangle) \\ + \frac{1}{2}(\alpha_0|0\rangle - \alpha_1|1\rangle)(\beta_1|E_1\rangle - \beta_3|E_3\rangle) \\ + \frac{1}{2}(\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_2|E_2\rangle + \beta_4|E_4\rangle) \\ + \frac{1}{2}(\alpha_0|0\rangle - \alpha_1|1\rangle)(\beta_2|E_2\rangle - \beta_4|E_4\rangle).\end{aligned}$$

By letting $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, we get,

$$\begin{aligned}\alpha_0|0\rangle - \alpha_1|1\rangle &= Z|\psi\rangle \\ \alpha_0|1\rangle + \alpha_1|0\rangle &= X|\psi\rangle \\ \alpha_0|1\rangle - \alpha_1|0\rangle &= XZ|\psi\rangle\end{aligned}$$

Thus, the most general evolution that can occur on a single may be written as,

$$\begin{aligned}|\psi\rangle\ |E\rangle \mapsto \frac{1}{2}|\psi\rangle(\beta_1|E_1\rangle + \beta_3|3\rangle) + \frac{1}{2}(Z|\psi\rangle)(\beta_1|E_1\rangle - \beta_3|3\rangle) \\ + \frac{1}{2}(X|\psi\rangle)(\beta_2|E_2\rangle + \beta_4|4\rangle) + \frac{1}{2}(XZ|\psi\rangle)(\beta_2|E_2\rangle - \beta_4|4\rangle).\end{aligned}$$

Specific errors may described as special cases of the right side of the above equation, by substituting specific values into the equation.

2.2 Encoding

An naive idea one might think of is to duplicate the value of the logical qubit into the ancilla, however, this isn't possible as a result the no-cloning theorem, as presented below.

Theorem (No-cloning)**.** *There is no superoperator $\mathcal{F}$ that performs*

$$|\psi\rangle\langle\psi| \otimes |s\rangle\langle s| \overset{\mathcal{F}}{\mapsto} |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|$$

for arbitrary choices of $|\psi\rangle$ (where $|s\rangle$ is some fixed ancilla state). That is, there is no quantum operation which can clone an unknown arbitrary quantum state.

Keeping the no-cloning theorem in mind we must come up with an alternate way to implement U_{enc}, the unitary matrix which maps $|\psi\rangle\,|00\cdots0\rangle$ to the code $|\psi_{enc}\rangle$ (where $|00\cdots0\rangle$ is the initial value of the ancilla).

A possible choice for U_{enc} for a three-qubit code would be the unitary matrix which maps

$$(\alpha_0\,|0\rangle + \alpha_1\,|1\rangle)\,|00\rangle \overset{U_{enc}}{\longmapsto} \alpha_0\,|000\rangle + \alpha_1\,|111\rangle$$

2.3 Error Recovery

When a qubit $|\psi\rangle$ is subjected to errors in a channel, then the result is a state with density matrix,

$$\sum_i \mathcal{E}_i\,|\psi\rangle\langle\psi|\,\mathcal{E}_i^{Q\dagger}$$

where $\mathcal{E}_i$ define the error model.

Similarly, the encoded state $|\psi_{enc}\rangle$ goes to a state with density matrix,

$$\sum_i \hat{\mathcal{E}}_i\,|\psi\rangle\langle\psi|\,\hat{\mathcal{E}}_i^{Q\dagger}$$

where $\hat{\mathcal{E}}_i$ are distinct from $\mathcal{E}_i$ due to the higher dimension of $|\psi_{enc}\rangle$ than the original logical qubit, as contributed by the ancilla.

In order to recover the original qubit, we must define a recovery operation $\mathcal{R}$, that undoes just enough of the noise on the encoded state, so that after decoding and tracing out the ancilla we are left with the original state.

Subject to the noise described by $\mathcal{E}_i$, we define the *fidelity* of $\mathcal{R}$ by

$$F(\mathcal{R},\mathcal{C},\mathcal{E}) = \min_{|\psi\rangle}\ \langle\psi|\,\rho_\psi\,|\psi\rangle$$

where

$$\rho_\psi = \mathrm{Tr}_{\mathrm{anc}}\Big(\sum_j \mathcal{R}_j U_e^\dagger\big(\sum_i \mathcal{E}_i U_{enc}\,\langle\psi|\ \langle00\cdots0|00\cdots0\rangle\ |\psi\rangle\,U_{enc}^\dagger\mathcal{E}_i^\dagger\big)U_e\mathcal{R}^\dagger\Big)$$

The fidelity gives us the minimum probability that any state $|\psi\rangle$ is encoded, transformed by channel errors and is decoded by $\mathcal{R}$ to some state $|\rho\rangle$ such that there is no error in the encoded state. Therefore, the term $(1-F(\mathcal{R},\mathcal{C},\mathcal{E}))$, gives an upper bound on the probability with which any encoded state can end up in a wrong state after decoding.

A recovery operation $\mathcal{R}$ is *error correcting* when its fidelity is 1 with respect to the error operators defined by $\mathcal{E}$. When this happens,

$$\mathrm{Tr}_{\mathrm{anc}}\left[\sum_j \mathcal{R}_j\left(U_{enc}^\dagger\left(\sum_i \hat{\mathcal{E}}_i\left|\psi_{enc}\right\rangle\!\left\langle\psi_{enc}\right|\hat{\mathcal{E}}_i^\dagger\right)U_{enc}\right)\mathcal{R}_j^\dagger\right] = |\psi\rangle\langle\psi|$$

2.4 Quantum Codes

2.4.1 Three-Qubit Code for Bit-Flip Errors

The error model we are interested in is the *bit-flip channel* where a qubit may flip with probability p, as described by

$$\rho = |\psi\rangle\langle\psi| \mapsto \rho_f = (1-p)\,|\psi\rangle\langle\psi| + pX\,|\psi\rangle\langle\psi|\,X.$$

We may obtain a three-qubit bit-flip code by mapping the basis states $|0\rangle$ to $|000\rangle$ and $|1\rangle$ to $|111\rangle$ as

$$\alpha_0\,|0\rangle + \alpha_1\,|1\rangle \mapsto \alpha_0\,|000\rangle + \alpha_1\,|100\rangle \mapsto \alpha_0\,|000\rangle + \alpha_1\,|111\rangle\,.$$

This encoding is essentially an embedding of a state from a 2-dimensional subspace to a larger 8-dimensional subspace. Note that this isn't the same a simple repetition rule.

If at most 1-qubit error occurs on any codeword for this code, then decoding this using the inverse of the encoding operation, the Toffoli gate will recover the original state. The reader is encouraged to work out this fact for themselves.

2.4.2 Three-Qubit Code for Phase-Flip Errors

The error model we are interested in is the *phase-flip channel*. This channel has no direct analog in the classical case. However, there exists a rather simple technique to transform a phase-flip error into a bit-flip error. Consider the Hadamard bases $|+\rangle$ and $|-\rangle$. A phase flip error in Hadamard bases takes the $|+\rangle$ state to the $|-\rangle$ state and vice versa. Therefore in the Hadamard basis, phase-flip error are just like bit-flip errors.

Therefore, we can encode $|0\rangle$ to $|+++\rangle$ and $|1\rangle$ to $|---\rangle$. According to this rule the encoding operation we get is

$$\alpha_0\,|0\rangle + \alpha_1\,|1\rangle \mapsto \alpha_0\,|000\rangle + \alpha_1\,|100\rangle \mapsto \alpha_0\,|+++\rangle + \alpha_1\,|---\rangle\,.$$

The recovery operation performed is identical to the recovery process the three-bit code for bit-flip errors only now with respect to the Hadamard basis.

2.4.3 Nine-Qubit Shor Code

This code is a combination of the three-qubit code for bit-flip errors and the the three-qubit code for phase-flip errors. It allows us to correct simultaneously correct at most 1 bit-flip error and 1 phase-flip error.

The encoding for the nine-qubit shor code is a two stage process. First, each qubit is encoded as in the three-qubit phase-flip code,

$$|0\rangle \mapsto |+++\rangle\,,$$

$$|1\rangle \mapsto |---\rangle\,.$$

Second, each qubit in the phase-flip code is are encoded as in the three-qubit bit-flip code,

$$|+\rangle \mapsto \frac{1}{\sqrt{2}}(\,|000\rangle + |111\rangle),$$

$$|-\rangle \mapsto \frac{1}{\sqrt{2}}(\,|000\rangle - |111\rangle).$$

Thus, the final codeword is

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}(\,|000\rangle + |111\rangle)(\,|000\rangle + |111\rangle)(\,|000\rangle + |111\rangle),$$

$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}(\,|000\rangle - |111\rangle)(\,|000\rangle - |111\rangle)(\,|000\rangle - |111\rangle).$$

The correctness of this code follows naturally from correctness of the three-qubit code for bit-flip errors and the the three-qubit code for phase-flip errors. The reader is encouraged to work out the proof of correctness of the nine-bit shor code for themselves.

3 Exercises

1. Given a n qubit system, where there is a probability p of a bit flipping after a certain operation. What is the probability that at least k bits get flipped after said operation? What is the probability that at most k bits get flipped?

2. In a 1 qubit system where we are using the three-qubit code for bit-flip errors, the qubit gets flipped with probability p after any operation. What is the probability that we can continue to use this code for n operations consecutively.

3. Give a proof of correctness of the three-qubit code for bit-flip errors.

4. Give a proof of correctness of the three-qubit code for phase-flip errors.

5. Give a proof of correctness of the nine-qubit shor code.