Quantum Error Correction

Week 10

Introduction

Introduction

- Abstract models of computation (think Turing machines) are ideal and error free. Real computers? Not so much.
- It is impossible to get rid of these errors, we can however develop techniques to recover from these errors.

Classical Error Correction

Classical Error Correction

The error correction process can be broken down into:

- Characterising the error model.
- Introducing redundancy through encoding.
- Error recovery process.

The Error Model

- We must first understand the errors that need to be corrected before developing the correction technique.
- Bits, during processing are subjected specific transformations, called a *channel*.
  - e.g. Bit-flip channel. As the name suggests a bit-flip channel flips bits with some probability p.
- For the sake of simplicity we shall assume independence of errors, however a more robust error model would account for correlation between errors.
- Thus we come up with an error model, $\mathcal{E}$ consisting of independent operations $\mathcal{E}_i$, each occurring with different probabilities p_i.

Encoding

- Once we have our error model, we must encode our information in a way that is robust against the errors we described.
- This is done by adding extra bits called the *ancilla* to the logical bit. All the bits in totality are called the *codeword*.
- The general idea is that, even when some bits are corrupted in the codeword, the uncorrupted bits would contain enough information to extract the logical bit.

Error Recovery

- Once we are done processing our bits we must undo the errors that inevitably creep in.
- We must able to unambiguously distinguish between codewords after the errors to correct them,

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

Fault Tolerance

- To compute by encoding, operating on, and decoding bits is a natural idea. However it ignores the probability that the encoding the recovery process would themselves be prone to errors.
- The theory of *fault-tolerant* computing attempts to provide a solution by describing procedures to compute directly on the codewords.

Quantum Error Correction

Quantum Error Correction

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

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

- The transformations being carried out on a qubit $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ by its environment effectively form an operator, say $|E\rangle$.
- A generic evolution of a qubit would be,

$$\begin{aligned}(\alpha_0 |0\rangle + \alpha_1 |1\rangle) |E\rangle \mapsto & \alpha_0\beta_1 |0\rangle |E_1\rangle + \alpha_0\beta_2 |1\rangle |E_2\rangle \\ & + \alpha_1\beta_3 |1\rangle |E_3\rangle + \alpha_1\beta_4 |0\rangle |E_4\rangle .\end{aligned}$$

Error Models for Quantum Computation ii

- Carrying out algebraic manipulation, and substituting operation with the Pauli X, Y, and Z matrices, we get the most general evolution of qubit that can occur,

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

- Specific cases of this generic evolution may be considered when dealing with specific channels.

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

$$(\alpha_0 |0\rangle + \alpha_1 |1\rangle) |00\rangle \xmapsto{U_{enc}} \alpha_0 |000\rangle + \alpha_1 |111\rangle .$$

- When a qubit $|\psi\rangle$ and its the encoded state $|\psi_{enc}\rangle$ undergo errors in channel, the resultant states have density matrices,

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

  where $\mathcal{E}$ and $\hat{\mathcal{E}}$ are the error models for $|\psi\rangle$ and $|\psi_{enc}\rangle$.
- In order to recover the original qubit, we must define a recovery operation $\mathcal{R}$. The recovery operation is defined to maximise the probability of getting the correct qubit after its application.

- $\mathcal{R}$ is defined as,

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

where,

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

$$\dots U_{enc}^\dagger \mathcal{E}_i^\dagger \big) U_e \mathcal{R}^\dagger \Big)$$

Quantum Codes

Three-Qubit Code for Bit-Flip Errors

- Channel is a bit-flip channel, where a qubit may flip with probability p.
- Qubit evolution is 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 as,

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

- Recovery is the inverse of the encoding operation.
- This error code can correct at most 1 bit flip.

Three-Qubit Code for Phase-Flip Errors

- Channel is a bit-flip channel, where a qubit may flip with probability p.
- In the Hadamard basis $|+\rangle$ and $|-\rangle$, a phase flip error takes one basis vector to another. Therefore, by mapping the computational basis to the Hadamard basis, this problem can be reduced to that of making an error code for the bit-flip channel.
- Therefore, the encoding rule we get is,

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

- Recovery is the inverse of the encoding operation.
- This error code can correct at most 1 phase flip.

- This code was designed to correct an error involving at most one bit-flip and one phase flip.
- Encoding is a two step process. First, each qubit is encoded as in the three-qubit phase-flip code,

$$|0\rangle \mapsto |+++\rangle\,, \quad |1\rangle \mapsto |---\rangle\,.$$

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

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

Nine-Qubit Shor Code ii

- Thus, the final codeword is

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

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