Introduction to Quantum Computing
Lecture 12: Quantum Error Correction

Petros Wallden

School of Informatics, University of Edinburgh

26th October 2017
- Information processing is affected by random errors caused by noise.
- In practical applications, we either have truly noiseless systems or we protect against errors caused by noise.
- The process of protecting and correcting errors caused by noise is called *error-correction*.
- In classical computers, each bit can have at most one type of error, which is a *flip* $0 \rightarrow 1$ and $1 \rightarrow 0$. 


- A channel that induces a bit flip with same probability is called binary symmetric

\[
\begin{array}{c}
0 & \quad \frac{1-p}{p}
\end{array}
\begin{array}{c}
0 & \quad 0
\end{array}
\begin{array}{c}
1 & \quad \frac{p}{1-p}
\end{array}
\begin{array}{c}
1 & \quad 0
\end{array}
\]

Probability for flipping $p$ and for not flipping $(1 - p)$

- Quantum case more complicated (see below).

**Classical error correction:**

**Encode** each bit to many bits. Simpler example with three bits:

encode bit 0 to 000 and bit 1 to 111

The combination of 000 is the **logical** 0 and similarly 111 is the logical 1

- We assume that probability of flip $p < 1/2$ for each bit crossing the (binary symmetric) channel we consider
- **Majority voting**: We receive three bits having crossed the noisy channel. If we measure 000, 100, 010 or 001 then we say that the intended value of the bit sent was 0. (i.e. allow for one flip)
- If we had done no encoding, the probability of wrong outcome is $p$
- Then probability that using the 3 bits encoding we obtain wrong outcome is given by the probability that at least two flips occurred:
  $$3p^2(1 - p) + p^3$$
  so $p_e = 3p^2 - 2p^3$
  This is strictly less than $p$ provided $p < 1/2$
- By encoding the bit to 3 bits, we reduced the probability of transmitting the wrong result
- This code is called *repetition code*
- Note that error-correction succeeds with some probability (not always) and also depends on the type of channel used (symmetric, value of $p$, etc)
Three Qubit Flip Code

- There are extra difficulties for Quantum Error Correction
  1. **No cloning:** We cannot copy unknown quantum states (necessary for the repetition code)
  2. **Errors are continuous:** There are infinite different types of errors, as opposed to just one kind in classical bits (flip). Any unitary operation corresponds to a different type of quantum error
  3. **Measurement destroys quantum information:** In classical codes, one measures the bits to deduce the logical bit that was sent. In quantum case, if we measure the qubit we disturb the system and the quantum information is lost
- Despite all this, quantum error correction is still possible!
- Let us assume that we have a **bit flip channel**. This is a channel that with probability $(1 - p)$ does nothing to the state $|\psi\rangle$ and with probability $p$ it applies a Pauli $X$ $|\psi\rangle$ which “flips” the qubit.

$$X(a |0\rangle + b |1\rangle) = a |1\rangle + b |0\rangle$$
- We encode the state $|\psi\rangle = a|0\rangle + b|1\rangle$ to the state
  $|\psi\rangle_L = a|000\rangle + b|111\rangle$
  $|0\rangle \rightarrow |0\rangle_L = |000\rangle$
  $|1\rangle \rightarrow |1\rangle_L = |111\rangle$
  $|0\rangle_L, |1\rangle_L$ are the logical states. The circuit that implements this transformation is this (check!)

- The code will be able to detect and correct mistakes that occur in at most one qubit
1. **Error-detection or syndrome diagnosis**: Perform a measurement that tells us what error (if any) has occurred and does not alter the state of the qubit if no errors happened. There are 4 error syndromes

- $P_0 = |000⟩⟨000| + |111⟩⟨111|$ no error
- $P_1 = |100⟩⟨100| + |011⟩⟨011|$ bit flip on first qubit
- $P_2 = |010⟩⟨010| + |101⟩⟨101|$ bit flip on second qubit
- $P_3 = |001⟩⟨001| + |110⟩⟨110|$ bit flip on third qubit

Note that these measurements do not tell what is the qubit “value” but only that if there is a flip
e.g. If a flip at the first qubit we have $|ψ_1⟩ = a|100⟩ + b|011⟩$ which has $⟨ψ_1| P_1 |ψ_1⟩ = 1$

Important is to note that the state remains the same after the syndrome measurement

$P_1 |ψ_1⟩ = |ψ_1⟩$
2. **Recovery**: Depending on the error syndrome we can correct the error by applying a unitary and recover the (encoded) state that was sent

e.g. If the syndrome is $P_1$, we apply at the first qubit Pauli $X$

$$X \otimes 1 \otimes 1 (a |100\rangle + b |011\rangle) = a |000\rangle + b |111\rangle$$

- This procedure recovers the correct state always, if there is at most one qubit corrupted. Similarly to classical case, if $p < 1/2$ of flipping a single qubit, this procedure improves the probability of obtaining the correct result

- It is interesting to note that quantum channels with particular errors affect in different way different states. E.g. the state

$$\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

remains invariant from the action of a bit-flip channel
The bit-flip code is similar to the classical case. However, many different types of errors can corrupt a qubit.

An example is the phase-flip:

$$a |0⟩ + b |1⟩ → a |0⟩ − b |1⟩$$

This is equivalent with a channel that with some probability $p$ applies the Pauli $Z$.

Note the action of such channel on the states $|±⟩$:

$$|+⟩ = \frac{|0⟩+|1⟩}{\sqrt{2}} \quad → \quad \frac{|0⟩−|1⟩}{\sqrt{2}} = |−⟩$$

$$|−⟩ = \frac{|0⟩−|1⟩}{\sqrt{2}} \quad → \quad \frac{|0⟩+|1⟩}{\sqrt{2}} = |+⟩$$

It acts exactly as the bit-flip channel, but in a rotated basis.

We encode the state $|ψ⟩ = a |0⟩ + b |1⟩$ to the state

$$|ψ⟩_L = a |++⟩ + b |−−⟩$$

$$|0⟩ → |0⟩_L = |++⟩$$

$$|1⟩ → |1⟩_L = |−−⟩$$

$|0⟩_L$ and $|1⟩_L$ are the logical states.
Three Qubit Phase Flip

The circuit that implements this transformation is this (check!)

\[|\psi\rangle \quad \text{H} \]
\[|0\rangle \quad \text{H} \]
\[|0\rangle \quad \text{H} \]

1. Error detection: The 4 error syndromes
\[P_0 = |+++-\rangle\langle+++-| + |----\rangle\langle----| \quad \text{no error} \]
\[P_1 = |--++\rangle\langle--++| + |++--\rangle\langle++--| \quad \text{phase flip on first qubit} \]
\[P_2 = |+-+-\rangle\langle+++-| + |---+\rangle\langle--++| \quad \text{phase flip on second qubit} \]
\[P_3 = |+-+-\rangle\langle+++-| + |---+\rangle\langle--++| \quad \text{phase flip on third qubit} \]
2. **Recovery:** Depending on the syndrome we apply the relevant unitary
e.g. phase flip of the second qubit, we apply $1 \otimes Z \otimes 1$

$$1 \otimes Z \otimes 1(a |+ − +\rangle + b |− + −\rangle) = a |+++\rangle + b |− − −\rangle$$
- A simple code can fix both flip and phase errors. It can fix any single qubit error!
- The first such code is due to Peter Shor (1995)
- There are other codes that require fewer qubits
- It is a combination of qubit phase flip and bit flip codes
- It encodes a single qubit using nine (9) qubits
Shor’s Code

- We first encode the qubit using a phase-flip code
  \[ |0\rangle \rightarrow |+ + +\rangle, \quad |1\rangle \rightarrow |- - -\rangle \]
- Then each of those qubits are encoded with bit-flip code, i.e.
  \[ |+\rangle \rightarrow (|000\rangle + |111\rangle)/\sqrt{2} \quad \text{and} \quad |-\rangle \rightarrow (|000\rangle - |111\rangle)/\sqrt{2} \]
Overall the two codewords (logical bits) are:

\[ |0\rangle \rightarrow |0\rangle_L \rightarrow \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \]

\[ |1\rangle \rightarrow |1\rangle_L \rightarrow \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \]

1. Error detection:
First we compare the first two qubits \( Z_1Z_2 \) and the second and third \( Z_2Z_3 \). This procedure detects if there was a bit flip at one of the three first qubits. We then do the same for the second and third group of three-qubits and we have a syndrome for if and where a bit flip has occurred.
Then, by treating the group of three qubits as one, we do the syndrome measurement for the phase flip.
e.g. if a flip occurred at the first qubit
$(|000⟩ + |111⟩) \rightarrow (|000⟩ − |111⟩)$ but the second and third blocks of qubits are still unaltered, so overall we have
$(|000⟩ − |111⟩)(|000⟩ + |111⟩)(|000⟩ + |111⟩)$
- In the above procedure, we may detect for the same qubit, both bit-flip and phase-flip.

In next lecture after introducing the stablizer formalism, we will see the exact syndrome measurements that need to be done

2. Recovery: Depending on the syndrome, we identify the bit that is corrupted and type of error (bit flip or phase flip or both). We can then correct it by applying at the corrupted qubit $X$, $Z$ or $XZ$
Shor’s Code

- Shor’s code is constructed to correct errors that occur to a single qubit only (out of the nine required). Provided that the probability $p$ of (any) error is small enough, one can show that the above code reduces the probability of a mistake.

- It is important to note, that Shor’s code can actually correct any error (arbitrarily small or in any basis), provided it corrupts a single qubit.

- This follows from the fact that any error acting on a single qubit can be written as a linear combination in the following way:

$$ E_i = e_{i0}1 + e_{i1}X + e_{i2}Z + e_{i3}XZ $$

Therefore

$$ E_i |\psi\rangle = e_{i0} |\psi\rangle + e_{i1}X |\psi\rangle + e_{i2}Z |\psi\rangle + e_{i3}XZ |\psi\rangle $$

Measuring the error syndrome collapses this superposition to one of the:

$$ |\psi\rangle, X |\psi\rangle, Z |\psi\rangle, XZ |\psi\rangle $$

which can be corrected with the appropriate recovery procedure.
1. **Code**: Encode the qubits to logical qubits using some code. No measurement takes place, so it is not the same as copying the qubits (unlike classical error-correction)

2. **Error detection**: Apply a measurement that detects if and what error exists. The error syndrome determine what error exists (which qubit and what type)

3. **Recovery (correction)**: Apply a unitary correction according to the error syndrome, in order to recover the initial logical qubit

   - How many errors and of what type we can tolerate depends on the code used
   - Therefore what type of code one needs to use depends on the type of errors induced by his channel
   - We assumed that errors corrupt qubits independently. i.e. the probability that the 1st qubit is corrupted is independent from any error to the 2nd qubit. This is an assumption useful and in many cases realistic but not the most general