Quantum Computing: Foundations to Frontier Fall 2018

Lecture 10

Lecturer: Henry Yuen *Scribes: Sumner Alperin, Maihao Guo*

1 Overview

In this lecture we discussed schemes for correcting errors which are liable to arise in real quantum circuits. We began from a discussion of classical error correcting methods, and their super-cession by the invention of the transistor, before moving on to the case of quantum errors. In particular, we examined routines which allow for the undoing of bit-flip and phase-flip errors, and showed that, given the ability to undo single qubit bit-flip and phase-flip errors, all single qubit unitary errors can be protected against as well. Finally, we introduced Shor's encoding, the scheme which allows for simultaneous protection against bit-flips and phase-flips, and introduced the quantum fault tolerance threshold theorem.

2 Classical Errors

In the early days of computing, computers used vacuum tubes to encode logical information and perform logic. These vacuum tubes were prone to error, noise and failure, are physically large, and required heating, cooling, and a large amount of power to operate. The error that the unavoidable failure of these devices produced lead many to believe that there was an upper limit to the size of computers and by extension, the size of the computations they could reasonably perform.

This prevailing attitude garnered the ire of John Von Neumann. In 1947, he published a paper entitled "Probabilistic Logics an the Synthesis of Reliable Organisms from Unreliable Components", in which he showed that, using $O_p(n \log n)$ gates, error could be sufficiently mitigated through redundancy. By embedding several copies of a computation, C, in a circuit C' which checks C for errors (and, by extrapolation, embedding copies of C' in C''), the effective error rate of the system could be reduced to tolerable levels.

Though this result is ingenious, shortly after its publication it was rendered unnecessary by the invention of the transistor, the primary component of all computers today. Error rates for transistors are several orders of magnitude lower than those of vacuum tubes, and several billion transistors may be placed inside, say, the chassis of a cell phone – and because error rates are so low, much of the logic performed by these transistors can be done without error correction. Nevertheless, basic classical error correcting methods serve to motivate our foundational models for quantum error correction.

3 Error Correction in a Classical Channel

The primary relevance of error correction to classical computing is actually in channels for the communication of logical information between the channels.

Suppose that Alice desires to send Bob a single logical bit, $b \in \{0, 1\}$ over a noisy channel, which with probability p flips b to 1 if $b = 0$, and to 0 if $b = 1$. Thus, with probability $1 - p$, Alice sends her intended bit, but with probability p, sends the opposite bit instead.

The simplest error correcting code (ECC) for dealing with such noise is the repetition code (RC). Instead of sending the single "logical" bit b, Alice sends Bob three copies thereof, sending him the "physical" bits bbb. Bob then concludes that the bit Alice meant to send is whichever bit occurs in the majority of cases in bbb. Thus, if only one error occurs, Bob will be able to deduce the bit Alice intended to send, in spite of the error.

3.1 Proof of the Validity of RC

Suppose bit errors happen with probability p. Decoding errors will occur only if two or three bit flips occur. This occurs with likelihood:

$$\binom{3}{2} p^2(1-p) + p^3 \tag{1}$$

The error rate is reduced if:

$$\binom{3}{2} p^2(1-p) + p^3 < p \tag{2}$$

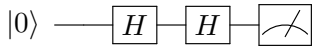
$$3p - 2p^2 < 1 \tag{3}$$

$$p < \frac{1}{2} \tag{4}$$

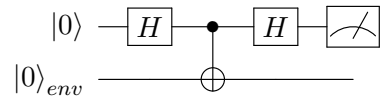
Thus, for sufficiently low p, the RC reduces the effective error rate. Higher numbers of physical bits further increase the ability to reduce error.

4 Quantum Errors

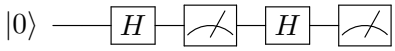
We turn now to examine quantum errors. The simplest way to conceive of error is as the unintentional application of a unitary gate, possibly as a controlled interaction with some qubit(s) representing the environment. Thus, the idealized quantum circuit



may, due to environmental interaction, be transformed into



which, as we have seen, is equivalent to the circuit



Such interactions are called decoherence, because they collapse the quantum mechanical superpositions and entanglements within a circuit ahead of the desired time of measurement.

5 Quantum Error Correction

At first, it seems tempting to simply use the RC to transmit quantum mechanical information over erroneous channels. However, this would be in violation of the no cloning theorem; we cannot make 3 copies of the arbitrary qubit $|\psi\rangle$. Additionally, at first glance, it would seem that error verification may require measuring – which causes the decoherence we meant to prevent. Furthermore, where as in classical channels only bit flip errors were possible, there are infinitely many unitaries which may act upon even a single qubit – and thus, seemingly, an infinite number of possible types of errors which must be protected against.

5.1 Key Error Types

As we shall show, it is in fact sufficient to protect against only two types of errors.

The first are bit flip errors, represented by the Pauli X matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which maps $|0\rangle$ to $|1\rangle$ and vice versa.

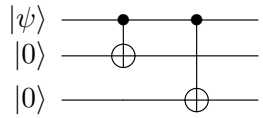
The second are phase flip errors, which we represent by the Pauli Z matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, which leaves $|0\rangle$ unaffected but maps $|1\rangle$ to $-|1\rangle$. It is also valuable to think of the phase flip as a bit flip in the $|+\rangle$,$|-\rangle$ basis, as it maps said qubits to eachother, just as the Pauli X matrix does to $|0\rangle$ and $|1\rangle$.

5.2 Quantum Bit Flip Code

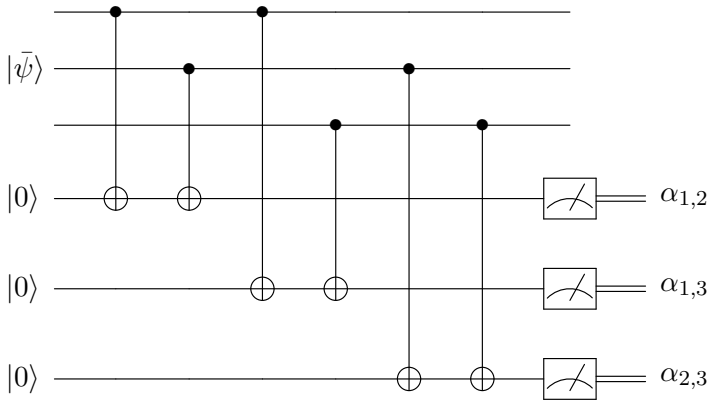
We now devise a quantum error correcting code that protects against bit flip errors. We simply use the classical repetition code: the qubit state $|0\rangle$ is mapped to the 3-qubit state $|000\rangle$ and the state $|1\rangle$ is mapped to $|111\rangle$. This does not violate the no-cloning theorem because we are only copying classical basis states.

Let $|\bar{0}\rangle$ represent the "physical" qubits $|000\rangle$, and let $|\bar{1}\rangle$ similarly represent $|111\rangle$. Then, if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, let $|\bar{\psi}\rangle$ be $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle = \alpha|000\rangle + \beta|111\rangle$.

We can achieve this encoding via the following circuit:

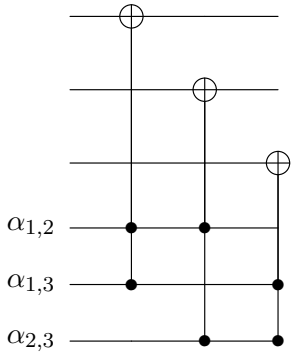


Suppose a bit flip error X acting on the second qubit, $X_2|\bar{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle$. We don't want to measure this qubit to detect the error; instead, we want to apply a unitary operation for error detection. We achieve this as follows:



The measurement outcomes $\alpha_{i,j} \in \{0, 1\}$ are called the syndrome of the circuit. The bit $\alpha_{i,j}$ records the parity of the i'th and j'th qubits. If the qubits are equal (with respect to the standard basis), then $\alpha_{i,j} = 0$. Otherwise, it will be $\alpha_{i,j} = 1$.

In the case of a single bit flip, two of the $\alpha_{i,j}$ will be 1. In the example we gave, $X_2|\bar{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle$, so $\alpha_{1,2}$ and $\alpha_{2,3}$ will both yield 1 after measurement. This would indicate that the shared control qubit of $\alpha_{1,2}$ and $\alpha_{2,3}$ has been affected by a bit flip error, which we can then undo by the following Correction circuit:



The two qubits indicated by the black dots have to be set to 1 in order for the target qubit to be flipped.

As an example, consider a bit flip error X_3 acting on the third qubit of $|\bar{\psi}\rangle$:

$X_3|\bar{\psi}\rangle = \alpha|001\rangle + \beta|110\rangle$

$\downarrow$ detection

$\alpha|001\rangle|011\rangle + \beta|110\rangle|011\rangle$

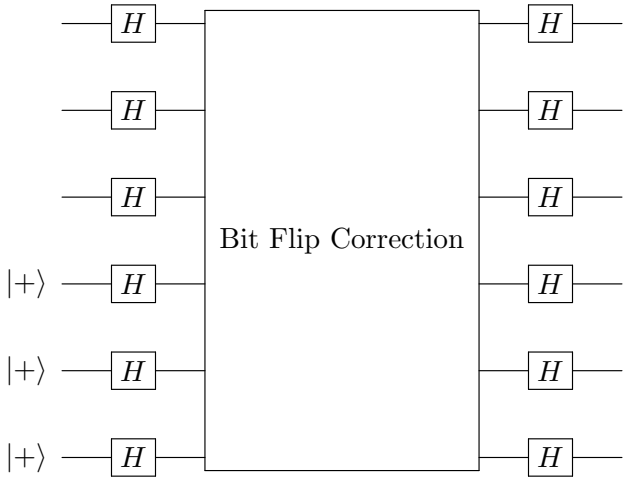
$\downarrow$ correction

$(\alpha|000\rangle + \beta|111\rangle)|011\rangle$

5.3 Phase Flip Errors

If a phase flip error occurs and we use the bit flip code from above: $|\bar{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle$, notice that $Z_1|\bar{\psi}\rangle = Z_2|\bar{\psi}\rangle = Z_3|\bar{\psi}\rangle = \alpha|000\rangle - \beta|111\rangle$, so we cannot detect which one is the erroneous qubit using the bit flip code. Therefore, we need another way of protecting against phase flip errors. Observe that phase flip errors are simply bit flip errors in the $\{|+\rangle, |-\rangle\}$ basis, where $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we encode $|\bar{\psi}\rangle$ to be $\alpha|+\rangle|+\rangle|+\rangle + \beta|-\rangle|-\rangle|-\rangle$. Suppose a phase flip error Z acting on the third qubit, $Z_3|\bar{\psi}\rangle = \alpha|+\rangle|+\rangle|-\rangle + \beta|-\rangle|-\rangle|+\rangle$. We can achieve this encoding by applying Hadamard gates to every qubit, apply bit flip correction, then apply Hadamard gates at the end:



5.4 The 9-qubit Shor code

In order to put these two codes together into a single one, Peter Shor came up with a 9-qubit Shor code, that can correct both bit flips and phase flip errors, so long as they occur on a single qubit. We will then see that this implies that the Shor code can correct arbitrary single-qubit errors. The Shor code is an example of a quantum error correcting code (QECC).

5.4.1 Encoding

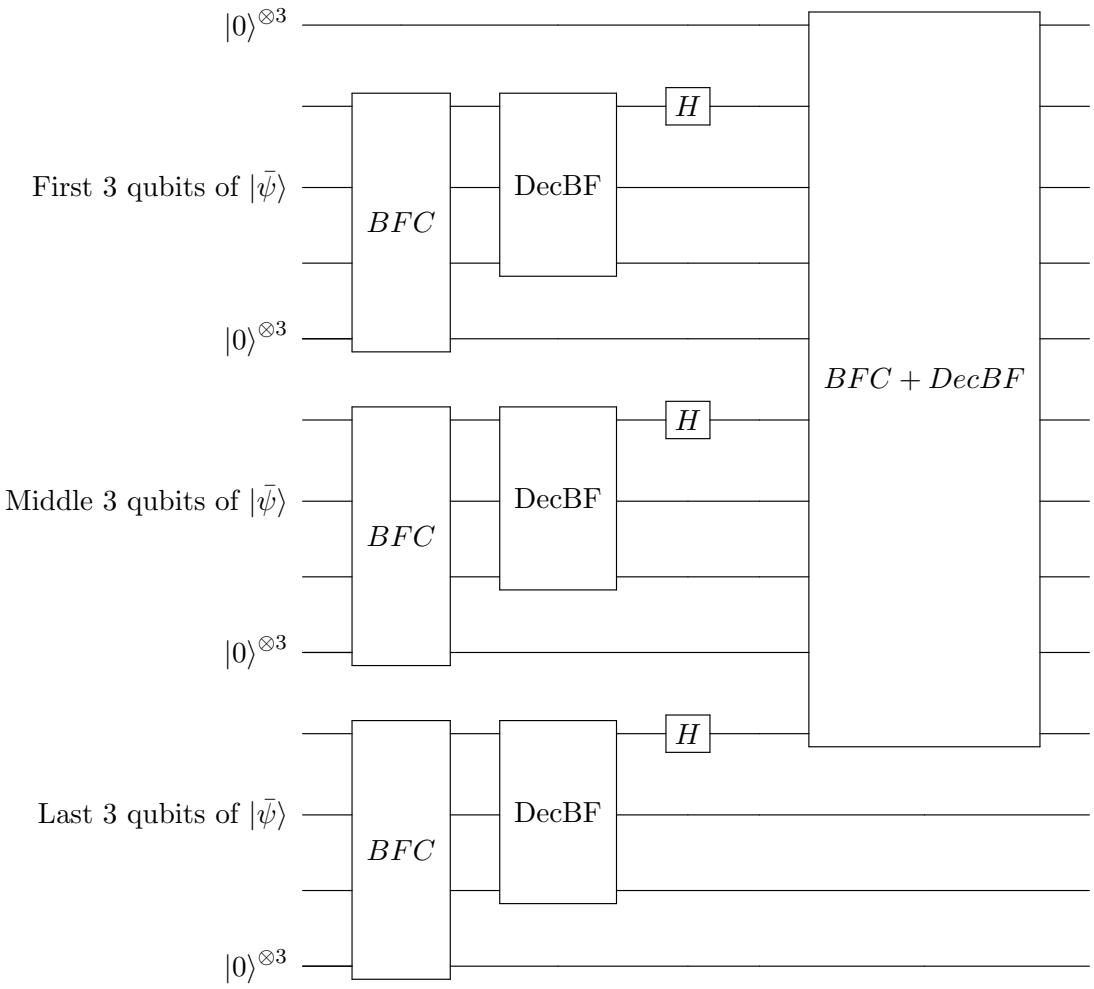
$|0\rangle \to |\bar{0}\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$

$|1\rangle \to |\bar{1}\rangle = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then we have $|\bar{\psi}\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$.

5.4.2 Detecting and Correcting errors

We detect and correct errors for the Shor code in stages. First, we apply the bit flip correction two each group of three qubits, and then decode. This next circuit will do most of the error correction.



In the circuit above, "BFC" denotes Bit Flip Corrector for 3 qubits, described in Section 5.2. The first three BFC gates are applied to consecutive groups of three qubits. The last BFC and DecBF gate is applied to the second, sixth, and tenth wires shown in the circuit.

"DecBF" denotes the map $|000\rangle \mapsto |000\rangle$, and $|111\rangle \mapsto |100\rangle$. Thus this maps $\alpha|000\rangle + \beta|111\rangle$ to $(\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle$.

What does this (partial) circuit do? Let's walk through an example. Suppose we have a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ that we encode using the Shor code, to get codeword $|\bar{\psi}\rangle$. Then, suppose there is a bit flip error acting on the seventh qubit:

$$X_7|\bar{\psi}\rangle = \frac{\alpha}{\sqrt{8}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|100\rangle + |011\rangle) + \frac{\beta}{\sqrt{8}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|100\rangle - |011\rangle).$$

After the BFC operations are applied on each triple of qubits, we get the state $|\bar{\psi}\rangle$ (with whatever the ancilla qubits are). When we apply the operation DecBF followed by the Hadamard gate, the state of the second, sixth and tenth qubits is

$$\frac{\alpha}{\sqrt{8}}|000\rangle + \frac{\beta}{\sqrt{8}}|111\rangle \tag{5}$$

which notice is a codeword in the quantum bit flip code. When we apply the final BFC gate, nothing happens, and if we decode, we get the qubit $|\psi\rangle$.

What if there was a phase flip error? Let's imagine that there was a phase error on the fourth qubit of our codeword $|\bar{\psi}\rangle$. After running the circuit above, we would have, in the second, sixth and tenth qubits the state

$$\frac{\alpha}{\sqrt{8}}|010\rangle + \frac{\beta}{\sqrt{8}}|101\rangle$$

But note that we can apply the BFC operation on these to get (5). From this we can then decode to get $|\psi\rangle$.

Observation Using the same reasoning as above, the Shor code can detect and correct a ZX error on the same qubit. Try $Z_5X_5|\bar{\psi}\rangle$ as an exercise.

We can conclude that Shor code can detect and correct single bit flips and phase flips. What's more, it implies that Shor code can detect and correct **any** single qubit error:

Fact For all single qubit operators P, we can write P as a linear combination of the identity matrix I, the X matrix, the Z matrix, and the ZX matrix: there exists $a, b, c, d \in \mathbb{C}$ such that $P = aI + bX + cZ + dZX$.

Thus for any single-qubit error P, we have

$$P|\bar{\psi}\rangle = a|\bar{\psi}\rangle + bX|\bar{\psi}\rangle + cZ|\bar{\psi}\rangle + dZX|\bar{\psi}\rangle \tag{6}$$

If we apply the error correction circuit C above, we get

$$\begin{aligned} C(P|\bar{\psi}\rangle)(|0\rangle^{\otimes 12}) &= aC|\psi\rangle|0\rangle + bCX|\psi\rangle|0\rangle + cCZ|\psi\rangle|0\rangle + dCZX|\psi\rangle|0\rangle & (7)\\ &= a|\psi\rangle|0\rangle + b|\psi\rangle|e_X\rangle + c|\psi\rangle|e_Z\rangle + d|\psi\rangle|e_{ZX}\rangle & (8)\\ &= |\psi\rangle \otimes (a|0\rangle + b|e_X\rangle + c|e_Z\rangle + d|e_{ZX}\rangle) & (9) \end{aligned}$$

where e_X, e_Z, e_{ZX} denote some states transformed from ancilla states by circuit C. After applying C, we obtain the correct state $|\psi\rangle$ and the residual qubits $(a|0\rangle + b|e_X\rangle + c|e_Z\rangle + d|e_{ZX}\rangle)$ can be discarded.

Similarly to the classical case, there are many types of quantum error correcting codes that people have come up with–for example, they can handle more errors than a single qubit.

6 Quantum Fault Tolerance

We have lots of cool QECCs, but they don't immediately allow us to protect quantum computations from error. This is because the encoding/decoding operations themselves are also erroneous. In our analysis of the Shor code, we assumed the syndrome measurements and recovery circuits were performed perfectly.

It takes quite a bit more work but people have shown that it is indeed possible to make quantum computations fault tolerant, in an analogous way to von Neumann's proof that classical computation can be carried out in the presence of noise.

This culminated in the Quantum Fault Tolerance Threshold Theorem [Aharonov&Ben-Or, Zurek et al.]:

There exists ($\exists$) a universal constant $p \geq 10^{-6}$, s.t. for all ($\forall$) circuit C on n qubits and of size $poly(n)$, there exists ($\exists$) a circuit C' on $poly(n)$ qubits and of size $poly(n)$, s.t. even if each qubit and gates of C' fails independently with probility p, the result of the ideal computation C can be recovered from C' with high probability.

The Fault-Tolerance Theorem is the justification for all the experimental efforts in quantum computing. It says that noise is not a fundamental obstacle to large scale quantum computing.

As long as we can get to $p \leq p_{threshold}$, then it's off to the races.There is significant focus to determin how large $p_{threshold}$ can be. We are currently far away from achieving low enough noise, but experimental groups are making steady progress.

7 Frontier

1. *Making physical qubits more reliable* – Experimental groups have achieved $p < 0.001$ for one or two qubits in isolation. However, putting many qubits together drives up error for everyone, so they're trying to figure out how to keep it low.
2. *Better error correcting codes and fault tolerance schemes* – The current best schemes require thousands of physical qubits per logical qubit. It would be better to lower this.

References

[1] P. Shor *Fault-Tolerant Quantum Computation*, Quantum Physics quant-ph/9605011, 1996.

[2] D. Aharonov, M. Ben-Or, *Fault-Tolerant Quantum Computation with Constant Error Rate*, Quantum Physics quant-ph/9611025, 1996.

[3] E. Knill, R. Laflamme, W. Zurek, *Resilient quantum computation: error models and thresholds*, Quantum Physics quant-ph/9702058, 1997.