Topics in Quantum Information **U. Waterloo CO 781, Fall 2006**
Debbie Leung and Ashwin Nayak (Instructors) **Gus Gutoski (Scribe) (Edited by DL)**
Fault Tolerance and Threshold Theorem **October 11, 2006**

1 Fault Tolerance (FT) and Threshold Theorem (TT)

This section makes no use of quantum formalism—it is entirely classical in nature. We may talk of "quantum gates" and "quantum circuits", but everything said in this lecture applies equally well to classical circuits and gates.

Definition 1 (Quantum Error Correcting Code (QECC)) *An n-qubit* quantum error correcting code (QECC) *is a subspace of a 2^n-dimensional Hilbert space with the property that any error on no more than t qubits can be reversed (at least in an idealized information theoretic sense).*

The following table compares assumptions on the noise model and the reliability of quantum operations for each of several applications of QECC.

Application	**Assumptions on Noise Model**	**Assumptions on Encode/Decode Operations**
Quantum Key Distribution (QKD)	any error on t or fewer qubits	can deal with some imperfections
Quantum Secret Sharing	any error on t or fewer qubits	perfect
Noisy Quantum Channel Coding	i.i.d. errors on each qubit	perfect
Fault-Tolerant Quantum Computation Threshold Theorem	ranges from i.i.d. to more general noise	only require low probability of error in each gate

1.1 Overview

The goal of fault-tolerant quantum computation (FTQC) is to use noisy components to reliably implement quantum circuits of arbitrary size to any desired accuracy ε.

More specifically, suppose that p is the error rate of our quantum gates and suppose that we wish to implement a given quantum circuit with precision ε. Is it necessary that $p \to 0$ as $\varepsilon \to 0$? If so then we are in trouble because it seems unlikely that quantum gates can ever be constructed with arbitrarily small error rates.

Alternatively, is it the case that there exists some universal constant $p_{\mathrm{th}} > 0$ such that if $p < p_{\mathrm{th}}$ then the error rate p is "good enough" to achieve arbitrary accuracy? This latter case is far more desirable—if true, it would offer hope that arbitrarily accurate quantum computations can be performed even with faulty quantum gates. The following theorem asserts that indeed this is the case.

Theorem 2 (Threshold Theorem (TT)) *There exists a universal constant $p_{\mathrm{th}} > 0$ such that, if quantum gates can be implemented with error rate $p < p_{\mathrm{th}}$ then for any quantum circuit C and any accuracy parameter $\varepsilon > 0$ we have that C can be implemented with accuracy ε using quantum gates with error rate p.*

At the time of this writing, the quantity p_{th} is known to be at least 1.94×10^{-4}.

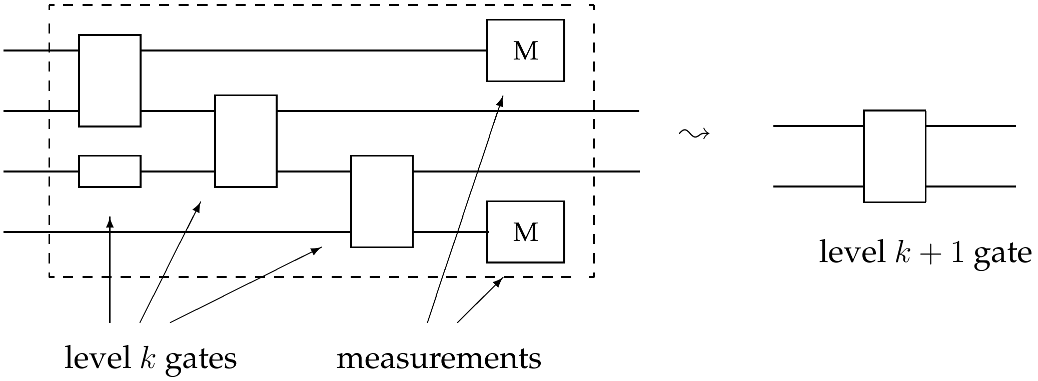

Figure 1: Gates in each level are constructed using gates from lower levels

1.2 The Concatenation Approach to Fault-Tolerance and "Level-Reduction"

One approach to implementing fault-tolerant quantum computation under active research is the "level reduction method" described as follows. Essentially, each level consists of implementations of quantum gates in some universal set such that the error of the implementations decreases rapidly with the level number.

More explicitly, suppose that we can implement our universal set of quantum gates with an error rate p. Then level 0 is defined to be this set of universal gates and we say that the *error* of level 0 is p. In order to construct level 1, we simulate each gate in our universal set using only gates from level 0 such that each simulated gate has error at most $\mathcal{O}(p^t)$ for some $t > 1$. Similarly, the universal set of gates at level k has error $\mathcal{O}(p^{t^k})$ and we construct level $k+1$ by simulating each gate in our universal set using only gates from level k such that the simulated gates in level $k+1$ have error $\mathcal{O}(p^{t^{k+1}})$.

Of course, it is impossible to achieve such simulations without using some form of quantum error correcting code. Such a code will typically encode one *logical* qubit or gate into several *physical* qubits or gates. Each level treats the gates in lower levels as physical (or *primitive*) gates in the sense that they are used in a "black box" manner, so that each level does not depend upon how gates in lower levels are constructed. See Figure 1.

For greater generality, let us assume that if p is the error of level k then the error of level $k+1$ is cp^t for some constants c and $t > 1$. Let us compute the error p_k of level k:

$$p \overset{\text{level 0}}{\longmapsto} cp^t \overset{\text{level 1}}{\longmapsto} c\left(cp^t\right)^t = c^{1+t}p^{t^2} \overset{\text{level 2}}{\longmapsto} \cdots \overset{\text{level } k}{\longmapsto} c^{1+t+\cdots+t^{k-1}}p^{t^k} = c^{\frac{t^k-1}{t-1}}p^{t^k} \overset{\text{def}}{=} p_k.$$

If this fault-tolerance scheme is to be of any help then we certainly require that the error improve at each level. In other words, we require that our base error rate p satisfy

$$p > cp^t.$$

We can compute an upper bound p_{th} for all such p in terms of c and t by solving

$$p_{\text{th}} = cp_{\text{th}}^t.$$

The solution to this equation is

$$p_{\text{th}} = c^{-\frac{1}{t-1}}.$$

Substituting this solution back into our expression for p_k yields

$$p_k = c^{\frac{t^k-1}{t-1}}p^{t^k} = p_{\text{th}}\left(c^{\frac{1}{t-1}}p\right)^{t^k} = p_{\text{th}}\left(\frac{p}{p_{\text{th}}}\right)^{t^k}.$$

In other words, the error p_k at level k drops doubly exponentially in the number of levels k. This result may seem encouraging, and indeed it is. But by the same token, it is easily seen that the amount of resources required to implement each successive level increases exponentially with the number of levels k.

More specifically, suppose that a quantum circuit C is composed of $\mathrm{size}(C)$ quantum gates. Suppose further that each gate in level k is sumulated with at most N gates from level $k-1$ for each k. Then we have

$$\mathrm{size}(C) \overset{\text{level 0}}{\longmapsto} N\,\mathrm{size}(C) \overset{\text{level 1}}{\longmapsto} N^2\,\mathrm{size}(C) \overset{\text{level 2}}{\longmapsto} \cdots \overset{\text{level } k}{\longmapsto} N^{k-1}\,\mathrm{size}(C),$$

which grows only singly exponentially in k.

If C is to be implemented with accuracy ε then we must implement each gate in C with accuracy at least $\varepsilon/\,\mathrm{size}(C)$, since error is additive. Hence, under the level method it suffices to implement enough levels k so that each gate in the kth level has error

$$p_k < \frac{\varepsilon}{\mathrm{size}(C)}.$$

That is,

$$p_k = p_{\mathrm{th}} \left(\frac{p}{p_{\mathrm{th}}}\right)^{t^k} < \frac{\varepsilon}{\mathrm{size}(C)} \implies t^k < \frac{\log\left(\frac{\varepsilon}{\mathrm{size}(C)p_{\mathrm{th}}}\right)}{\log\left(\frac{p}{p_{\mathrm{th}}}\right)} = \frac{\log\left(\frac{\mathrm{size}(C)p_{\mathrm{th}}}{\varepsilon}\right)}{\log\left(\frac{p_{\mathrm{th}}}{p}\right)}.$$

This expression may be used to bound the number of gates appearing in the level k simulation:

$$N^k\,\mathrm{size}(C) < \left(\frac{\log\left(\frac{\mathrm{size}(C)p_{\mathrm{th}}}{\varepsilon}\right)}{\log\left(\frac{p_{\mathrm{th}}}{p}\right)}\right)^{\frac{\log N}{\log t}} \mathrm{size}(C) = \text{poly}\log\left(\mathrm{size}(C), \log\left(\frac{1}{\varepsilon}\right)\right)$$

where the final equality serves only to highlight the relevant fact—that the number of gates used in the level k simulation of C requires no more than a number of gates that is polynomial in $\mathrm{size}(C)$ and $\log\left(\frac{1}{\varepsilon}\right)$. The fact that this scaling factor is only polynomial (as opposed to exponential or higher) tells us that fault-tolerance can be implemented efficiently, provided that the original error p is smaller than p_{th}.

2 Lecture Plan

During the next two lectures we will discuss the following:

- Proof sketch for the Threshold Theorem (apparently we just did that in Section 1).
- Universal set of quantum gates that is suitable for fault-tolerant quantum computation.
- Assumptions.
- Fault-tolerant implementations.

3 Universal Set of Quantum Gates

Any computation consists of:

1. State preparation (e.g. $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, bell states, etc.)
2. Universal set of quantum gates
3. Measurements (e.g. in $\{|0\rangle, |1\rangle\}$ basis or in $\{|+\rangle, |-\rangle\}$ basis)

Items 1 and 3 are fairly straightforward. It should be noted, however, that it only makes sense to assume that we can prepare and measure states that can actually be prepared and measured relatively easily in the lab. It is generally accepted that the states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ have this property.

Let us discuss item 2. A set S of quantum gates is called *universal* if each gate in S acts upon no more than k qubits for some fixed k and if any unitary operation on any number of qubits can be approximated arbitrarily closely using only gates from S.

Universal sets, even finite universal sets, are known to exist. For example, the set $\{\mathrm{CNOT}, H, P, \mathrm{Toffoli}\}$ is universal, where

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad \mathrm{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Another universal set of gates is $\left\{\mathrm{CNOT}, H, \sqrt{P}\right\}$.