Quantum Error Correction I

Bei Zeng

University of Guelph

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Why Error Correction?

The Power of quantum computing:

$$U_f: |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$$

therefore

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

Coherence – quantum parallelism!

Decoherence! $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \rightarrow |0\rangle$ or $|1\rangle$.

Schrodingers cat Coherence is ok for a few atoms or photons in lab when the coupling to environment is weak enough. For a system as big as a cat, comprised of billions upon billions of atoms, decoherence happens almost instantaneously, so that the cat can never be both alive and dead for any measurable instant.

Why Error Correction?

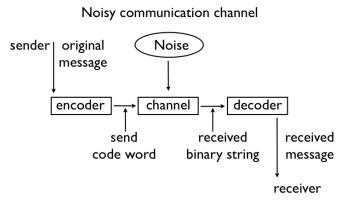
Reading: by Serge Haroche and Jean-Michel Raimond, Physics Today, 51, August 1996 Peter Shor: There is no real hard problem in the world...We are simply not smart enough...

	Analog Computer	Quantum Computer
Input	$ec{x}(0)$	$ \psi angle$
Computing	$\frac{d\vec{x}}{dt} = f(\vec{x})$	$irac{\partial}{\partial t} \psi angle = \mathcal{H} \psi angle$
Output	$\vec{x}(T)$	measurement

Analog Computers are Continuous, Unreliable. They have been replaced by digital computers for almost all uses. Can we build a DIGITAL quantum computer?

ション ふゆ マ キャット しょう くしゃ

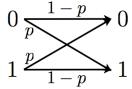
Basic ideas for Error Correction



◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Classical Error Correction

Digital Communication.



Binary Symmetric Channel. The Repetition Code:

$$0 \to 000, \quad 1 \to 111.$$

Decoding: Majority Voting.

Probability of Two flips: $3p^2(1-p) + p^3$, therefore probability of error: $p_e = 3p^2 - 2p^3$. $p_e < p$ if $p < \frac{1}{2}$.

Classical Error Correction

In Classical World... Digital computer with error correction:

 $0 \rightarrow 000, \quad 1 \rightarrow 111.$

Errors $0 \leftrightarrow 1$, discrete.

But in Quantum World...

♦ Continuous errors:

 $|0\rangle \rightarrow U|0\rangle, \ |1\rangle \rightarrow U|1\rangle$

 \diamond Measurement destroys coherence!

 $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$

♦ No-cloning theorem!

 $|\psi\rangle|\psi\rangle\neq\alpha|0\rangle|0\rangle+\beta|1\rangle|1\rangle$

ション ふゆ マ キャット しょう くしゃ

Still hopeless?

Starting from a Simple Case

Binary Symmetric Channel: $0 \leftrightarrow 1$. Quantum Bit flip Channel: $|0\rangle \leftrightarrow |1\rangle$. $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ The Repetition Code:

$$0 \rightarrow 000, \quad 1 \rightarrow 111.$$

The Quantum Bit Flip Code:

$$\begin{aligned} |0\rangle &\to |000\rangle \equiv |0_L\rangle, \quad |1\rangle \to |111\rangle \equiv |1_L\rangle \\ |\psi\rangle &= a|0\rangle + b|1\rangle \to a|000\rangle + b|111\rangle \end{aligned}$$

うして ふゆう ふほう ふほう ふしつ

Encoding Circuit:



Quantum Bit Flip Code

$$|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$$

Bit Flip Errors:

$ \psi_0\rangle = a 000\rangle + b 111\rangle$	No Error
$ \psi_1\rangle = a 100\rangle + b 011\rangle$	flip on the 1st qubit
$ \psi_2\rangle = a 010\rangle + b 101\rangle$	flip on the 2nd qubit
$ \psi_3\rangle = a 001\rangle + b 110\rangle$	flip on the 3rd qubit

Syndrome Diagnosis:

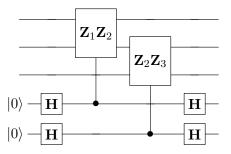
$$\begin{split} P_0 &\equiv |000\rangle\langle 000| + |111\rangle\langle 111| \\ P_1 &\equiv |100\rangle\langle 100| + |011\rangle\langle 011| \\ P_2 &\equiv |010\rangle\langle 010| + |101\rangle\langle 101| \\ P_3 &\equiv |001\rangle\langle 001| + |110\rangle\langle 110| \end{split}$$

No Error flip on the 1st qubit flip on the 2nd qubit flip on the 3rd qubit

Quantum Bit Flip Code

Syndrome Measurements:

	$\mathbf{Z}_1\mathbf{Z}_2$	$\mathbf{Z}_2\mathbf{Z}_3$	Recovery
$ \psi_0\rangle = a 000\rangle + b 111\rangle$	0	0	Ι
$ \psi_1\rangle = a 100\rangle + b 011\rangle$	1	0	\mathbf{X}_1
$ \psi_2\rangle = a 010\rangle + b 101\rangle$	1	1	\mathbf{X}_2
$ \psi_3\rangle = a 001\rangle + b 110\rangle$	0	1	\mathbf{X}_3



・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・
 ・

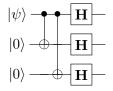
The Phase Flip Code

The Quantum Phase Flip Channel

$$|0\rangle \rightarrow |0\rangle \quad |1\rangle \rightarrow -|1\rangle, \quad \mathbf{Z} = \begin{pmatrix} 1 & 0\\ 0 & -1 \end{pmatrix}$$

Recall the Hadamard Transform $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and $\mathbf{H}\mathbf{X}\mathbf{H} = \mathbf{Z}$, which transforms $|0\rangle \rightarrow |+\rangle$, $|1\rangle \rightarrow |-\rangle$. Therefore we can do the encoding

$$|0\rangle \rightarrow |+++\rangle \equiv |0_L\rangle, \quad |1\rangle \rightarrow |---\rangle \equiv |1_L\rangle$$



▲ロト ▲園ト ▲ヨト ▲ヨト 三臣 - のへの

Combination of Errors

Theorem

If a Quantum Code corrects errors A and B, it also corrects $\alpha A + \beta B$.

Example

For the bit flip channel $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, consider the error $\alpha \mathbf{I_1} + \beta \mathbf{X_1}$. Use the encoding

$$|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$$

the output will be $\alpha |\psi_0\rangle + \beta |\psi_1\rangle$, with

 $|\psi_0\rangle = a|000\rangle + b|111\rangle, \quad |\psi_1\rangle = a|100\rangle + b|011\rangle$

We can still use the syndrome measurements $\mathbf{Z}_1\mathbf{Z}_2$ and $\mathbf{Z}_2\mathbf{Z}_3$. An arbitrary single-qubit error: a linear combination of $\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}$.

Shor Code

Bit Flip:
$$|0\rangle \rightarrow |000\rangle, |1\rangle \rightarrow |111\rangle$$
.
Phase Flip: $|0\rangle \rightarrow |+++\rangle, |1\rangle \rightarrow |---\rangle$.
And

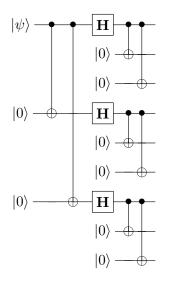
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

To fight against both bit flip and phase flip errors, we do a two step encoding: first encode to a phase flip code, then further encode to a bit flip code, we get the Shor Code

$$\begin{aligned} |0_L\rangle &\rightarrow \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)\\ |1_L\rangle &\rightarrow \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\end{aligned}$$

Shor Code

Encoding circuit:



Syndrome measurements: Bit Flip:

$\mathbf{Z}_{1}\mathbf{Z}_{2},$	$\mathbf{Z}_2\mathbf{Z}_3$
$\mathbf{Z}_{4}\mathbf{Z}_{5},$	$\mathbf{Z}_5\mathbf{Z}_6$
$\mathbf{Z}_{7}\mathbf{Z}_{8},$	$\mathbf{Z}_7\mathbf{Z}_9$

Phase Flip:

 $\begin{array}{l} \mathbf{X}_1\mathbf{X}_2\mathbf{X}_3\mathbf{X}_4\mathbf{X}_5\mathbf{X}_6 \\ \mathbf{X}_4\mathbf{X}_5\mathbf{X}_6\mathbf{X}_7\mathbf{X}_8\mathbf{X}_9 \end{array}$

Recovery: \mathbf{Z}_i for phase flip, \mathbf{X}_i for bit flip. Commuting Pauli Operators

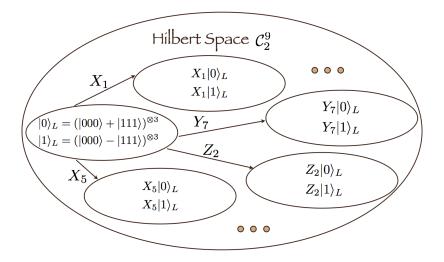
$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The commutation relations:

$\mathbf{X}\mathbf{Y} = -\mathbf{Y}\mathbf{X}, \ \mathbf{X}\mathbf{Z} = -\mathbf{Z}\mathbf{X}, \ \mathbf{Y}\mathbf{Z} = -\mathbf{Z}\mathbf{Y}$											
Shor Code:	\mathbf{Z}	\mathbf{Z}	Ι	Ι	Ι	Ι	Ι	Ι	Ι		
	Ι	\mathbf{Z}	\mathbf{Z}	Ι	Ι	Ι	Ι	Ι	Ι		
	Ι	Ι	Ι	\mathbf{Z}	\mathbf{Z}	Ι	Ι	Ι	Ι		
	Ι	Ι	Ι	Ι	\mathbf{Z}	\mathbf{Z}	Ι	Ι	Ι		
	Ι	Ι	Ι	Ι	Ι	Ι	\mathbf{Z}	\mathbf{Z}	Ι		
	Ι	Ι	Ι	Ι	Ι	Ι	Ι	\mathbf{Z}	\mathbf{Z}		
	\mathbf{X}	\mathbf{X}	\mathbf{X}	\mathbf{X}	\mathbf{X}	\mathbf{X}	Ι	Ι	Ι		
	Ι	Ι	Ι	\mathbf{X}	\mathbf{X}	\mathbf{X}	\mathbf{X}	\mathbf{X}	\mathbf{X}		

 $|0_L\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$ $|1_L\rangle \rightarrow \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$

A Picture of Shor's code



▲□▶ ▲圖▶ ▲臣▶ ▲臣▶ 三臣 - のへで

Quantum Error Correcting Criterion

Quantum Code: A subspace of $\mathbb{C}_2^{\otimes n}$

Code space basis $\{|\psi_i\rangle\}$

Errors: $\{\mathbf{E}_{\alpha}\}$

Quantum Error Correcting Criterion:

$$\langle \psi_i | \mathbf{E}_{\alpha}^{\dagger} \mathbf{E}_{\beta} | \psi_j \rangle = c_{\alpha\beta} \delta_{ij}$$

うして ふゆう ふほう ふほう ふしつ

 \diamond Orthogonal Condition: $\mathbf{E}_{\alpha}|\psi_i\rangle \perp \mathbf{E}_{\beta}|\psi_j\rangle$.

Classical: $i \neq j$.

 \diamond Coherence Condition: $\langle \psi_i | \mathbf{E}_{\alpha}^{\dagger} \mathbf{E}_{\beta} | \psi_i \rangle = c_{\alpha\beta}.$

Quantum: i = j.

Hamming Code

Recall that the Repetition Code, with encoding

 $0 \rightarrow 000, 1 \rightarrow 111$, we write the Code Parameters for this code as [3, 1].

This code corrects t = 1 error. Define the Code Distance

d = 2t + 1. We write it as [3, 1, 3].

In general, for an [n, k, d] code, we would want n small, k large and d large. But there are certainly trade-offs.

Let us first fix d = 3, and want a large rate k/n. We will show the construction of the [7, 4, 3] Hamming Code.

We start from the following encoding to make a Linear Code

1000	\rightarrow	1000110
0100	\rightarrow	0100101
0010	\rightarrow	0010011
0001	\rightarrow	0001111

Hamming Code

We can write a Generator Matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

then the encoding becomes

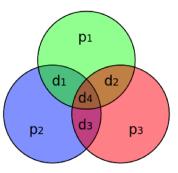
$$\mathbf{x} = \mathbf{a}\mathbf{G}$$

where

$$\mathbf{a} = a_3 a_2 a_1 a_0,$$

and

 $\mathbf{x} = x_6 x_5 x_4 x_3 x_2 x_1 x_0$ $d_1 d_2 d_3 d_4 p_1 p_2 p_3$



Syndrome: p_1, p_2, p_3 .

Quantum 7-bit Code

Hamming code Write its even subcode $\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \mathbf{G}_{\mathbf{e}} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

We now build a quantum 7-bit code via the encoding

$$|0\rangle \rightarrow |0\rangle_L = \frac{1}{2\sqrt{2}} \sum_{\mathbf{x} \in \mathbf{G}_e} |\mathbf{x}\rangle$$

 $= |0000000\rangle + |1100011\rangle + |0110110\rangle + |0001111\rangle$

 $+ |1010101\rangle + |1101100\rangle + |0111001\rangle + |1011010\rangle$

$$|1\rangle \rightarrow |1\rangle_L = \frac{1}{2\sqrt{2}} \sum_{\mathbf{x} \in \mathbf{G} \setminus \mathbf{G}_{\mathbf{e}}} |\mathbf{x}\rangle$$

- $= |1111111\rangle + |0011100\rangle + |1001001\rangle + |1110000\rangle$
- $+ |0101010\rangle + |0010011\rangle + |1000110\rangle + |0100101\rangle$

Syndrome Measurements

For

Let

$$\mathbf{G}_{\mathbf{e}} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad \begin{array}{cccc} \mathbf{M}_1 & = & \mathbf{X}_1 \mathbf{X}_2 \mathbf{X}_6 \mathbf{X}_7 \\ \mathbf{M}_2 & = & \mathbf{X}_2 \mathbf{X}_3 \mathbf{X}_5 \mathbf{X}_6 \\ \mathbf{M}_3 & = & \mathbf{X}_4 \mathbf{X}_5 \mathbf{X}_6 \mathbf{X}_7 \end{array}$$

Then we can write

$$\begin{aligned} |0_L\rangle &= \frac{1}{2\sqrt{2}} \sum_{\mathbf{x} \in \mathbf{G}_{\mathbf{e}}} |\mathbf{x}\rangle = (\mathbf{I} + \mathbf{M}_1)(\mathbf{I} + \mathbf{M}_2)(\mathbf{I} + \mathbf{M}_3)|0\rangle_7 \\ |1_L\rangle &= \frac{1}{2\sqrt{2}} \sum_{\mathbf{x} \in \mathbf{G} \setminus \mathbf{G}_{\mathbf{e}}} |\mathbf{x}\rangle = (\mathbf{I} + \mathbf{M}_1)(\mathbf{I} + \mathbf{M}_2)(\mathbf{I} + \mathbf{M}_3)\mathbf{X}_L|0\rangle_7 \end{aligned}$$

where

$$\mathbf{X}_L = \mathbf{X}_1 \mathbf{X}_2 \mathbf{X}_3 \mathbf{X}_4 \mathbf{X}_5 \mathbf{X}_6 \mathbf{X}_7$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

Phase flip syndromes: $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$.

Syndrome Measurements

Then for

$$\begin{aligned} |0_L\rangle &= (\mathbf{I} + \mathbf{M}_1)(\mathbf{I} + \mathbf{M}_2)(\mathbf{I} + \mathbf{M}_3)|0\rangle_7\\ |1_L\rangle &= (\mathbf{I} + \mathbf{M}_1)(\mathbf{I} + \mathbf{M}_2)(\mathbf{I} + \mathbf{M}_3)\mathbf{X}_L|0\rangle_7 \end{aligned}$$

Bit flip syndromes: N_1, N_2, N_3 . Logic Operations: (Fault-Tolerance)

 $\begin{aligned} \mathbf{X}_{L} &= \mathbf{X}_{1}\mathbf{X}_{2}\mathbf{X}_{3}\mathbf{X}_{4}\mathbf{X}_{5}\mathbf{X}_{6}\mathbf{X}_{7} \\ \mathbf{Z}_{L} &= \mathbf{Z}_{1}\mathbf{Z}_{2}\mathbf{Z}_{3}\mathbf{Z}_{4}\mathbf{Z}_{5}\mathbf{Z}_{6}\mathbf{Z}_{7} \\ \mathbf{H}_{L} &= \mathbf{H}_{1}\mathbf{H}_{2}\mathbf{H}_{3}\mathbf{H}_{4}\mathbf{H}_{5}\mathbf{H}_{6}\mathbf{H}_{7} \\ \mathbf{CNOT}_{L} &= \mathbf{C}_{1,8}\mathbf{C}_{2,9}\mathbf{C}_{3,10}\mathbf{C}_{4,11}\mathbf{C}_{5,12}\mathbf{C}_{6,13}\mathbf{C}_{7,14} \end{aligned}$

・ロト ・ 同ト ・ ヨト ・ ヨト ・ りゃぐ

Five Qubit Code

For the parameters [5, 1, 3], we have a perfect code because $(1 + (3 \times 5)) \times 2 = 2^5$. Let

we do the encoding

$$|0_L\rangle = \frac{1}{4}(\mathbf{I} + \mathbf{M}_1)(\mathbf{I} + \mathbf{M}_2)(\mathbf{I} + \mathbf{M}_3)(\mathbf{I} + \mathbf{M}_4)|0\rangle_5$$

$$|1_L\rangle = \frac{1}{4}(\mathbf{I} + \mathbf{M}_1)(\mathbf{I} + \mathbf{M}_2)(\mathbf{I} + \mathbf{M}_3)(\mathbf{I} + \mathbf{M}_4)\mathbf{X}_L|0\rangle_5$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 - のへで

Note that $\mathbf{M}_i^2 = 1$ and $(\mathbf{I} + \mathbf{M}_i)^2 = \mathbf{I} + \mathbf{M}_i$ and $(\mathbf{I} + \mathbf{M}_i)(\mathbf{I} - \mathbf{M}_i) = 0$

so it is straightforward to show that

$$\langle 0_L | 1_L \rangle = 0,$$

and further the quantum error correcting criterion, e.g.

$$\langle 0_L | \mathbf{X}_1 \mathbf{Y}_2 | 1_L \rangle = 0, \ \langle 0_L | \mathbf{X}_1 \mathbf{Y}_2 | 0_L \rangle = 0, \ \langle 1_L | \mathbf{X}_1 \mathbf{Y}_2 | 1_L \rangle = 0$$

Syndrome measurements:

U	Ι	$\mathbf{X}_1 \mathbf{Y}_1 \mathbf{Z}_1$		$\mathbf{X}_2\mathbf{Y}_2\mathbf{Z}_2$		$\mathbf{X}_3\mathbf{Y}_3\mathbf{Z}_3$		$\mathbf{X}_4 \mathbf{Y}_4 \mathbf{Z}_4$			$\mathbf{X}_{5}\mathbf{Y}_{5}\mathbf{Z}_{5}$					
\mathbf{M}_1	0	1	1	0	0	1	1	0	1	1	1	1	0	0	0	0
\mathbf{M}_2	0	0	0	0	1	1	0	0	1	1	0	1	1	1	1	0
\mathbf{M}_3	0	1	1	0	0	0	0	1	1	0	0	1	1	0	1	1
\mathbf{M}_4	0	0	1	1	1	1	0	0	0	0	1	1	0	0	1	1

Threshold Theorem

Threshold Theorem

An arbitrary long quantum computation can be performed reliably, provided that the average probability of error per gate is less than a certain critical value, the accuracy threshold.

Note: The accuracy threshold depends on quantum code ALONE!

Threshold Theorem

So....are we below threshold?

 \diamond Perhaps NOT: $p \sim 10^{-5},$ orders of magnitude away....

♦ We are...BELOW threshold! – Recent advances combining physics and computer science: Quantum computing against biased noise http://arxiv.org/abs/0710.1301

 \diamond Should we celebrate? Perhaps NO – we are JUST below threshold overhead are large...

Both threshold and overhead depend on quantum code ALONE!

◊ Yes? Making BETTER quantum codes! Better quantum codes can be designed. We are full of hope, when computer scientists meeting with physicists...