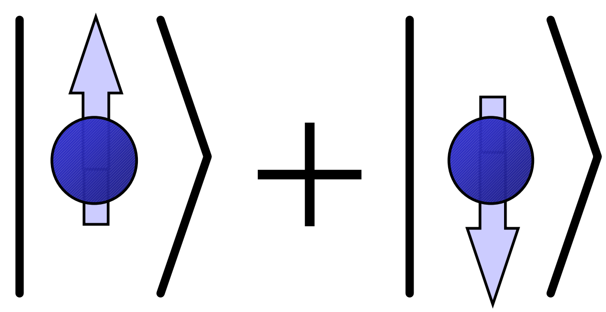
Quantum Computing Architectures

1:00-2:00 Fred Chong (UCD) - Intro, quantum algorithms, and error correction
2:00-2:30 Break and discussion
2:30-3:30 Ike Chuang (MIT) - Device technology and implementation issues
3:30-4:00 Break and official refreshments
4:00-5:00 Mark Oskin (UW) - Quantum architectures
5:00- Discussion

- Plenty of time for questions and discussion
- All materials available at:

http://www.cs.washington.edu/homes/oskin/quantum-tutorial

Quantum Computing for Architects



Fred Chong

University of California at Davis

Science Fiction?

- 5 and 7-bit machines have been built

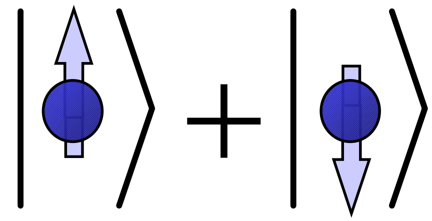
  [Vandersypen01, Laflamme99]
- 100-bit machines are planned
- Better technologies are coming

  [Kane98,Vrijen99,Nakamura99,Mooij99]
- Why architectural study?
  - perspective to guide device development

Outline

- Quantum bits and operations
- Algorithms
  - Quantum search
  - Factorization
- Error correction
- Teleportation

Quantum Bits (qubit)



- 1 qubit probabilistically represents 2 states

$$|a> \;=\; C_0|0> \;+\; C_1|1>$$

- Every additional qubit doubles # states

$$|ab> \;=\; C_{00}|00> \;+\; C_{01}|01> \;+\; C_{10}|10> \;+ C_{11}|11>$$

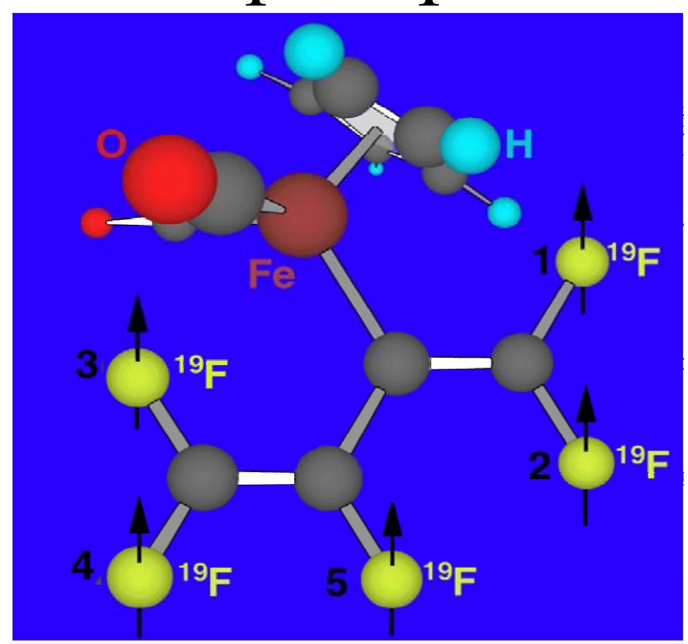
- *Quantum parallelism* on an exponential number of states
- But measurement collapses qubits to single classical values

7 qubit Quantum Computer

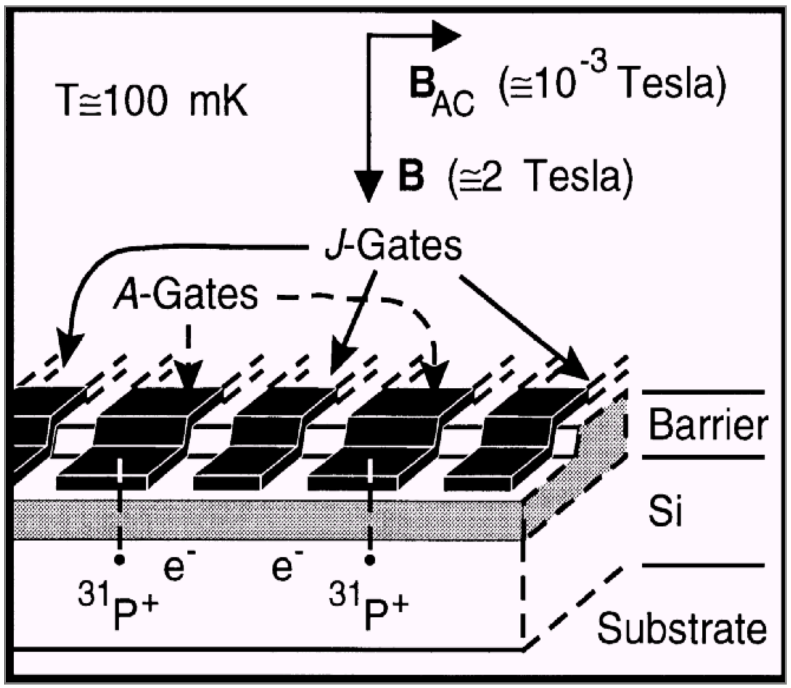
(Vandersypen, Steffen, Breyta, Yannoni, Sherwood, and Chuang, 2001)

- Bulk spin NMR: nuclear spin qubits
- Decoherence in 1 sec; operations at 1 KHz
- Failure probability = 10^{-3} per operation
- Potentially 100 sec @ 10 KHz = 10^{-6} per op

  - **pentafluorobutadienyl cyclopentadienyldicarbonyliron complex**



Silicon Technology



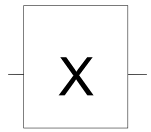
(Kane, Nature 393, p133, 1998)

Quantum Operations

- Manipulate probability amplitudes
- Must conserve energy
- Must be reversible

Bit Flip

X Gate
Bit-flip, Not



$\equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$

- Flips probabilities for |0> and |1>
- Conservation of energy

$$\sum_i C_i^2 = \alpha^2 + \beta^2 = 1$$

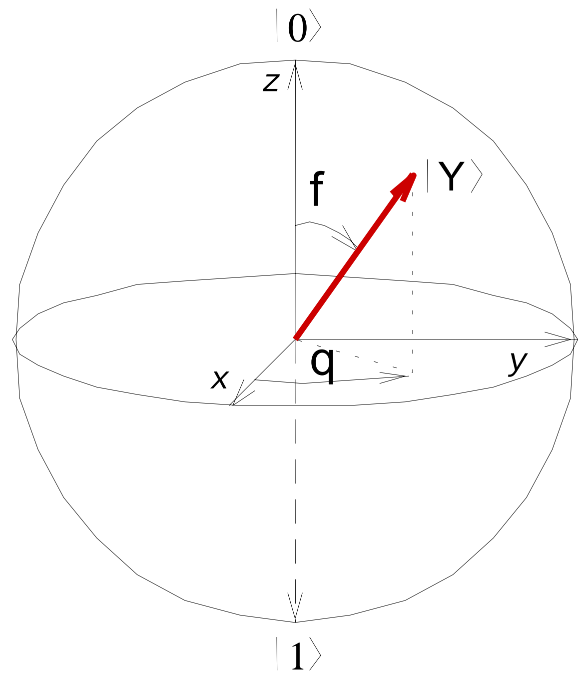
- Reversibility => unitary matrix

$$(X^*)^T X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I$$

(* means complex conjugate)

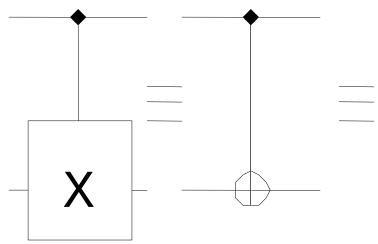
Bloch Sphere

- Visualize a qubit as a vector on a sphere
- Operations composed of a rotation primitive



Controlled Not

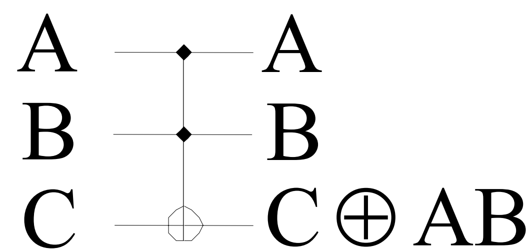
Controlled Not
Controlled X
CNot



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$$

- Control bit determines whether X operates
- Control bit is affected by operation

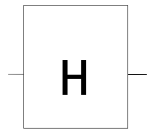
Quantum subsumes Classical



- Toffoli gate, or "controlled-controlled-not"
- NAND does not conserve energy
  – Number of inputs must equal number of outputs
- Toffoli gate simulates NAND
  – Inputs = a,b; c set to 1
  – Output = c

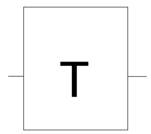
Universal Quantum Operations

H Gate
Hadamard



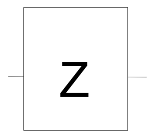
$$\equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \frac{(\alpha+\beta)\,|\,0> +(\alpha-\beta)\,|\,1>}{\sqrt{2}}$$

T Gate



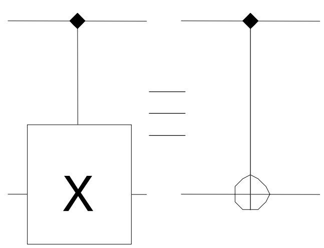
$$\equiv \begin{bmatrix}e^{-\frac{i\pi}{8}} & 0\\ 0 & e^{\frac{i\pi}{8}}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha e^{-\frac{i\pi}{8}}\,|\,0> +\beta e^{\frac{i\pi}{8}}\,|\,1>$$

Z Gate
Phase-flip



$$\equiv \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha\,|\,0> -\beta\,|\,1>$$

Controlled Not
Controlled X
CNot

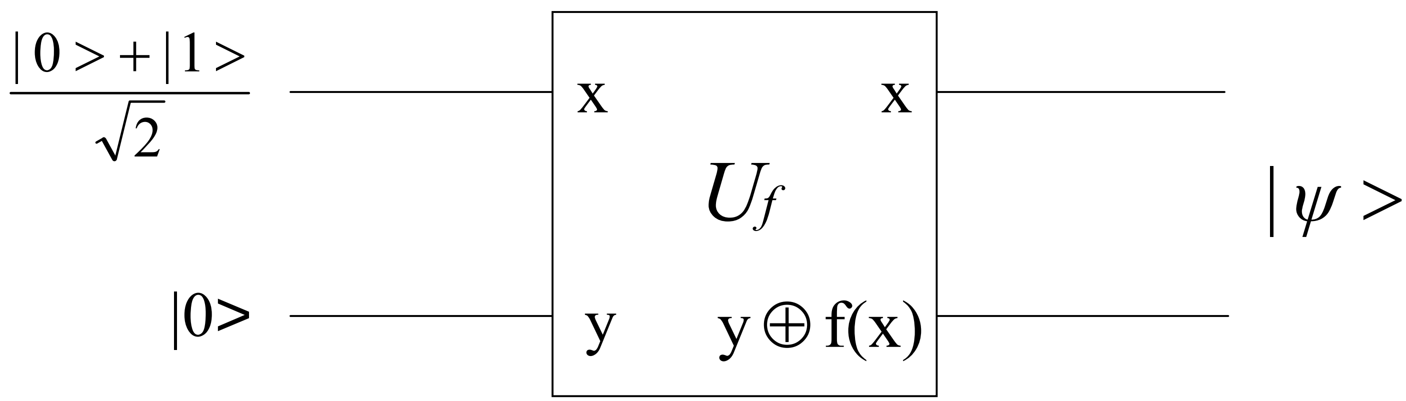


$$\equiv \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}a\\ b\\ c\\ d\end{bmatrix} = a\,|\,00> +b\,|\,01> +d\,|\,10> +e\,|\,11>$$

Quantum Algorithms

- Search (function evaluation)
- Factorization (FFT, discrete log)
- Key distribution
- Digital signatures
- Clock synchronization

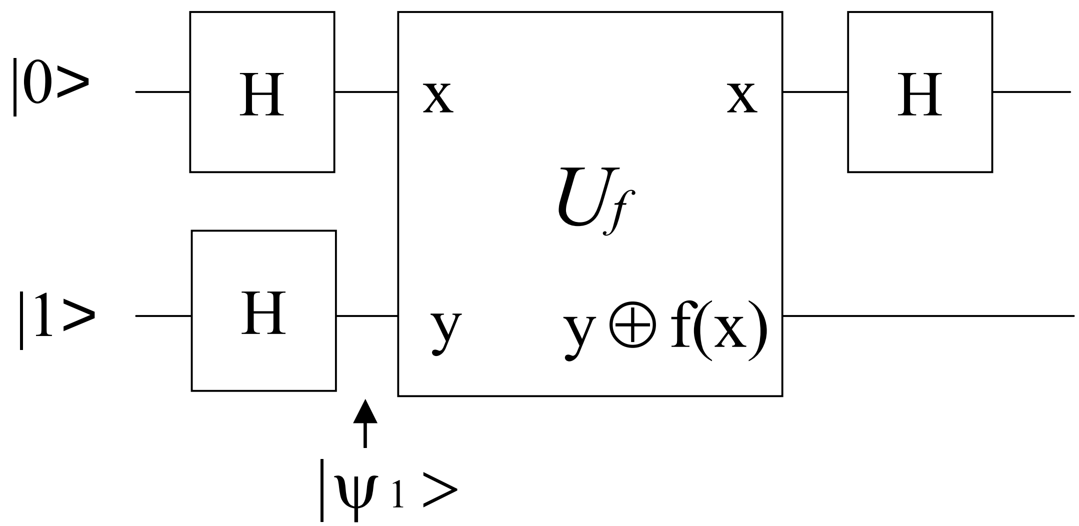
Quantum Parallelism



$$f(x) : \{0,1\} \rightarrow \{0,1\}$$

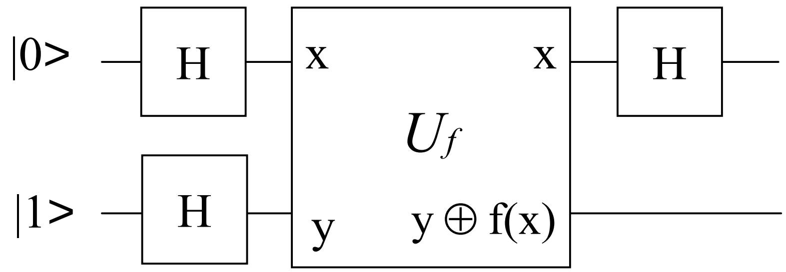
$$|\psi> = \frac{|0, f(0)> + |1, f(1)>}{\sqrt{2}}$$

Deutch's Algorithm(1) [Deutch 85]



$$|\psi_1> = \left[\frac{|0> + |1>}{\sqrt{2}}\right]\left[\frac{|0> - |1>}{\sqrt{2}}\right]$$

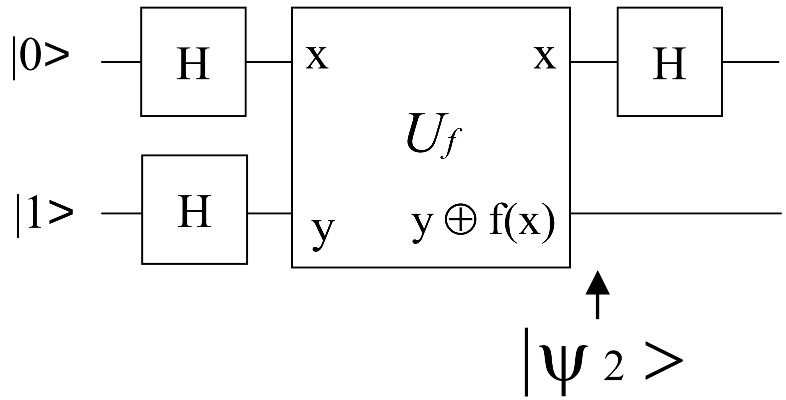
Deutch's Algorithm(2)



Note that the xor just flips the probabilities for |0> and |1> :

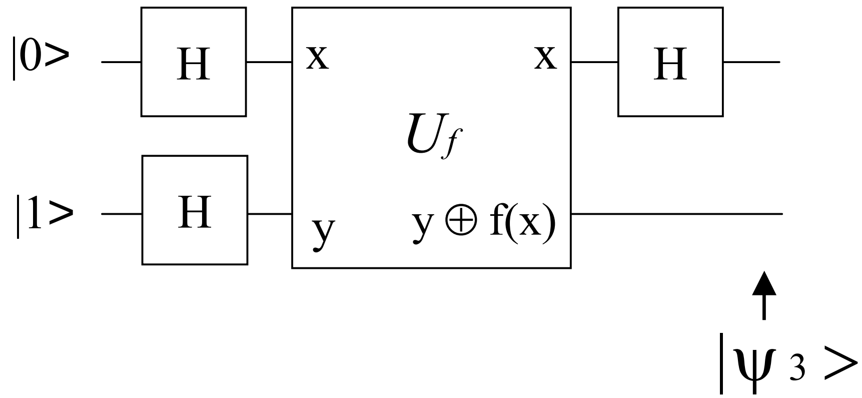
$$U_f\left(|x> \frac{|0> - |1>}{\sqrt{2}} \right) = (-1)^{f(x)} |x> \frac{|0> - |1>}{\sqrt{2}}$$

Deutch's Algorithm(3)



$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1) \end{cases}$$

Deutch's Algorithm(4)



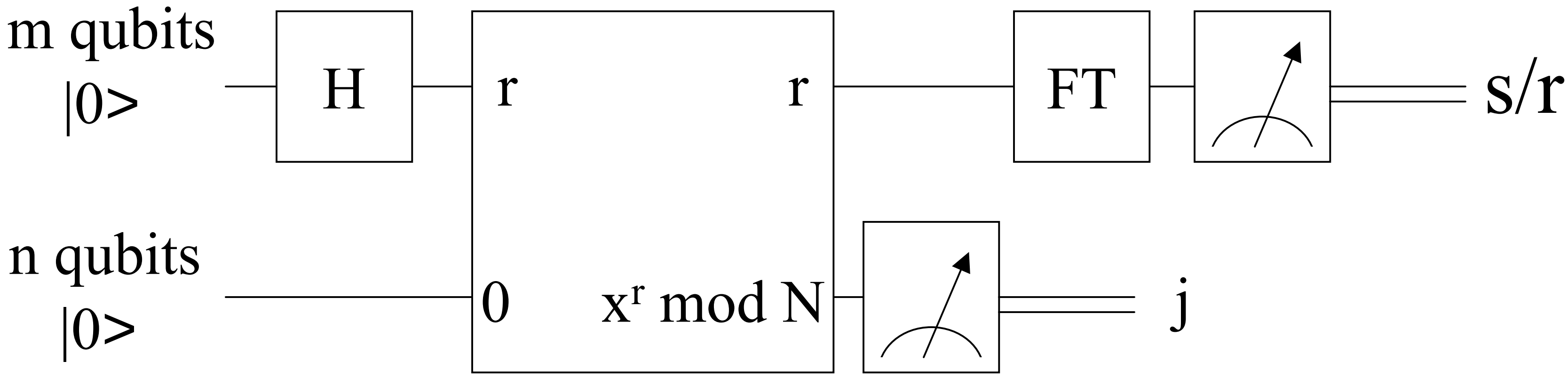
$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)=f(1) \\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & \text{if } f(0)\neq f(1) \end{cases}$$

$$= \quad \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Quantum Factorization

- For $N = pq$, where p,q are large primes,
  find p,q given N
- Let $r = \text{Order}(x,N)$, which is min value > 0
  such that $x^r \bmod N = 1$, x coprime N
- Then $(x^{r/2} +/- 1) \bmod N = p,q$
- eg $\text{Order}(2, 15) = 4$
  $(x^{4/2} +/- 1) \bmod 15 = 3,5$

Shor's Algorithm [Shor94]



j=1: |r> = |0> + |4> + |8> + |12> + ...

j=2: |r> = |1> + |5> + |9> + |13> + ...

j=4: |r> = |2> + |6> + |10> + |14> + ...

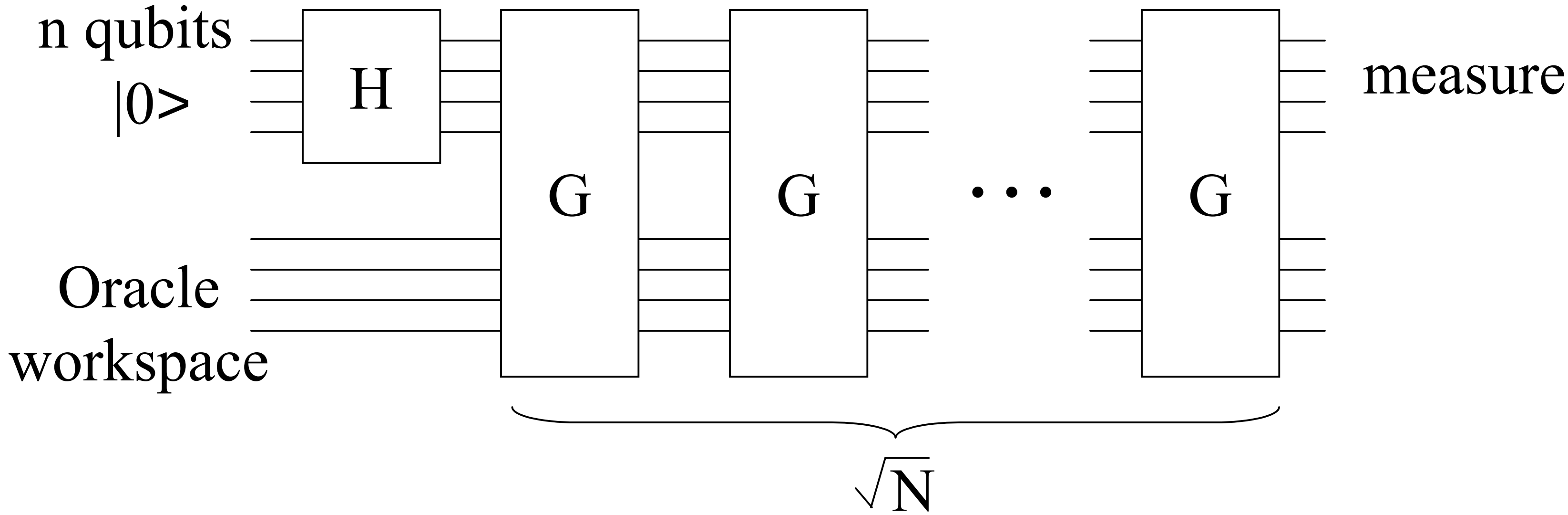
j=8: |r> = |3> + |7> + |11> + |15> + ...

Quantum Fourier Transform

- r is in the period, but how to measure r?
- QFT takes period r => period s/r
- Measurement yields I*s/r for some I
- Reduce fraction I*s/r =>

  r is the denominator with high probability!
- Repeat algorithm if pq not equal N
- $O(n^3)$ instead of $O(2^n)$!!!

Quantum Search (function evaluation)



- Iteratively concentrates probability towards desired measurement [Grover96]
- Can search N unordered items in $\sqrt{N}$ time

Error Correction is Crucial

- Need continuous error correction
  - can operate on encoded data

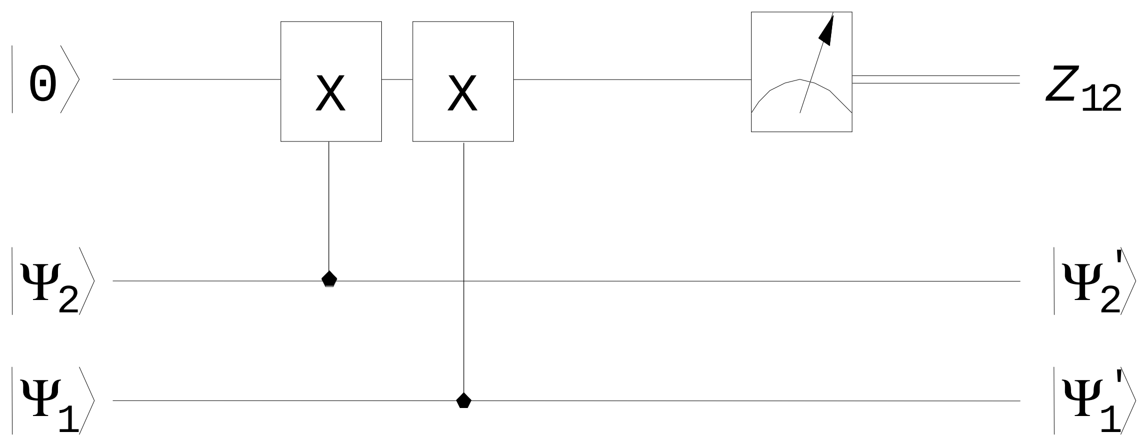
    [Shor96, Steane96, Gottesman99]
- Threshold Theorem [Ahanorov 97]
  - failure rate of 10^{-4} per op can be tolerated
- Practical error rates are 10^{-6} to 10^{-9}

Quantum Error Correction

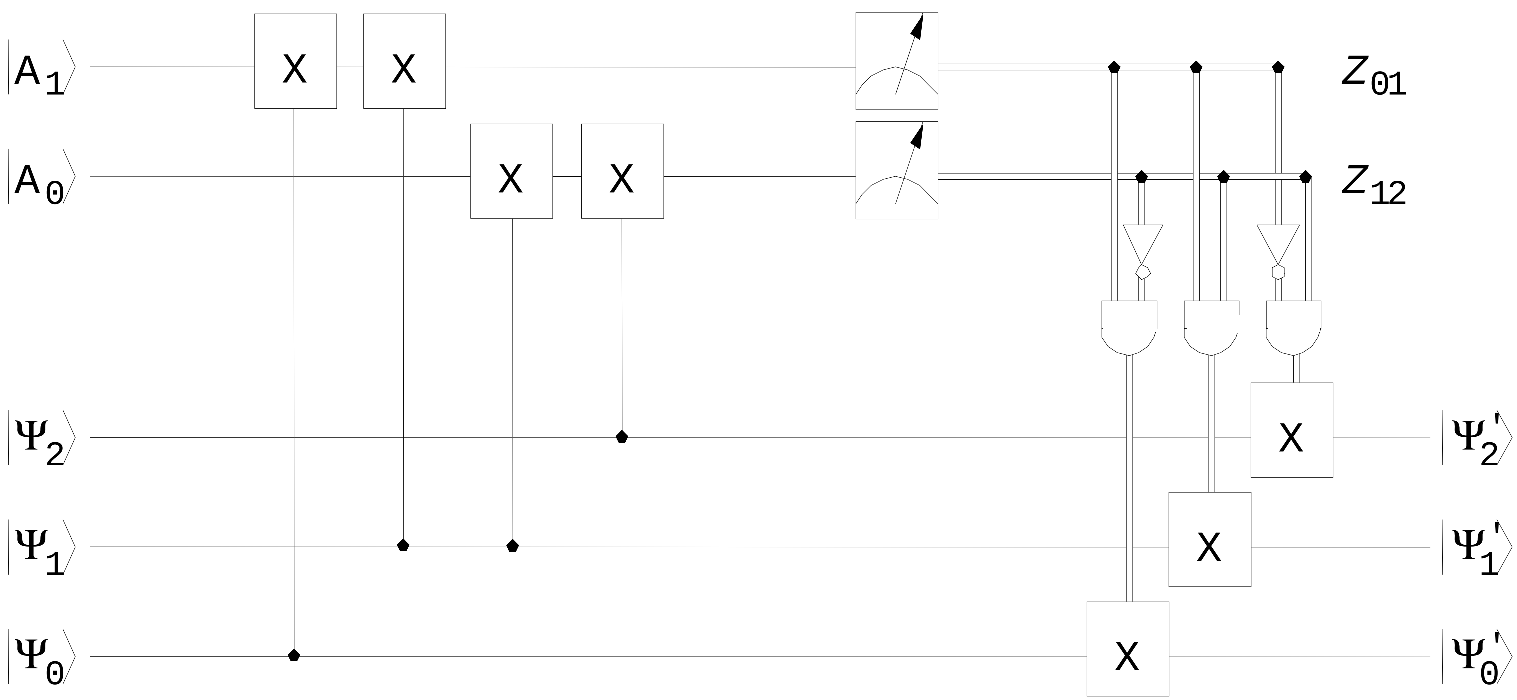
Z_{12}	Z_{23}	**Error Type**	**Action**
+1	+1	no error	no action
+1	-1	bit 3 flipped	flip bit 3
-1	+1	bit 1 flipped	flip bit 1
-1	-1	bit 2 flipped	flip bit 2

(3-qubit code)

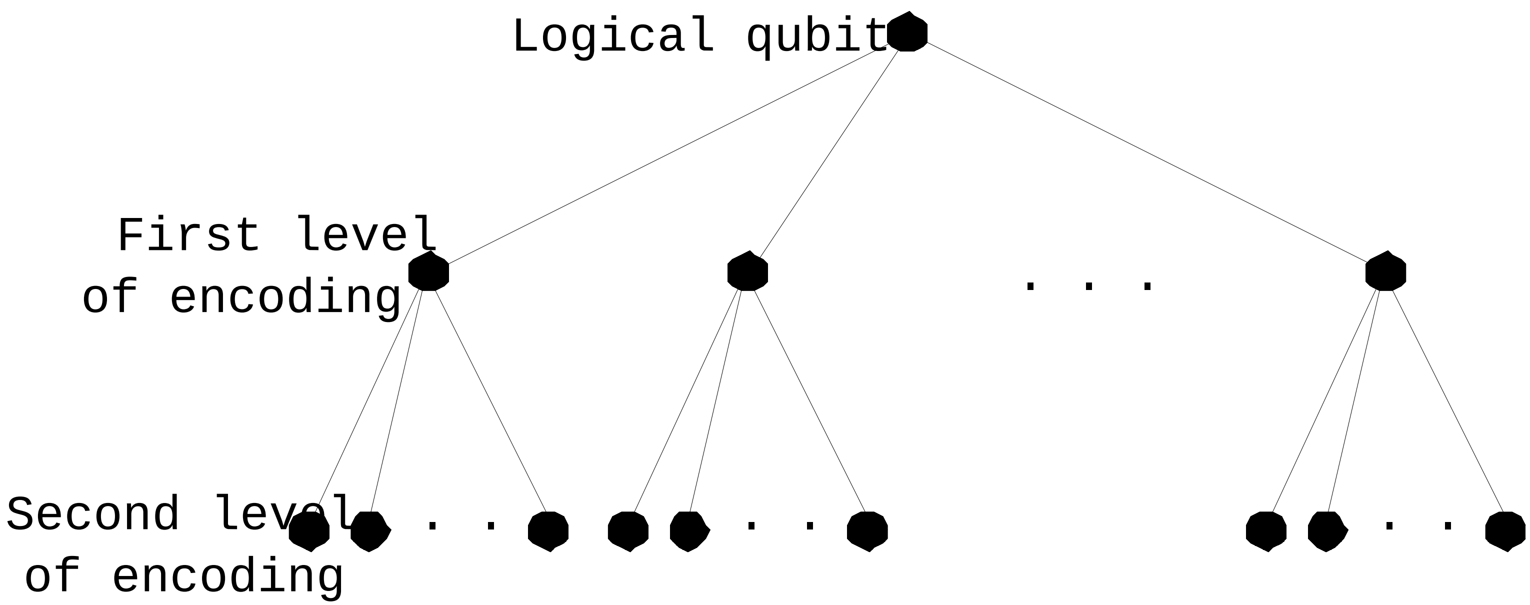
Syndrome Measurment



3-bit Error Correction



Concatenated Codes

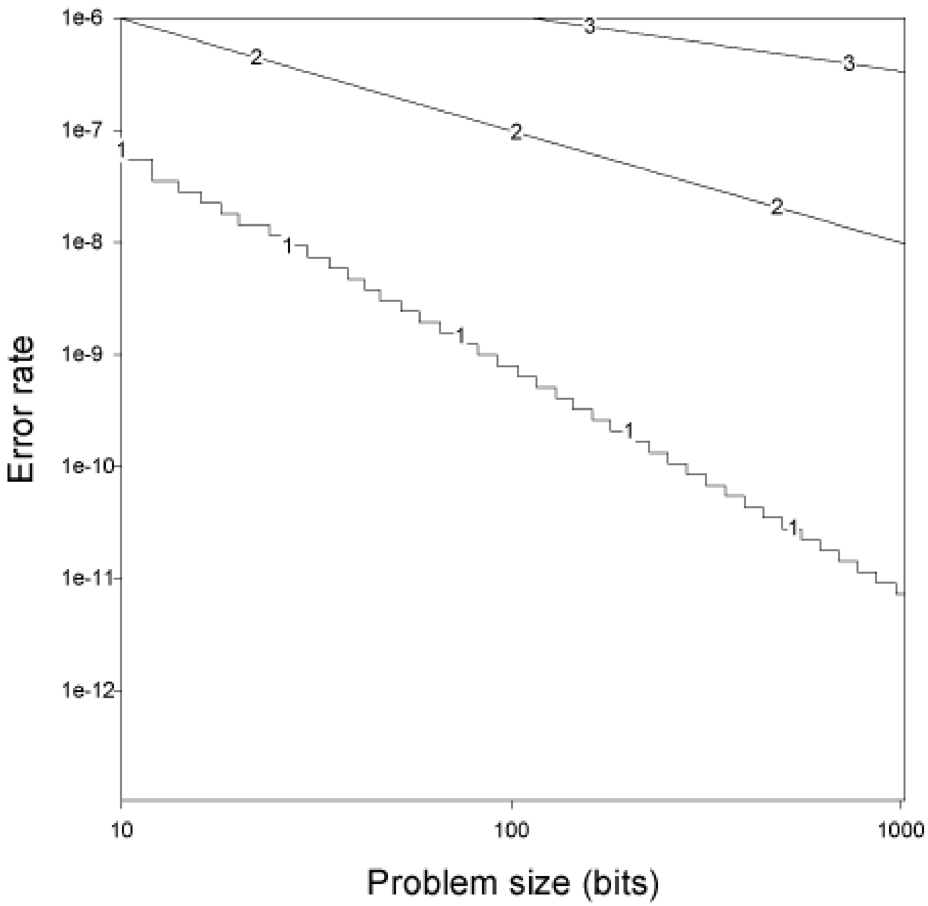


Error Correction Overhead

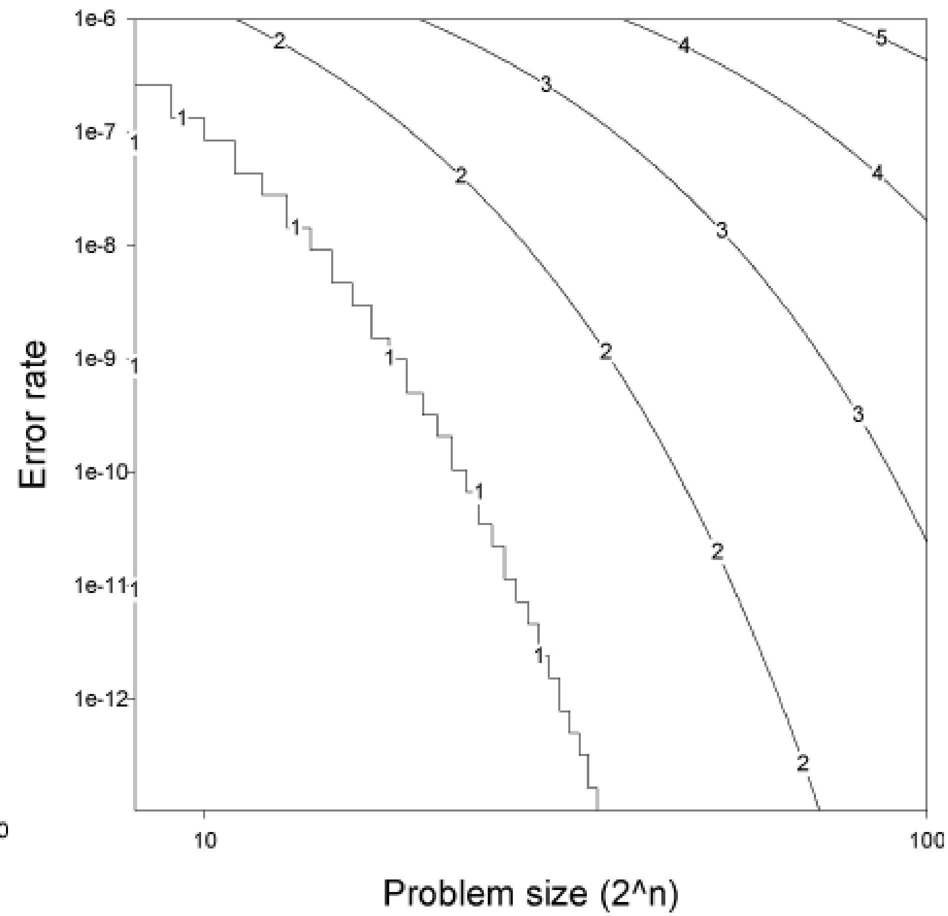
- 7-qubit code [Steane96], applied recursively

Recursion (k)	**Storage (7^k)**	**Operations (153^k)**	**Min. time (5^k)**
0	1	1	1
1	7	153	5
2	49	23,409	25
3	343	3,581,577	125
4	2,401	547,981,281	625
5	16,807	83,841,135,993	3125

Recursion Requirements

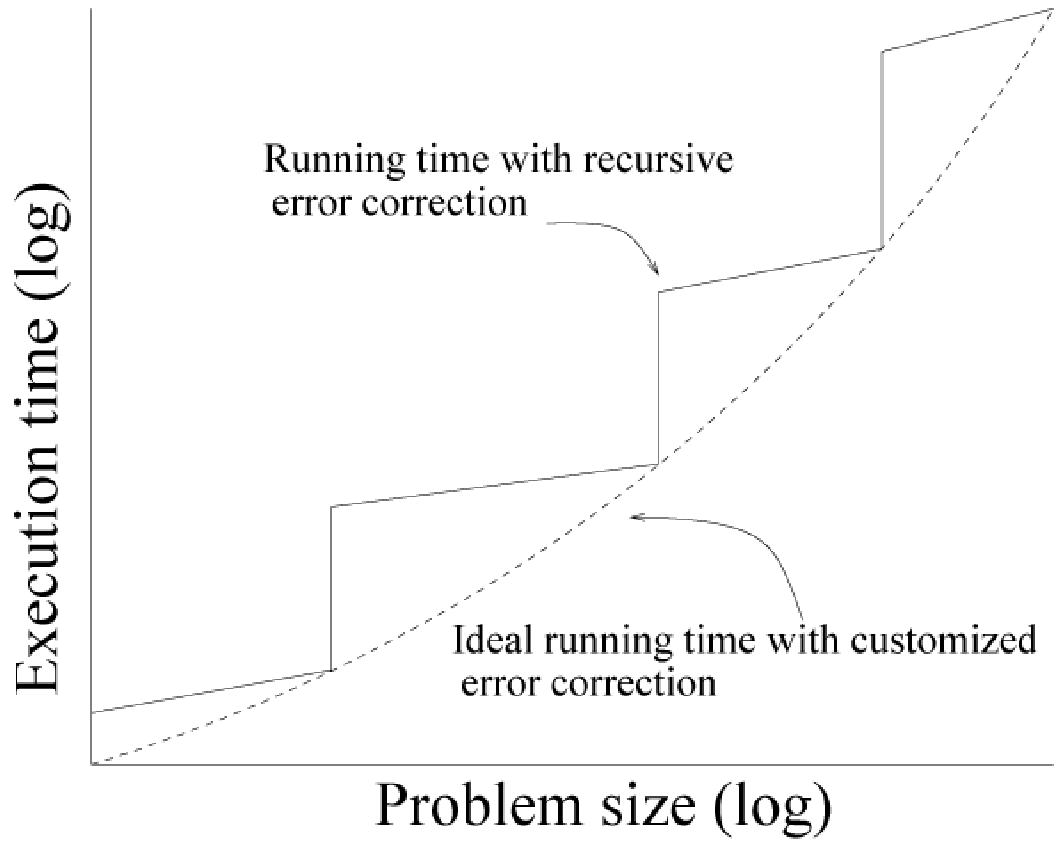


Shor's



Grover's

Clustering

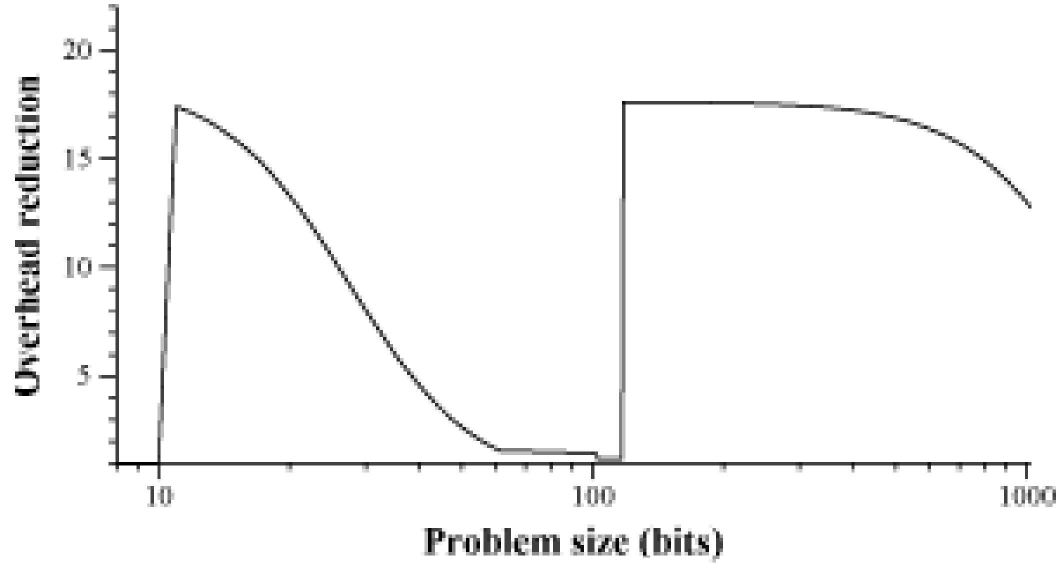


- Recursive scheme is overkill
- Don’t error correct every operation

[Oskin,Chong,Chuang IEEE Computer 02]

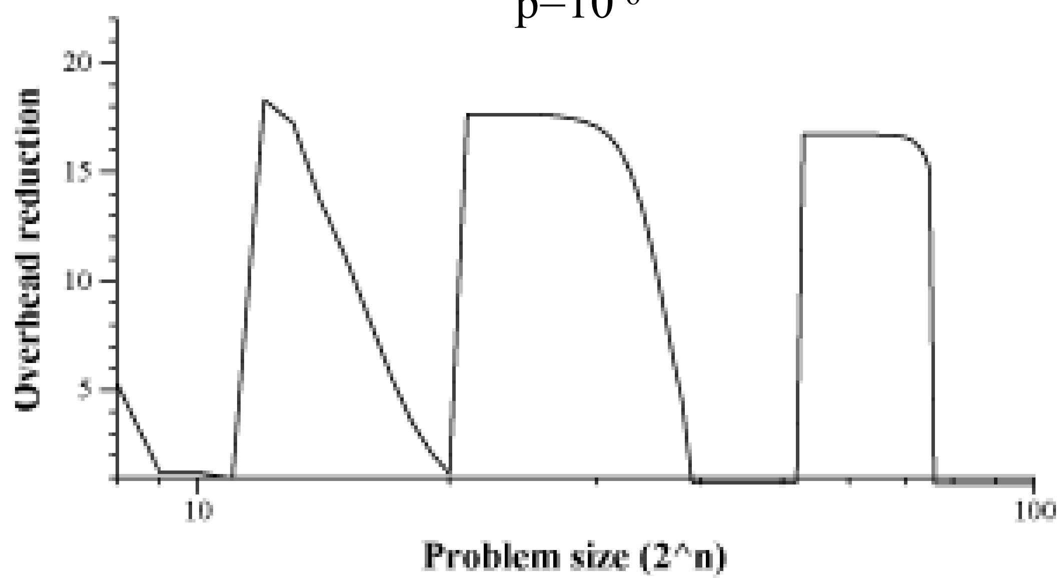
Space Savings

Shor's



$p=10^{-6}$

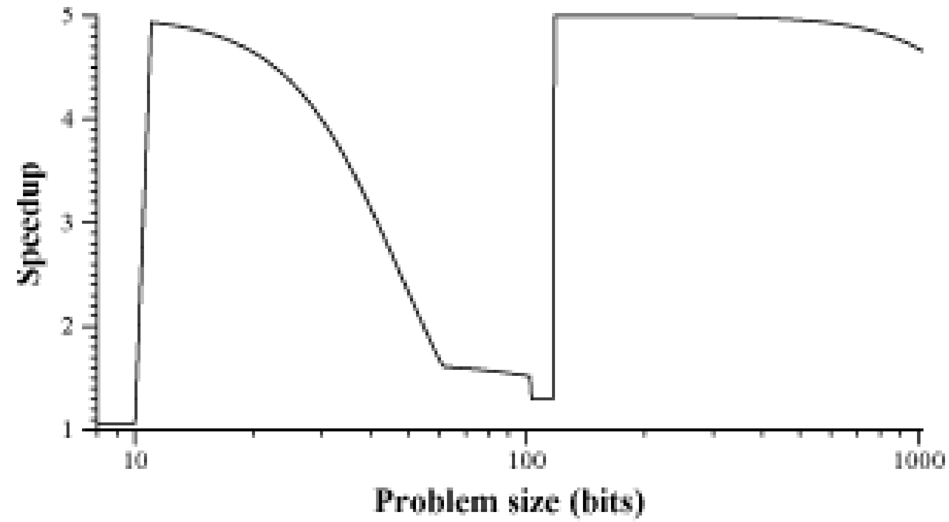
Grover's



$p=10^{-6}$

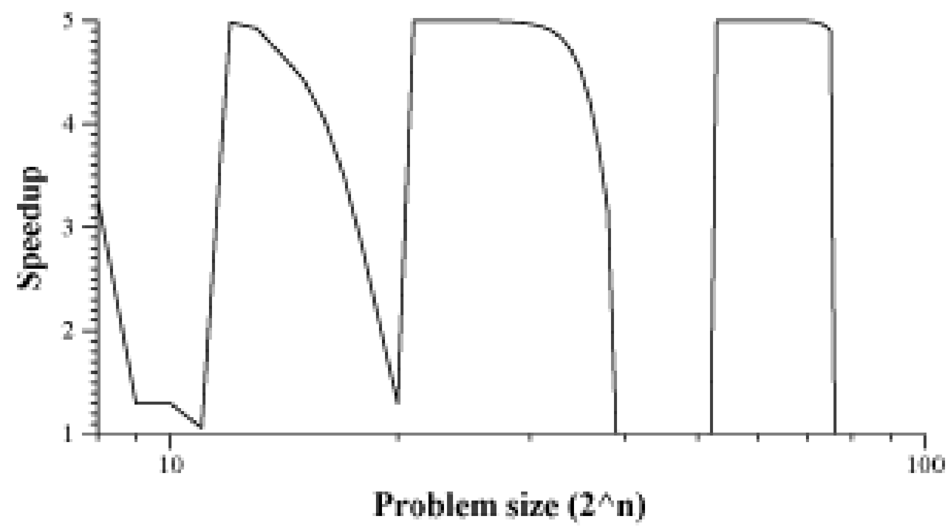
Time Savings

Shor's



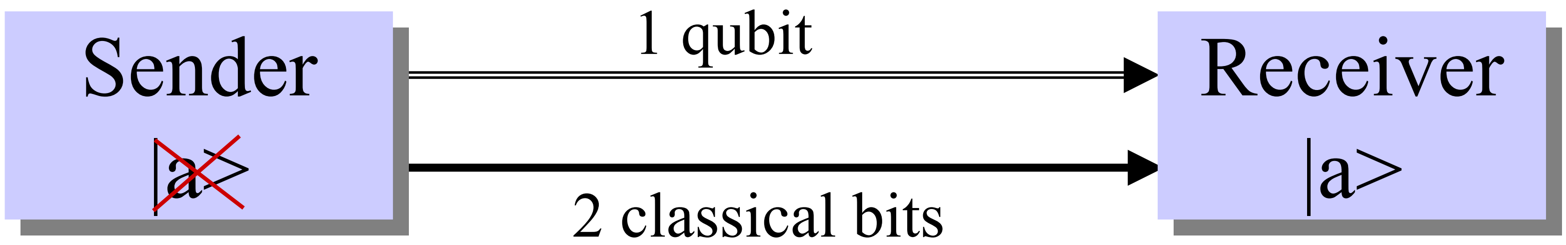
$p=10^{-6}$

Grover's



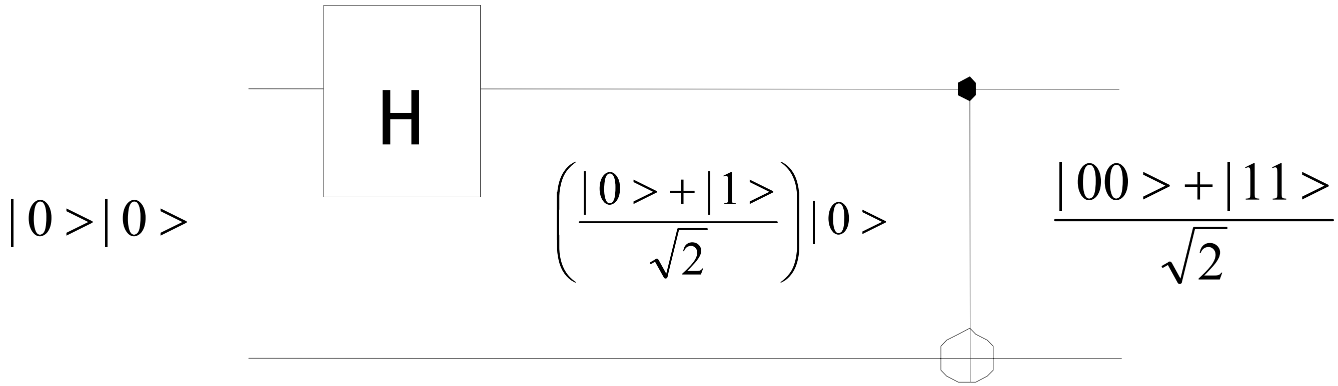
$p=10^{-6}$

Teleportation



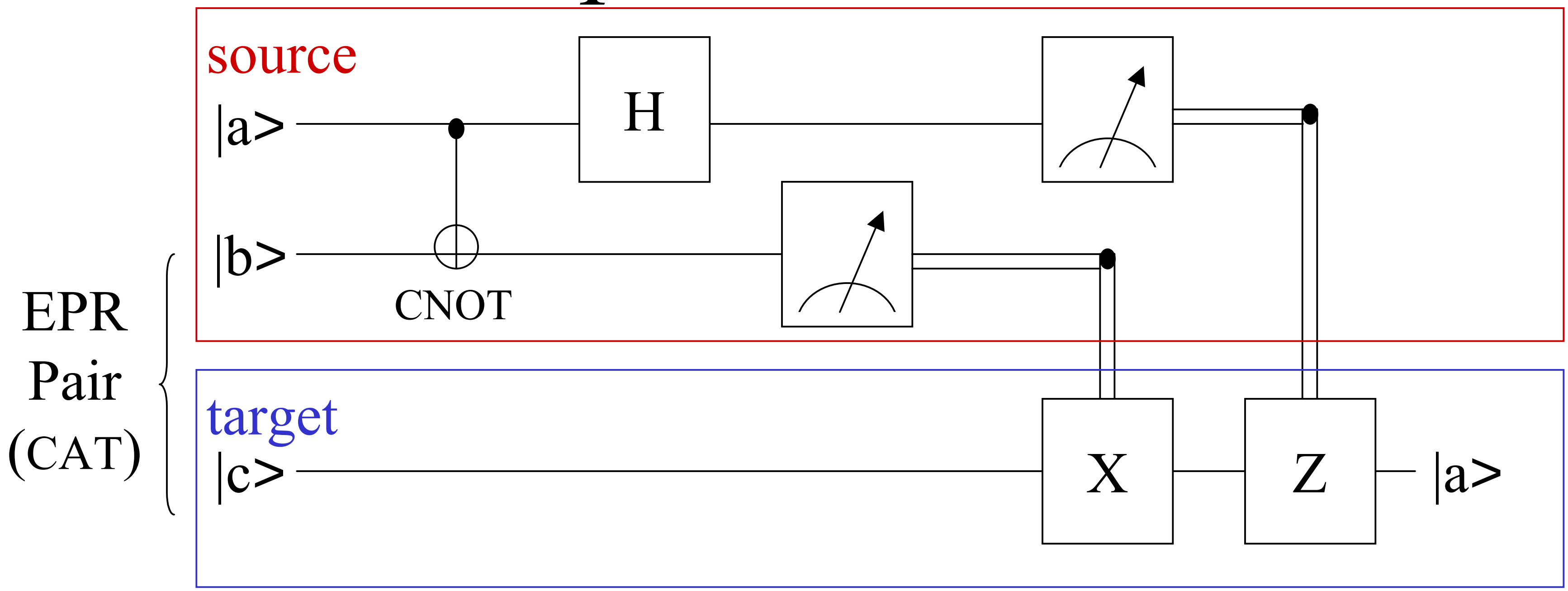
- Destroy source qubit and recreates at target
- Pre-communicate half of a CAT state

CAT State



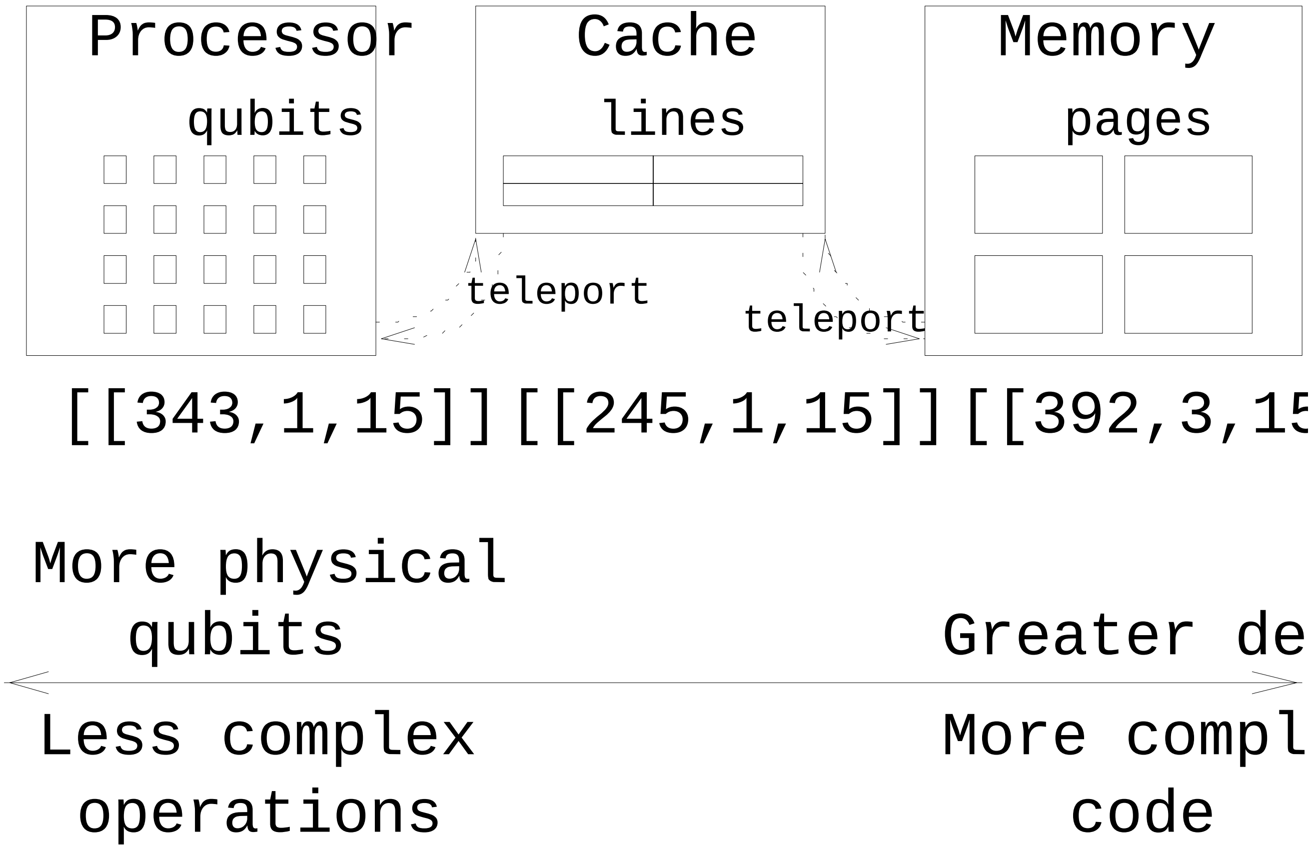
- Two bits are in “lockstep”
  - both 0 or both 1
- Named for Shrodinger’s cat
- Also “EPR pair” for Einstein, Podolsky, Rosen

Teleportation Circuit

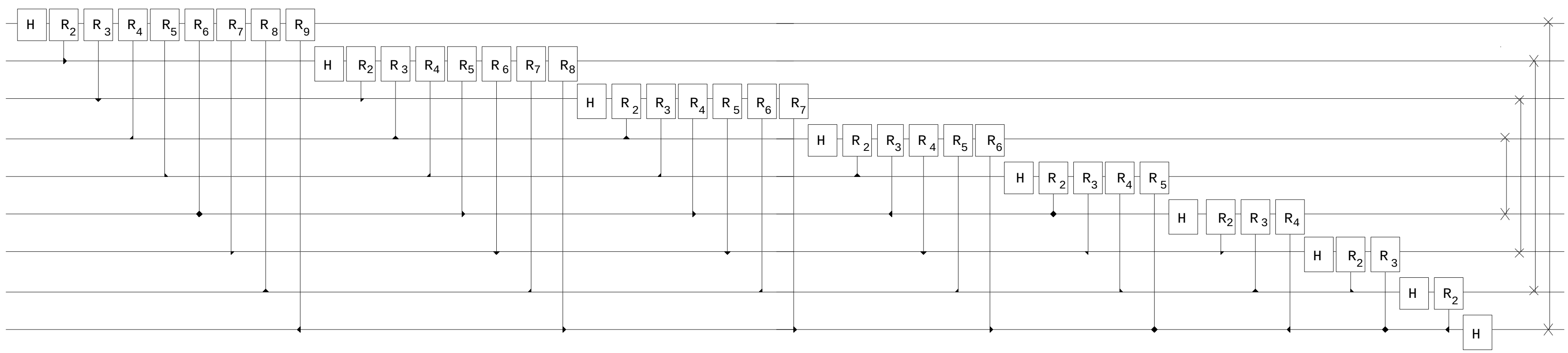


- Source generates |bc> EPR pair
- Pre-communicate |c> to target with retry
- Classical communication to set value
- Can be used to convert between codes!

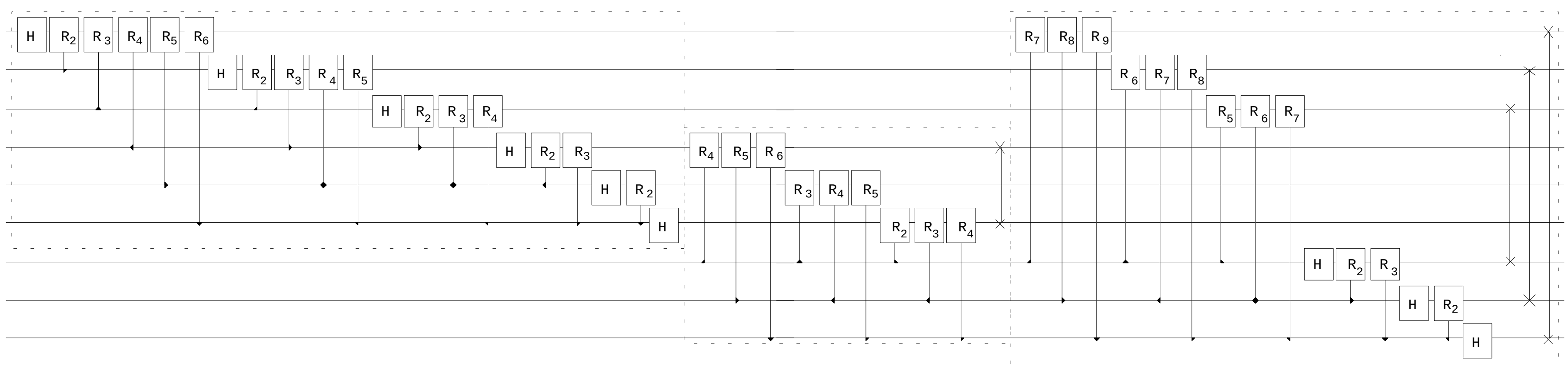
Memory Hierarchy



Quantum Fourier Transform



Blocked QFT


H R_2 R_3 R_4 R_5 R_6
H R_2 R_3 R_4 R_5
H R_2 R_3 R_4
H R_2 R_3
H R_2
H
R_4 R_5 R_6
R_3 R_4 R_5
R_2 R_3 R_4
R_7 R_8 R_9
R_6 R_7 R_8
R_5 R_6 R_7
H R_2 R_3
H R_2
H

Summary

- Quantum computers can be built
- Error correction allows scalability
- Tremendous potential for some applications

Rest of the afternoon

- Isaac Chuang - Quantum devices
  - How things really work
- Mark Oskin – Quantum architectures
  - What architects can do