

# Quantum Computing: Progress and Prospects

Tony Hey and Douglas Ross  
University of Southampton

# Plan of Lectures

- Lecture #1: Introduction to Quantum Information Theory - Fundamentals (Tony Hey)
- Lectures #2,3 & 4: Quantum Algorithms in Detail - Bell States, Quantum Teleportation, Grover's Quantum Search and Shor's Quantum Factorization (Douglas Ross)
- Lecture #5: Quantum Cryptography and Computing - State of the Art (Tony Hey)

# Introduction to Quantum Information Theory - Fundamentals

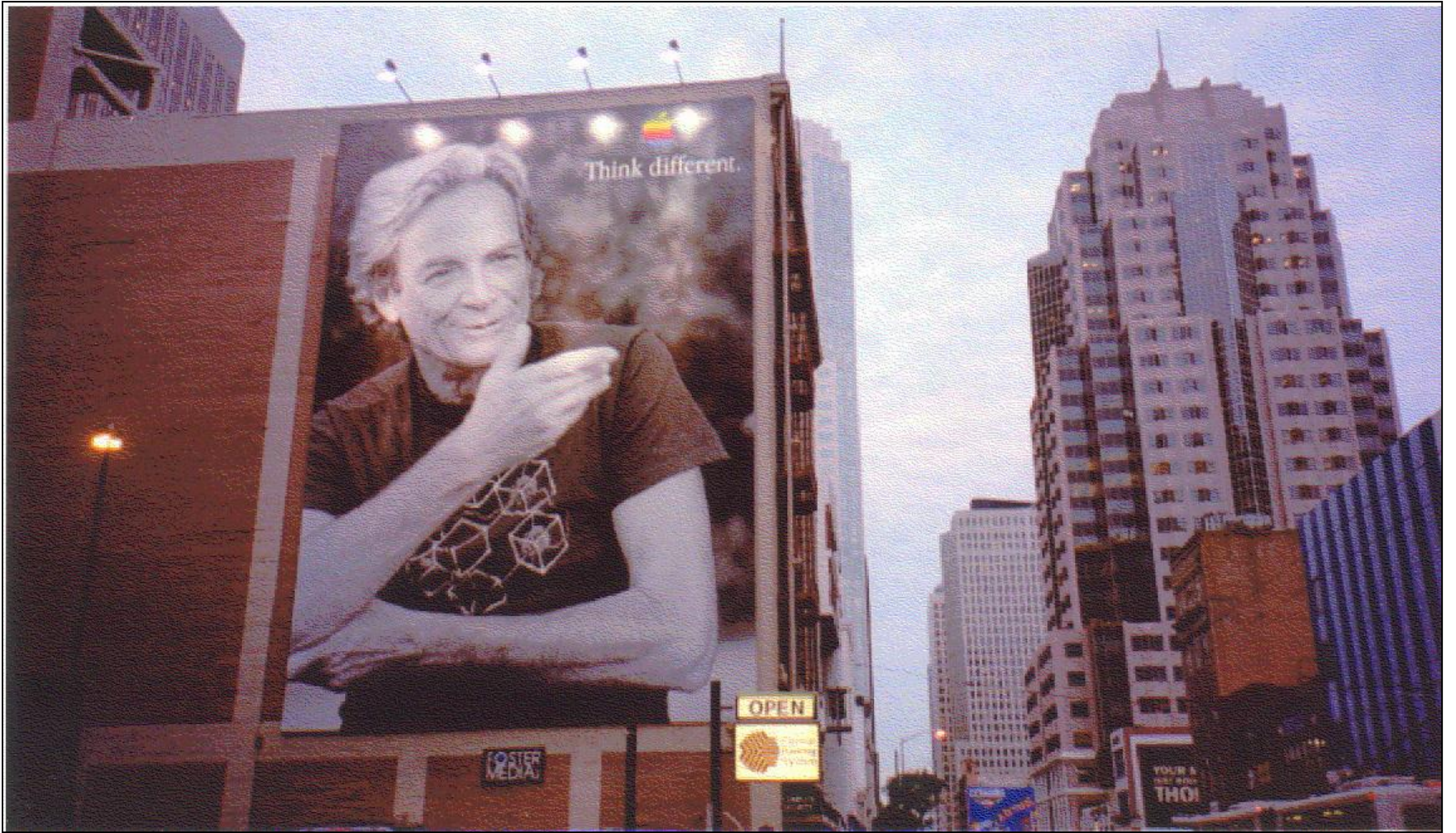
Tony Hey

Director of e-Science  
EPSRC, Swindon

[Tony.Hey@epsrc.ac.uk](mailto:Tony.Hey@epsrc.ac.uk)

# Outline of Lecture

- Feynman's Lectures
- Deutsch, Shor and RSA 129
- Reversible Computing
- Qubits and Quantum Gates
- EPR and Quantum Entanglement
- No Cloning and Teleportation
- Quantum Algorithms



# Feynman's Lectures

- 1959 : Plenty of Room at the Bottom
- 1981 : Simulating Physics with Computers
- 1982-87 : Limitations and Potentialities of Computers
  - published as 'The Feynman Lectures on Computation' (edited by Tony Hey and Robin Allen)



# Plenty of Room at the Bottom

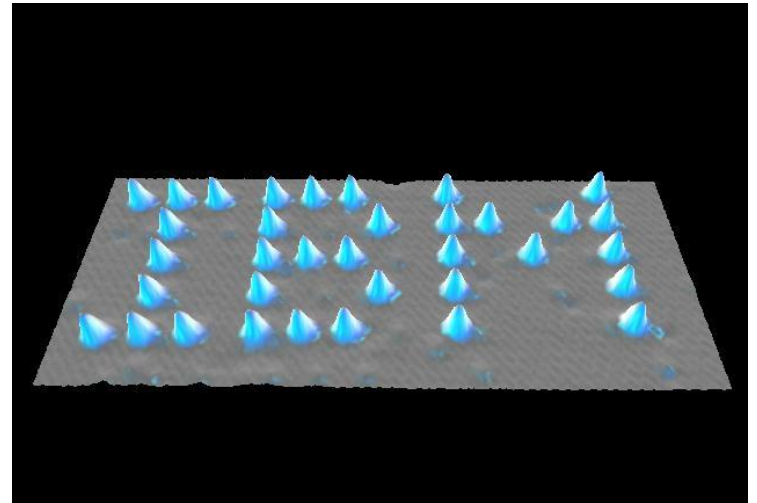
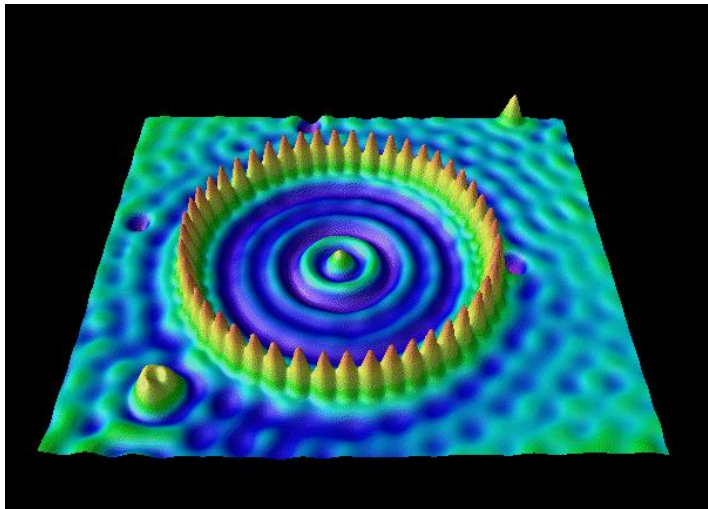
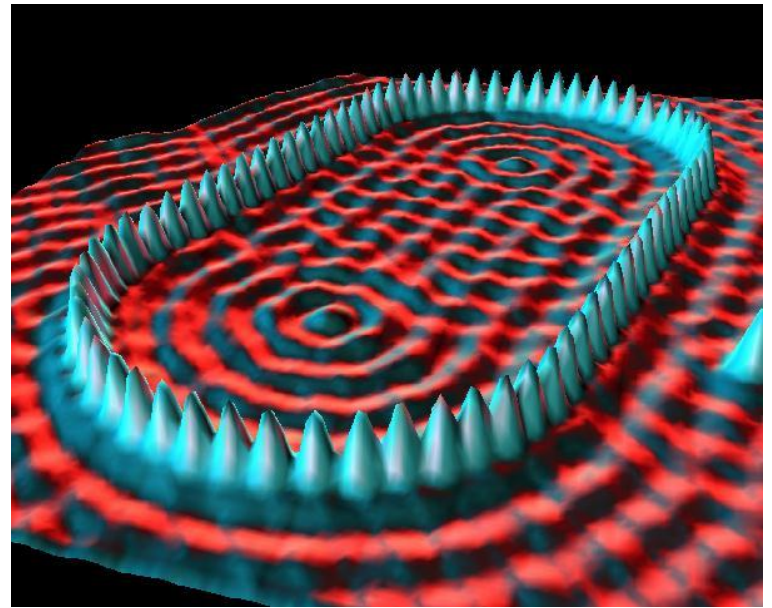
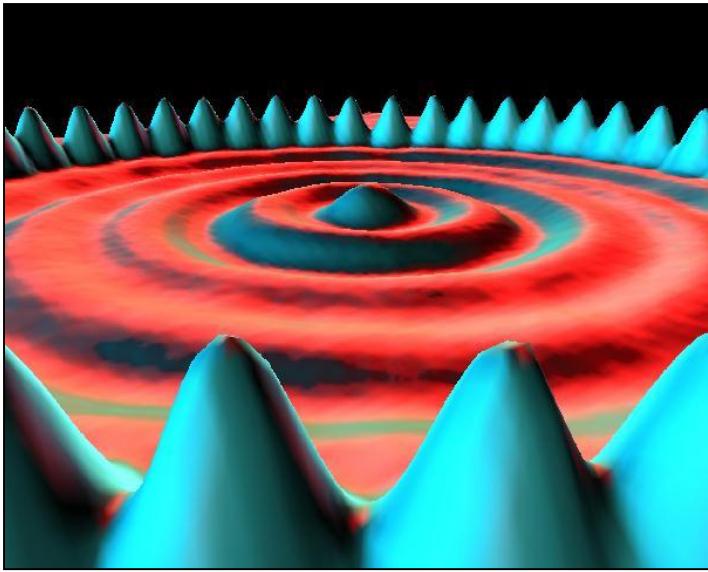
In 1959 Feynman gave an after-dinner talk at an APS meeting in Pasadena entitled 'There's Plenty of Room at the Bottom'

- "problem of manipulating and controlling things on a small scale"
- talking about the "staggeringly small world that is below"
- "what could be done if the laws are what we think; ...we haven't gotten round to it yet"

# Feynman and Nanotechnology

“In the year 2000, when they look back at this age, they will wonder why it was not until the year 1960 that anybody began to move in this direction.”





# Simulating Physics with Computers

- Can a universal classical computer simulate physics *exactly*?
- Can a classical computer *efficiently* simulate quantum mechanics?
- "I'm not happy with all the analyses that go with just classical theory, because Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem!"

Richard Feynman 1981

“How can we simulate the quantum mechanics?...Can you do it with a new kind of computer - a quantum computer? It is not a Turing machine, but a machine of a different kind.”

R P Feynman 1981

# Deutsch, Shor and RSA 129 (1)

Seminal paper by Deutsch (1985)

- Quantum computers can evolve a superposition of quantum states - each could follow coherently distinct computational paths till measure final output
- Such "quantum parallelism" could potentially outstrip power of classical computers

Why care?

# Deutsch, Shor and RSA 129 (2)

Universality of Turing Machines makes it possible to classify algorithms into complexity classes

- Algorithms for which time grows polynomially with problem size are said to be 'tractable' and in class 'P'

E.g. Matrix multiplication  $\sim O(N^3)$

- Algorithms for which time grows exponentially with problem size are said to be 'intractable' and in classes such as 'NP'

E.g. Travelling Salesman

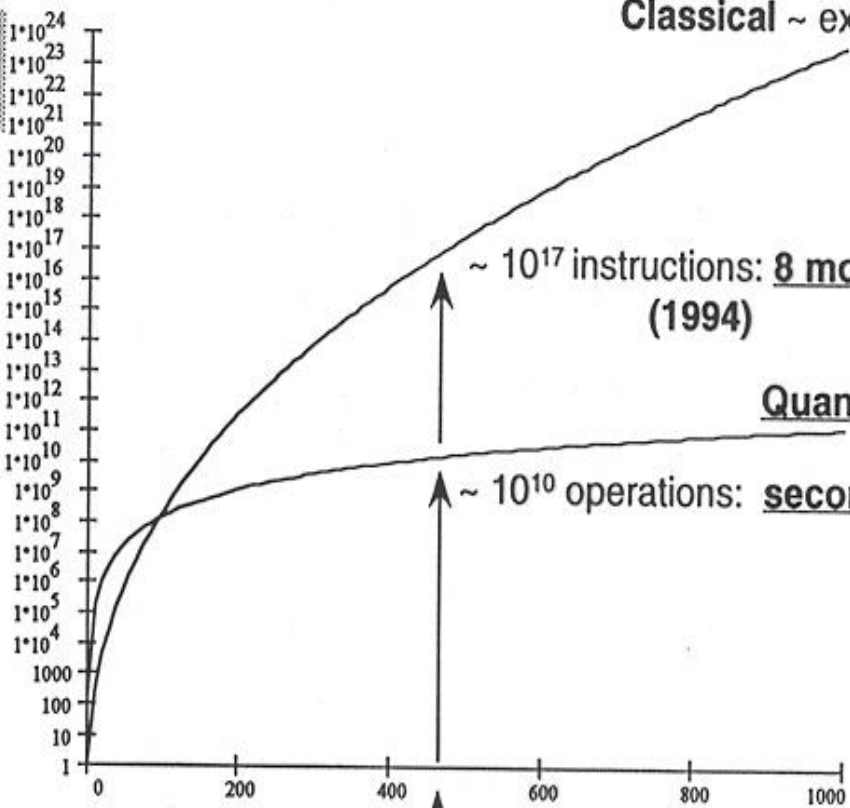
# Multiplication versus Factoring

3490529510		3278918299		11438162575788888768
8476509491		3268709549		92357799761468120102
4784961990		9619881908		18298721242362562551
3898133417	X	3448141317	=	84293570693524573389
7648384933		7642987992		78305971235639587050
8784399082		9425397982		58989075147599290026
0577		88533		879543541

Figure 1. Prime factors of the 129-digit number known as RSA-129.



# of instructions



Classical  $\sim \exp\{A[L^{1/3}\ln^{2/3}L]\}$

$\sim 10^{17}$  instructions: 8 months  
(1994)

Quantum  $\sim L^3$

$\sim 10^{10}$  operations: seconds

RSA129

# of bits, L,  
factored



# Reversible Computing (1)

Charles Bennett (1973)

Computation can utilize a series of steps, each logically reversible, and this in turn allows physical reversibility

⇒ Could this be a realistic way to reduce power consumption in CMOS?

⇒ Laws of quantum physics are reversible in time, so can we use quantum versions to build a quantum computer?

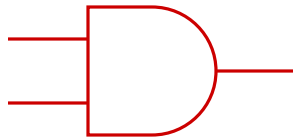
# Reversible Computing (2)

- Prior to Bennett's "epoch making" paper in 1973

⇒ Always assumed any computational step required

energy  $\sim kT$

e.g. AND gate



Computation compresses options from 2 to 1

$$\Rightarrow \Delta E = kT \log 2$$

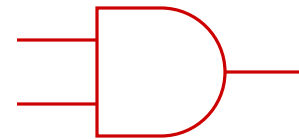
Is such an energy loss inevitable?

# Reversible Computing (3)

Bennett: No - computation can be done with no minimal loss of energy provided performed slowly enough!

Not purely academic question: present-day transistors dissipate  $\sim 10^8 kT$  per switch!

How do we do this?



AND gate is irreversible

(1,0), (0,1), (0,0) mapped to same output

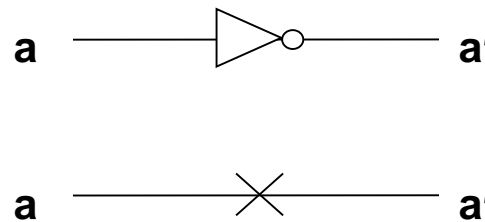
⇒ Destroys information and must generate heat

# Reversible Computing (4)

## Fredkin's Reversible Gates

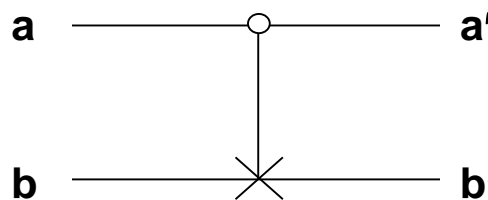
### An example

- Classical NOT gate  
Clearly reversible  
☑ use X symbol



A	NOT A
0	1
1	0

- Controlled NOT gate 'CN'  
NOT operation X  
controlled by input  
to O-wire

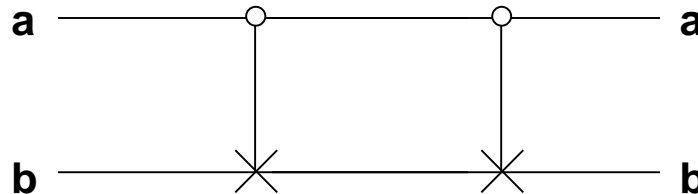


a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

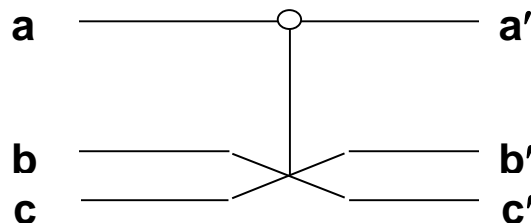
# Reversible Computing (5)

- CN gate reversible: from output can deduce input

Can reverse CN gate by repeating it:



- For complete set of operators to build all standard gates - such as AND, OR, XOR, NAND - need additional gate such as the 'Controlled Controlled Not' (CNN) gate (also known as a Toffoli gate) or the 'Fredkin' Exchange gate:



# Qubits and Quantum Gates (1)

## Qubits

Instead of classical bits made of 1's and 0's

⇒ quantum bit is quantum 2-level system

$|1\rangle$  and  $|0\rangle$  e.g.  $\uparrow$  and  $\downarrow$  for spin  $1/2$

- **General state is superposition**

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

- Ensemble measurement on  $|\psi\rangle$ 
  - ☑ Result 1 with probability  $|\alpha|^2$
  - ☑ Result 0 with probability  $|\beta|^2$

$$|\alpha|^2 + |\beta|^2 = 1$$

Normalization preserved by  
unitary operators  $U^\dagger U = 1$

# Qubits and Quantum Gates (2)

## Quantum Gates

- If define  $U_{NOT}$

$$U_{NOT}|1\rangle = |0\rangle$$

$$U_{NOT}|0\rangle = -|1\rangle$$

- In QM can consider operations with no classical counterpart  
e.g. Square-Root-of-Not

$$(U_{SRN})^2 = U_{NOT}$$

Aside:  $U_{SRN}$  just  $90^\circ$   
rotation of spin

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

$$U_{SRN}|0\rangle = \frac{1}{\sqrt{2}}(-|1\rangle + |0\rangle)$$



# Qubits and Quantum Gates (3)

## Quantum Registers

n-bit register:

$$|\psi_n\rangle = |1\rangle \otimes |1\rangle \dots \otimes |1\rangle \equiv |11\dots 1\rangle$$

If apply  $U_{SRN}$  to each qubit

$$\begin{aligned} |\psi_n'\rangle &= U_{SRN} \otimes U_{SRN} \dots \otimes U_{SRN} |11\dots 1\rangle \\ &= \frac{1}{2^{n/2}} (|1\rangle + |0\rangle) \otimes (|1\rangle + |0\rangle) \dots \otimes (|1\rangle + |0\rangle) \\ &= \frac{1}{2^{n/2}} \{ |11\dots 1\rangle + |11\dots 0\rangle + \dots + |00\dots 0\rangle \} \end{aligned}$$

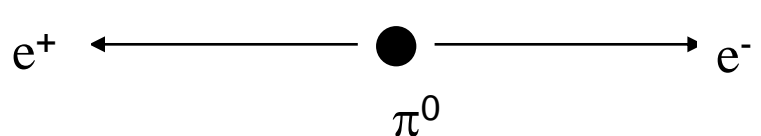
i.e. Linear number of operations generate register state with exponential ( $2^n$ ) number of terms

Ability to create quantum superpositions makes quantum parallel processing possible

# EPR and Quantum Entanglement (1)

- Consider decay of  $\pi^0$  to  $e^+e^-$  pair

$e^+e^-$  pair in spin 0 state



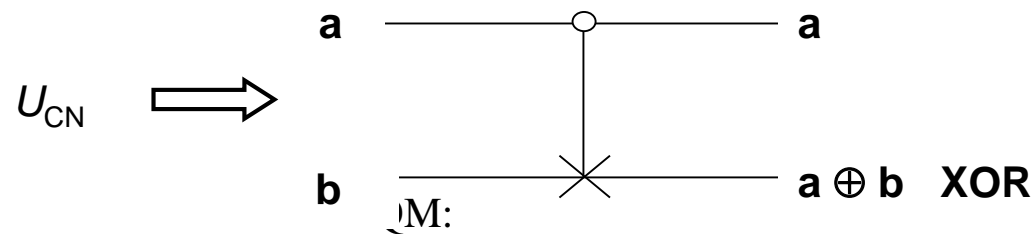
The diagram shows a central black dot labeled  $\pi^0$ . Two horizontal arrows originate from this dot: one pointing to the left towards the label  $e^+$ , and one pointing to the right towards the label  $e^-$ .

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left[ |\uparrow\rangle_1 |\downarrow\rangle_2 - |\downarrow\rangle_1 |\uparrow\rangle_2 \right]$$

- EPR were concerned with existence of "independent reality"
  - Bohr just said must consider whole system, even if separated
- Spooky 'faster than light' effects?
- Bell showed spin correlations predicted QM are not consistent with local, causal hidden variable theories
- Aspect's experiments (1981-2) support QM

# EPR and Quantum Entanglement (2)

Consider quantum CN gate



So:

$$|a\rangle |b\rangle \rightarrow |a\rangle |a \oplus b\rangle$$

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



Entangled or EPR state

# Quantum No Cloning Theorem

Wooters & Zurek 1982

An unknown quantum state cannot be cloned

⇒ Impossible to generate copies unless state already known

Proof: Suppose  $U_c$  is unitary cloning operator

$$U_c(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$$

$$U_c(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$$

But if

$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$$

$$U_c(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle$$

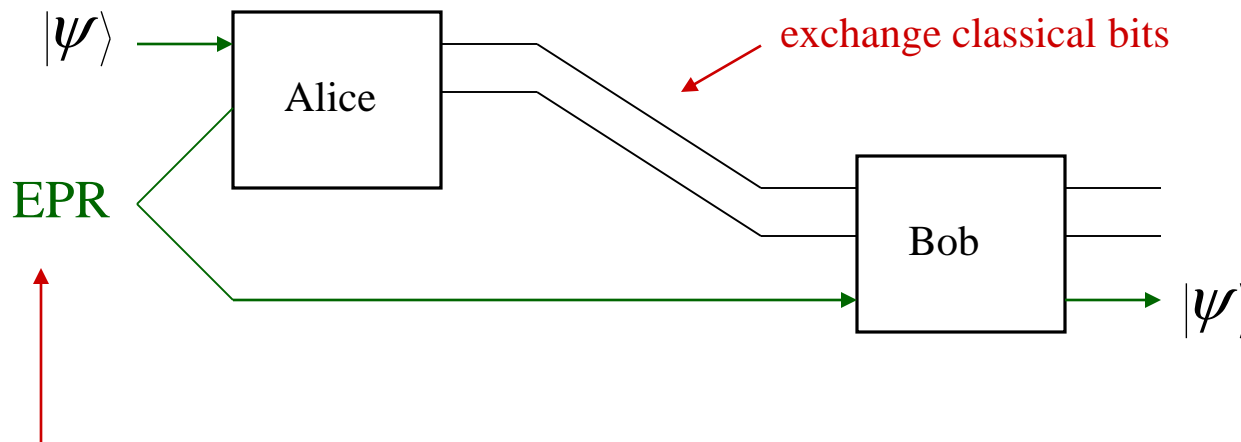
Conclude no operator  $U_c$  exists

# EPR and Quantum Entanglement (3)

Teleportation uses Quantum Entanglement as a Tool

Example: Quantum Teleportation (Bennett et al. 1982)

It is possible to transmit qubits without sending qubits!



Alice & Bob share EPR pair in advance

# Quantum Software

EE Times, November 24, 1999:

- IBM Almaden Research Laboratory, working with Microsoft Corporation scientists, have devised a way to create one-use only software by exploiting quantum states
- The act of using the software would alter the quantum states and thus destroy the software

“that’s why Microsoft were involved”

# Quantum Algorithms (1)

Many varieties of Turing Machine

e.g.     Deterministic TM     (DTM)  
          Probabilistic TM     (PTM)  
          Quantum TM         (QTM)

Many varieties of classical complexity classes

e.g.     Solve                 - with certainty in worst case     P  
          problem             polynomial time  
                               - with certainty in average case  
                               polynomial time             ZPP  
                               - with probability  $> 2/3$  in worst  
                               case polynomial time         BPP

Quantum analogues     QP, ZQP, BQP



# Quantum Algorithms (2)

Can a QTM beat a DTM and a PTM?

Bernstein & Vazirani (1993)

QTM can sample Fourier spectrum of Boolean function on  $n$  bits in polynomial time - not known for PTM

Berthiaume & Brassard (1994)

Showed decision problem soluble in polynomial time by QTM but exponential for DTM or PTM

Shor (1994)

Discovered polynomial time algorithms for factoring and discrete log (class BQP)

# Quantum Algorithms (3)

To date, about 6 significant quantum algorithms known

- Deutsch-Josza - True statement problem
- Shor - Factoring
- Kitaev - Factoring
- Grover - Database searching
- Grover - Estimating median
- Durr-Hoyer - Estimating mean

# Summary of Lecture #1

- Idea of new 'non-Turing' computer
- Shor's Quantum Factoring
- Quantum Superposition
- Quantum Entanglement
- Teleportation and Entanglement
- Quantum Algorithms