Frequently Asked Questions about

Quantum Computation & Quantum Information

Mahn-Soo Choi (Korea University)

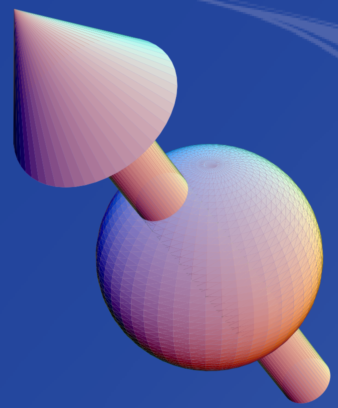
What is a quantum computer/machine?

A computer with quantum bits (qubits),

... and working in a fundamentally different way.

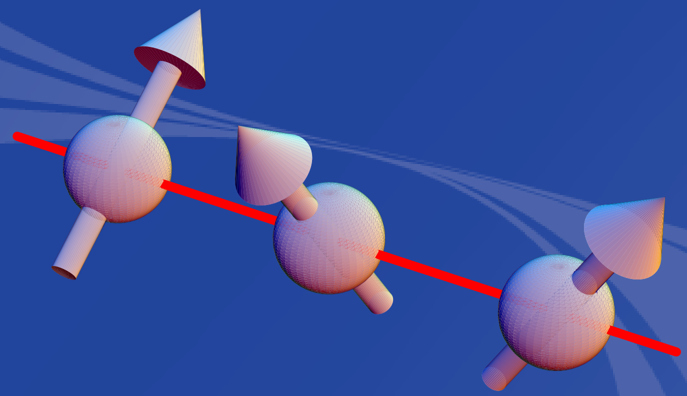
What is a quantum bit (“qubit”)?

A quantum-mechanical two-level system,



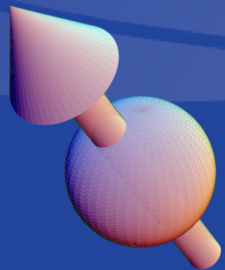
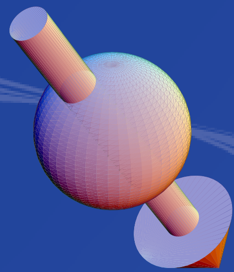
... which should be controllable.

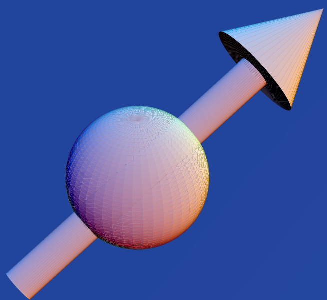
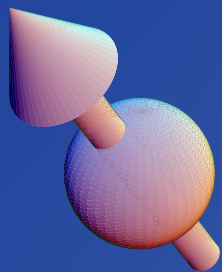
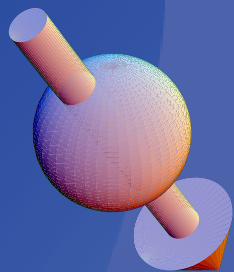
Qubits should interact with each other in a controllable way!



$$\mathscr{H}_{\mathrm{QC}} = \sum_i \frac{1}{2}\mathbf{B}_i \cdot \mathbf{S}_i + \sum_{i<j} \frac{1}{2} J_{ij}^{\perp} \left[S_i^+ S_j^- + S_i^- S_j^+ \right] + \sum_{i<j} J_{ij}^z S_i^z S_j^z$$

How different is a qubit from a classical bit?

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

 $=$  $+$  $= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$

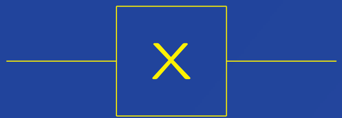
How does a quantum computer work?

Elementary Gates

- Hadamard gate

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = R_y(\pi/2)\sigma_z$$

- Pauli-X,Y,Z gates



$$= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

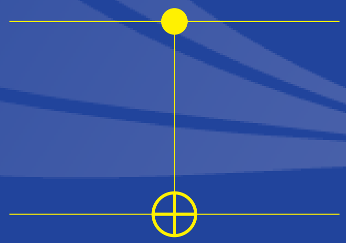
- Phase gates

$$-\boxed{\phi}- = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$$

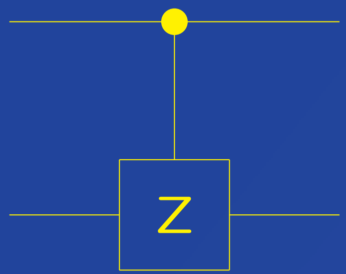
$$-\boxed{\mathsf{S}}- = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$-\boxed{\mathsf{T}}- = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

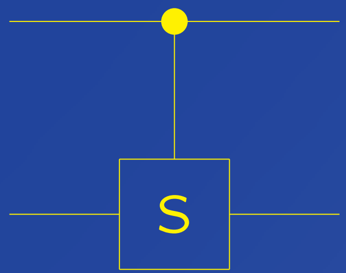
- controlled-NOT, controlled-Z, controlled-phase gates



$$= \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix}$$

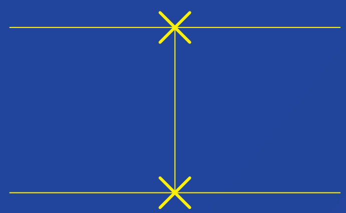


$$= \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix} = [\mathbf{1} \otimes H]\, U_{\mathsf{CNOT}}\, [\mathbf{1} \otimes H]$$



$$= \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & i \end{bmatrix}$$

- Swap gate



$$= \begin{bmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{bmatrix}$$

What is quantum computation?

And how can you implement it physically?

$$U = \exp\left(-\frac{i}{\hbar}\mathscr{H}\tau_{\mathrm{op}}\right), \quad i\hbar\frac{d}{dt}|\psi\rangle = \mathscr{H}|\psi\rangle$$

Why is it faster? Or is it faster?

Deutsch (1985) Problem:

"Can we know whether $f(x)$ is *constant* or *balanced* by running the black box *only once*?"

Quantum parallelism

For computational basis state $(|x\rangle, |y\rangle = |0\rangle, |1\rangle)$,

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

$$U_f : \begin{pmatrix} \mathbb{I} & \\ & \mathbb{I} \end{pmatrix}, \quad \begin{pmatrix} \sigma_x & \\ & \sigma_x \end{pmatrix}, \quad \begin{pmatrix} \mathbb{I} & \\ & \sigma_x \end{pmatrix}, \quad \begin{pmatrix} \sigma_x & \\ & \mathbb{I} \end{pmatrix}$$

For superposition states, $|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$,

$$|+\rangle\,|-\rangle = \frac{1}{2}(|0\rangle\,|0\rangle - |0\rangle\,|1\rangle + |1\rangle\,|0\rangle - |1\rangle\,|1\rangle)$$

$$U_f : |+\rangle\,|-\rangle \mapsto \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle\right] \otimes |-\rangle$$

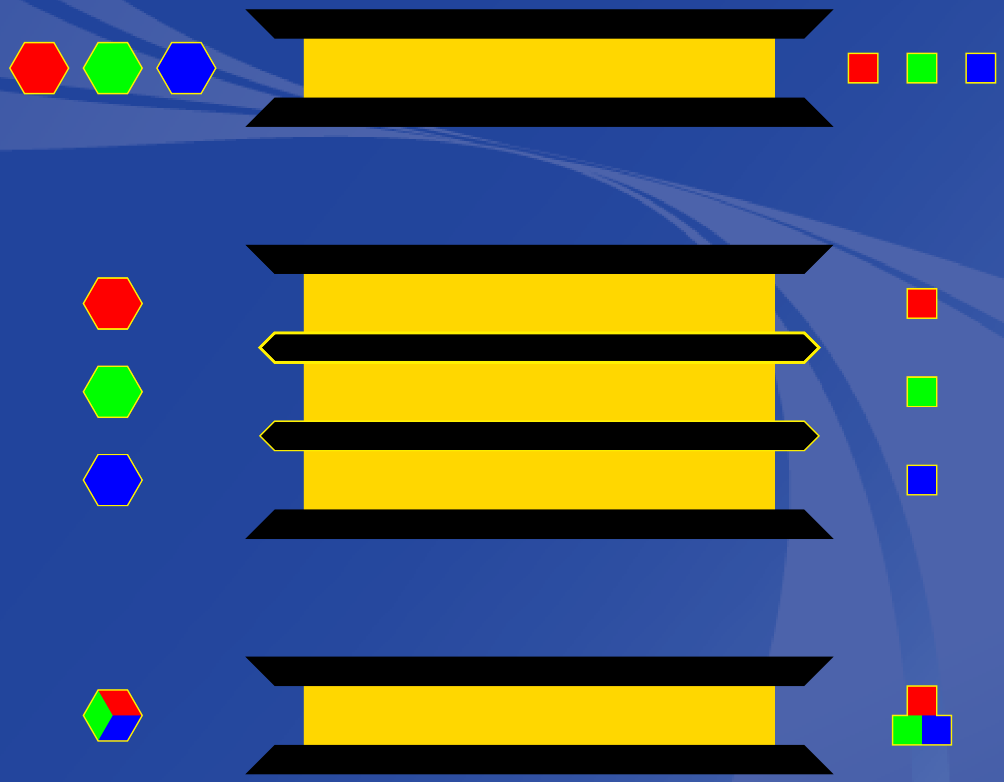
$$= (-1)^{f(0)} \begin{cases} |+\rangle\,|-\rangle\,, & f(0) = f(1) \\ |-\rangle\,|-\rangle\,, & f(0) \neq f(1) \end{cases}$$

Experimental demonstration

by Chuang *et al.* (1998) using NMR.

So, WHY is it faster?

(Or, what is "quantum parallelism"?)



$$f(a\,|0\rangle + b\,|1\rangle) := a\,|f(0)\rangle + b\,|f(1)\rangle$$

Is it always faster?

No!

There is only one quantum algorithm (Shor's factorization algorithm) that is known to be exponentially faster than any classical algorithm.


Shor (1994)

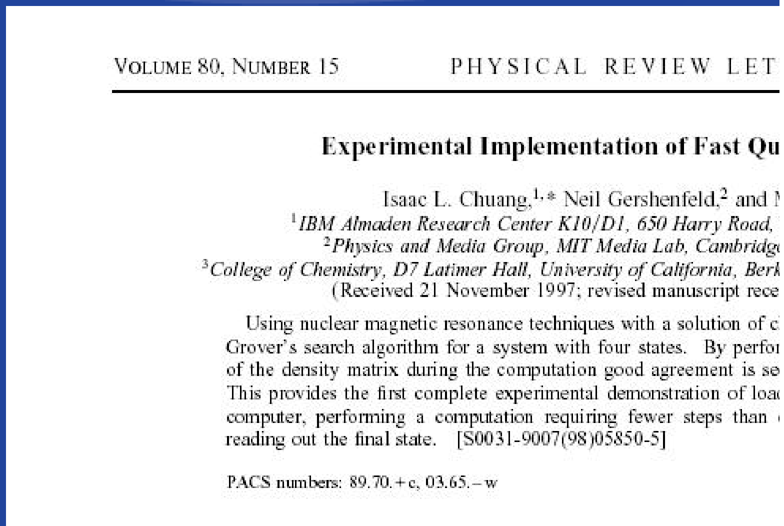
What will quantum computers be good at?

These are the most important applications currently known:

- Cryptography – perfectly secure communication.
- Searching, especially algorithmic searching (Grover's algorithm).
- Factorization of large numbers (Shor's algorithm).
- Simulations of quantum many-body systems.

Is it possible to build a quantum computer?

Quantum computers have already been built,



VOLUME 80, NUMBER 15 PHYSICAL REVIEW LET

Experimental Implementation of Fast Qu

Isaac L. Chuang,[1,*] Neil Gershenfeld,[2] and N

[1]*IBM Almaden Research Center K10/D1, 650 Harry Road,*

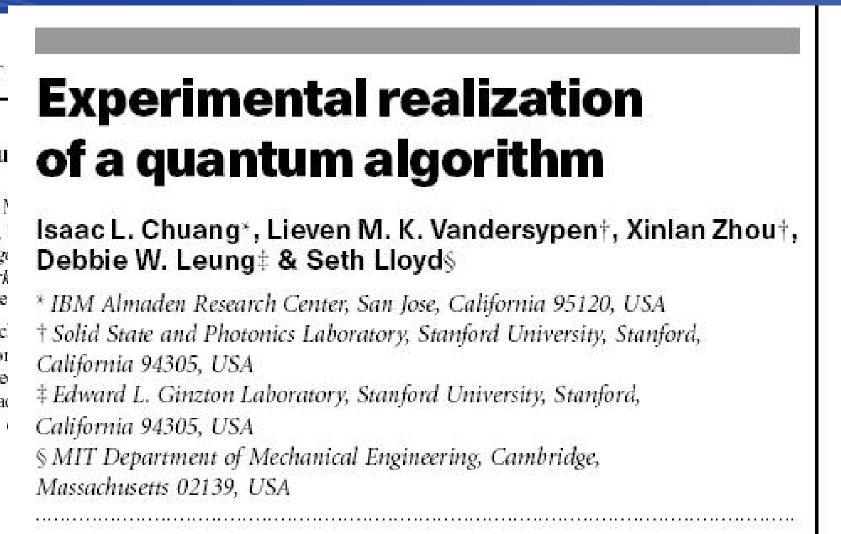
[2]*Physics and Media Group, MIT Media Lab, Cambridg*

[3]*College of Chemistry, D7 Latimer Hall, University of California, Berk*

(Received 21 November 1997; revised manuscript rece

Using nuclear magnetic resonance techniques with a solution of c Grover's search algorithm for a system with four states. By perfo of the density matrix during the computation good agreement is se This provides the first complete experimental demonstration of loa computer, performing a computation requiring fewer steps than reading out the final state. [S0031-9007(98)05850-5]

PACS numbers: 89.70.+c, 03.65.–w



Experimental realization of a quantum algorithm

Isaac L. Chuang*, Lieven M. K. Vandersypen†, Xinlan Zhou†, Debbie W. Leung‡ & Seth Lloyd§

* *IBM Almaden Research Center, San Jose, California 95120, USA*

† *Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305, USA*

‡ *Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA*

§ *MIT Department of Mechanical Engineering, Cambridge, Massachusetts 02139, USA*

and are working "properly". But, ...

Why don’t we use the quantum computers?

Currently working quantum computers only have less than 10 qubits.

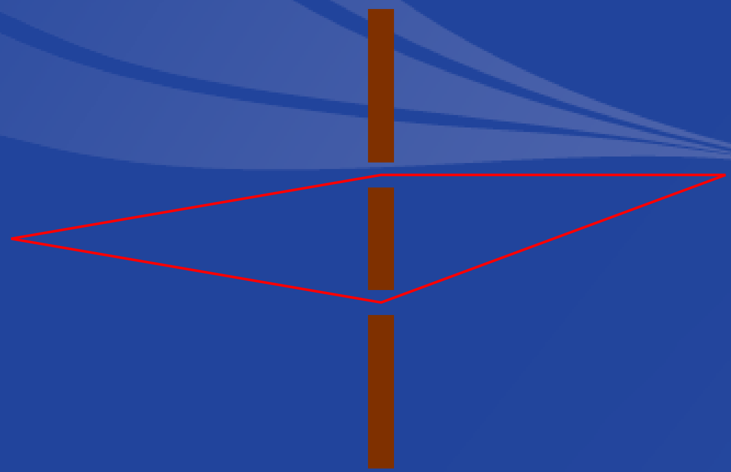
What makes it difficult to build a practical quantum computer?

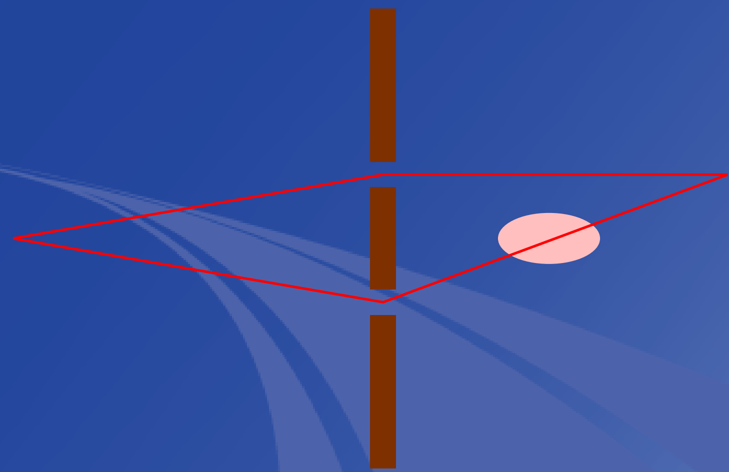
Decoherence!

Without coherence, qubits behave just like classical bits!

No quantum parallelism! No entanglement!

What is "decoherence" ("dephasing")?





$$\psi_1 \propto \sin\left(2\pi\frac{L_1}{\lambda} - \omega t\right), \qquad \psi_1 \propto \sin\left(2\pi\frac{L_1}{\lambda} - \omega t\right),$$

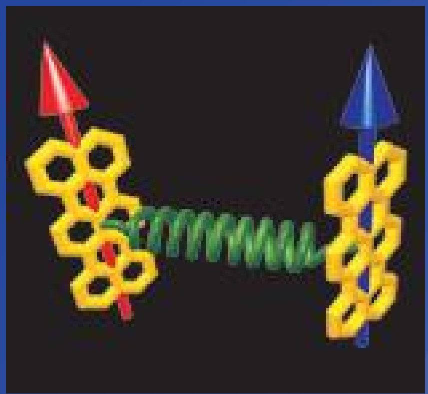
$$\psi_2 \propto \sin\left(2\pi\frac{L_2}{\lambda} - \omega t\right), \qquad \psi_2 \propto \sin\left(2\pi\frac{L_2}{\lambda} - \omega t + \phi\right),$$

$$\langle|\psi|^2\rangle \propto 2\cos^2\left(\pi\frac{\Delta L}{\lambda}\right) \qquad \langle|\psi|^2\rangle \propto \int d\phi\, 2\cos^2\left(\pi\frac{\Delta L}{\lambda} - \frac{\phi}{2}\right)$$

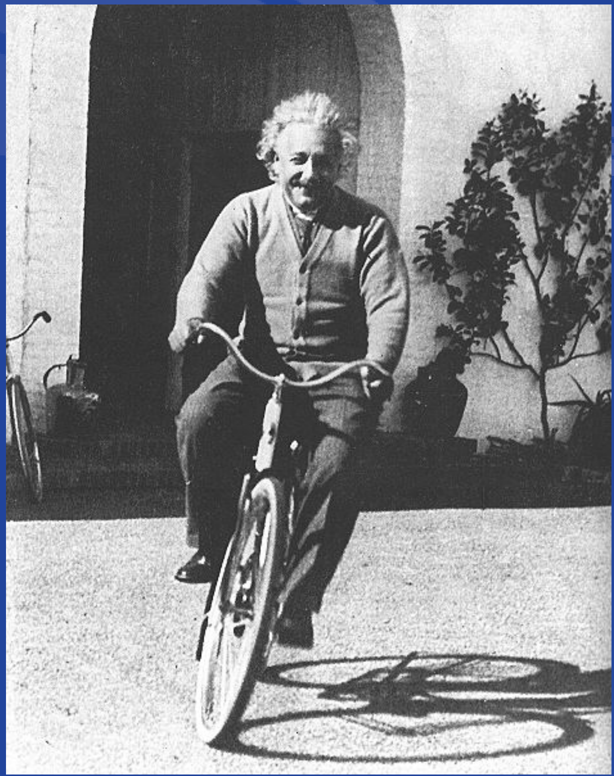
What is entanglement?

A quantum state whose wave function cannot be written as a product of individual wave functions:

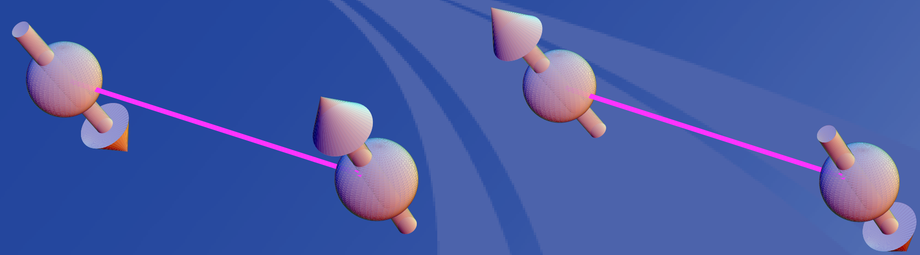
$\|\uparrow\rangle \otimes \|\downarrow\rangle$	separable ,
$(\|\uparrow\rangle + \|\downarrow\rangle) \otimes (\|\uparrow\rangle - \|\downarrow\rangle)$	separable ,
$\|\uparrow\rangle \otimes \|\downarrow\rangle + \|\downarrow\rangle \otimes \|\uparrow\rangle$	entangled!!



And, what is special about it?



Non-locality!



- Einstein *et al.* (1935)
- Bell (1965)

What is it useful for?

- Quantum computation – it is generally believed that entanglement is essential for the exponential speed-up.
- Cryptography (key distribution, etc.)
- Quantum teleportation

What is “quantum teleportation”?

- Goal. Can we use classical information to realize transmission of quantum information? Say, Bob has a qubit, but he doens’t know its state. There’s no quantum channel available.
- Problem. Bob cannot measure his qubit; single measurement on a single qubit does not give any information of the quantum state.

B.E. = Bell entangler

B.M. = Bell measurement

$U = 1_A$, σ_A^x, σ_A^y, or σ_A^z

At time $t = t_1$, an entangled pair is prepared and shared between Alice (A) and Bob (B):

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\}$$

At time $t = t_2$, Bob has a particle C in an unknown state

$$|\psi\rangle_C = a\,|0\rangle_C + b\,|1\rangle_C \,.$$

The total wave function at this moment is given by

$$|\Psi\rangle_{ABC} = |\phi^+\rangle_{AB} \otimes |\psi\rangle_C$$

$$|\Psi\rangle_{ABC} = \frac{1}{2}\Big\{ |\psi\rangle_A \otimes |\phi^+\rangle_{BC} + \sigma_1\,|\psi\rangle_A \otimes |\psi^+\rangle_{BC}$$

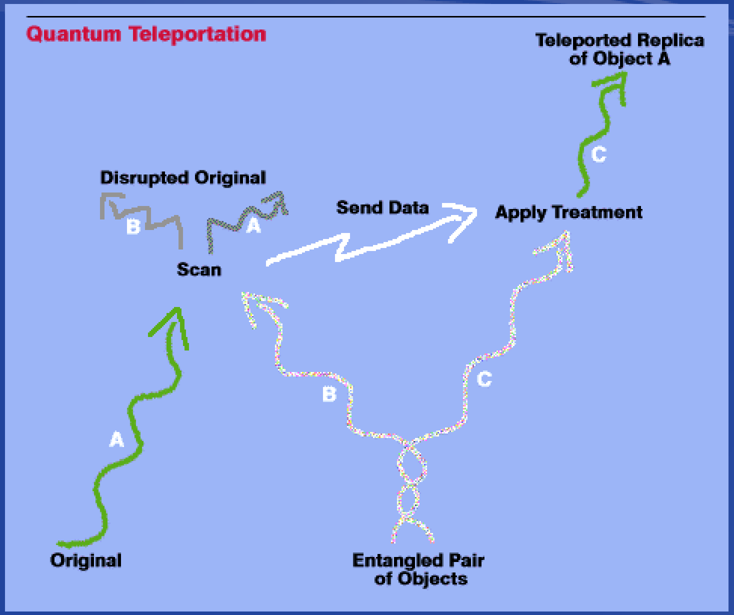
$$+ (-i\sigma_2)\,|\psi\rangle_A \otimes |\psi^-\rangle_{BC} + \sigma_3\,|\psi\rangle_A \otimes |\phi^-\rangle_{BC} \Big\},$$

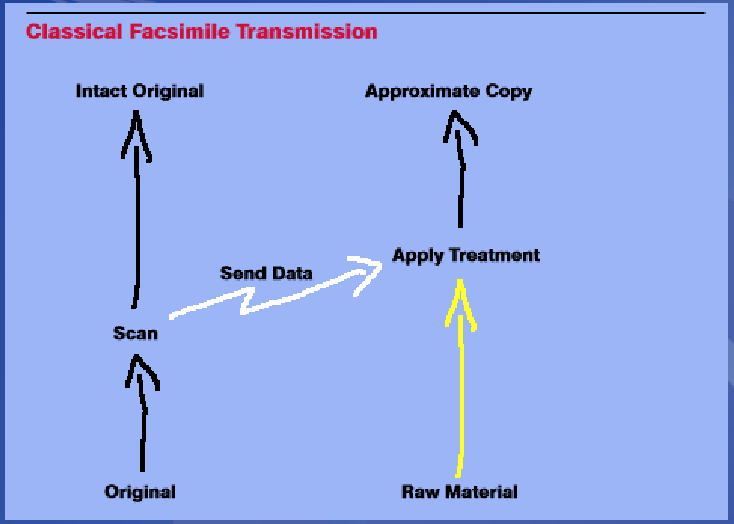
At $t = t_3$, Bob performs a *Bell measurement*. Then the total wave function *collapses* to one of the four states with equal probability

$$|\Psi\rangle_{ABC} = |\psi\rangle_A \otimes |\phi^+\rangle_{BC}$$
$$|\Psi\rangle_{ABC} = \sigma_1 |\psi\rangle_A \otimes |\psi^+\rangle_{BC}$$
$$|\Psi\rangle_{ABC} = -i\sigma_2 |\psi\rangle_A \otimes |\psi^-\rangle_{BC}$$
$$|\Psi\rangle_{ABC} = \sigma_3 |\psi\rangle_A \otimes |\phi^-\rangle_{BC}$$

Bob tells Alice of his measurement result.

How different is it from classical FAX?





Where can I get more information about quantum computation and quantum information?

Google, for "quantum computer".

http://www.qubit.org/ (Oxford University, UK)

...

Bell, J. S., “??” Physics (N.Y.) **1**, 195 (1965).
Chuang, I. L., L. M. K. Vandersypen, X. Zhou, D. W. Leung, & S. Lloyd, “Experimental realization of a quantum algorithm,” Nature (London) **393**, 143 (1998).
Deutsch, D., “Quantum theory, the Church-Turing principle and the universal quantum computer,” Proc. R. Soc. London A **400**, 97 (1985).
Einstein, A., B. Podolsky, & N. Rosen, “??” Phys. Rev. **47**, 777 (1935). The use of composite spin-1/2 systems to illustrate the Einstein-Podolsky-Rosen paradox started with **?**.
Shor, P. W., “??” in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, CA, 1994), p. 124.