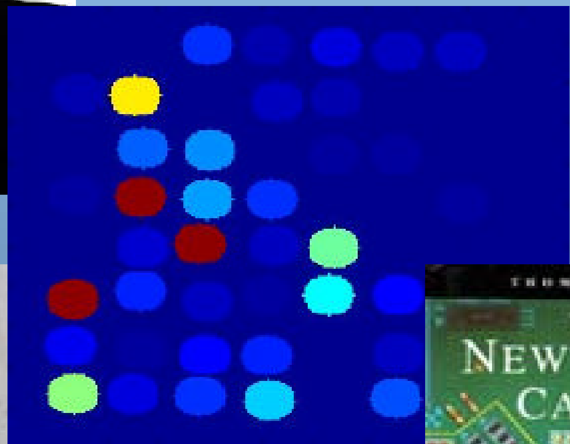
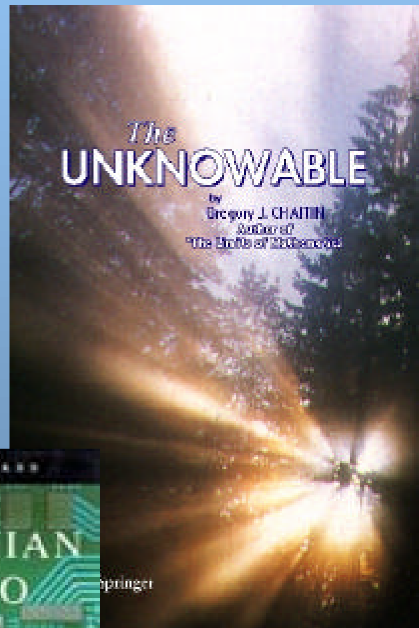
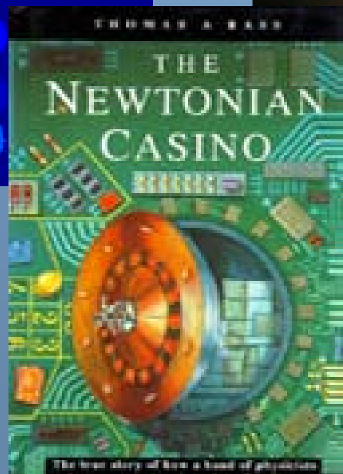
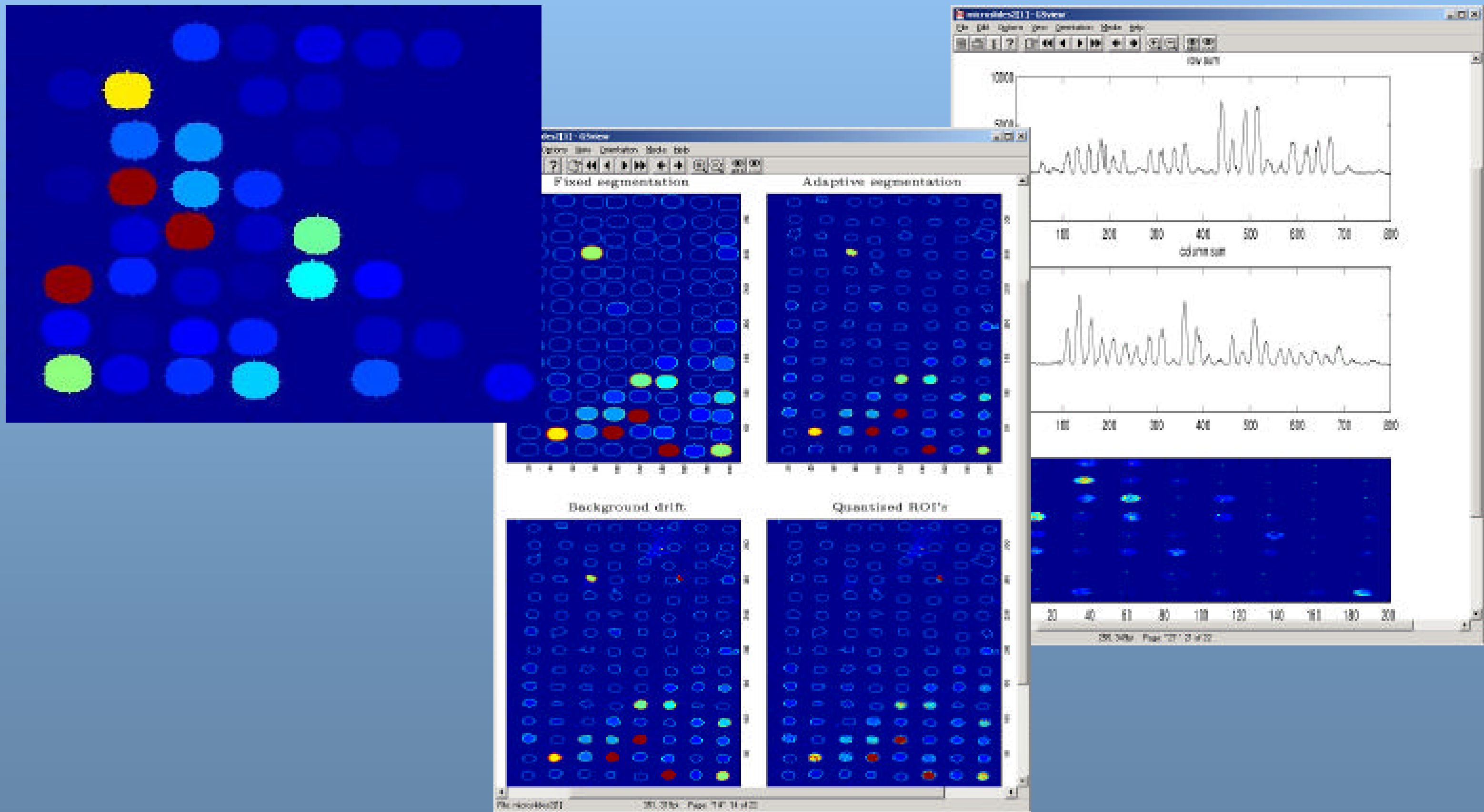
"Year 2020" -Topics in Information Theory for Further Studies







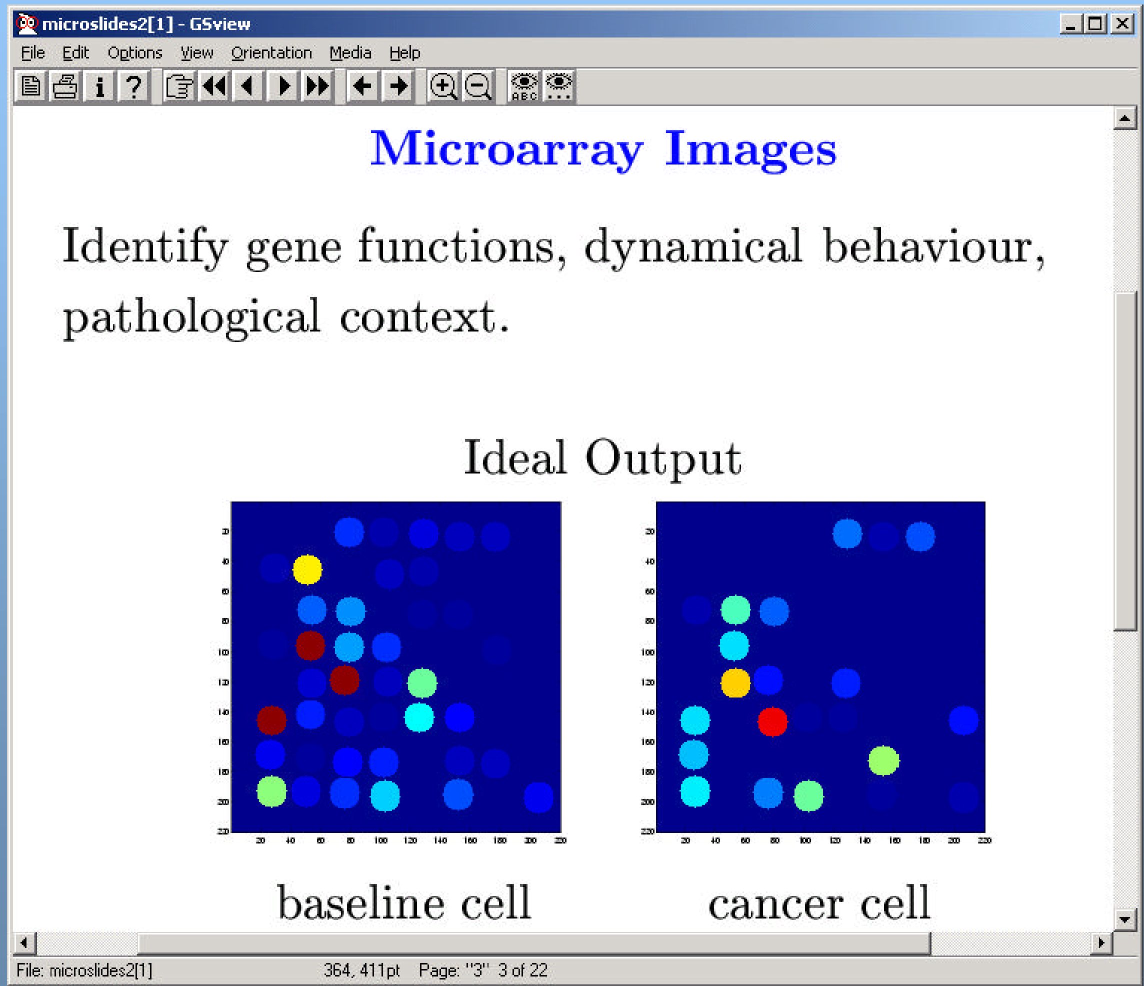
Comprestimation



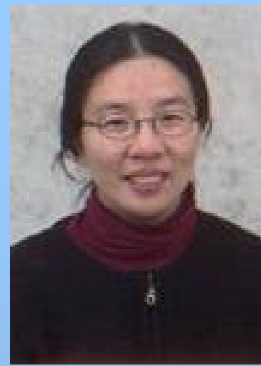
Compresstimation

- lossy compression of ”non-natural” images (regular lossy compression uses MSE)
- compression of images so that the statistical inferences on the compressed images remain valid
- E.g. compression of microarray images

Microarray images



Comprestimation cont.



- also known as ”Multi-terminal data compression”
- T. Han & S.Amari; R. Jörnsten & B. Yu;

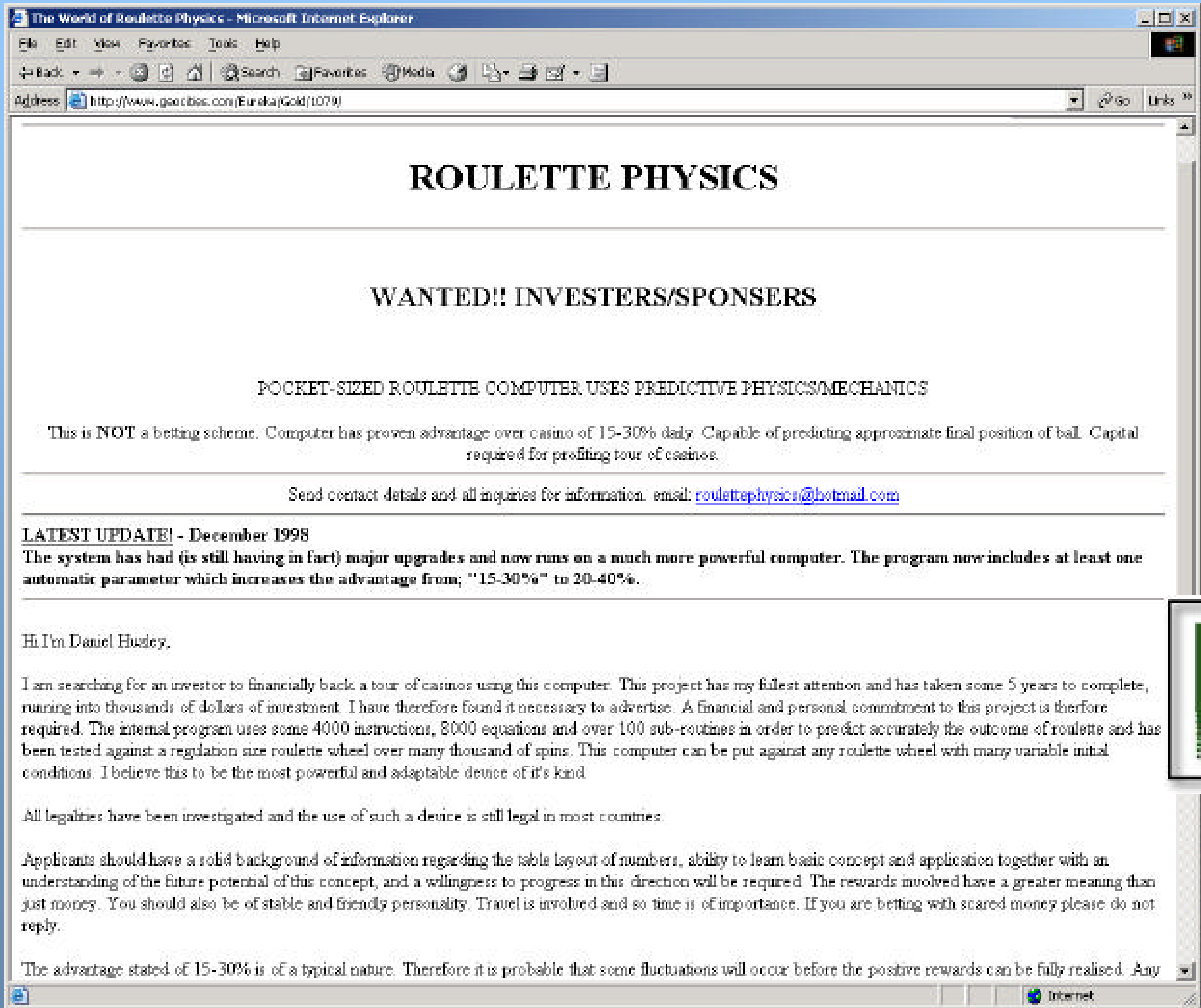
Algorithmic Information Theory

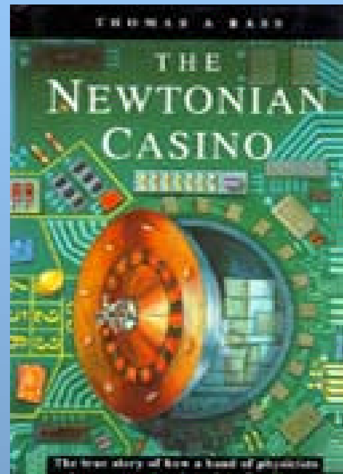
Algorithmic Information Theory

- …as used by Chaitin for ”meta-mathematics”
- incompleteness theorems
  - ✓Gödel (logic)
  - ✓Turing (algorithm)
  - ✓The Halting Probability Omega (information, randomness)

http://www.umcs.maine.edu/~chaitin/

Physics, information and games

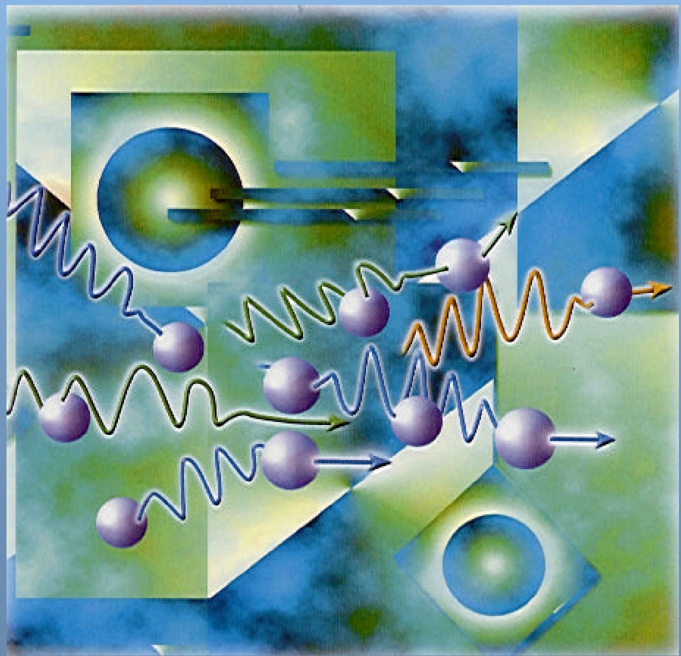




PREDICTION
COMPANY

2020: Quantum Odyssey

"On Quantum Computing and information transmission"



Motivation

- Computers as physical systems
- Technological issues
  - ✓miniaturization and speedup - Moore's law
  - ✓need for energy efficiency

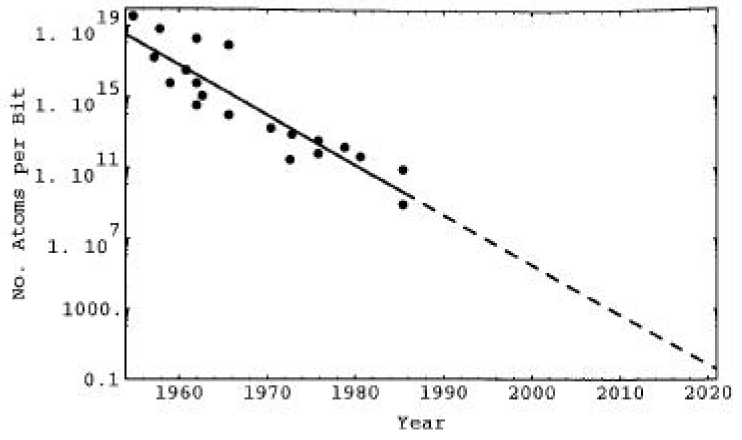


Fig. 1.1 The number of atoms needed to represent one bit of information as a function of calendar year. As the vertical axis is on a logarithmic scale, the straight line fit suggests the trend is exponential. Extrapolation of the trend suggests that the one-atom-per-bit level is reached in about the year 2020. Adapted from [Keyes88].

Why would we bother?

- Cryptography: QC can break RSA codes
- Communication of messages that betray the presence of eavesdropping
- Teleportation: moving qubits around without having them ever being transmitted over an insecure channel

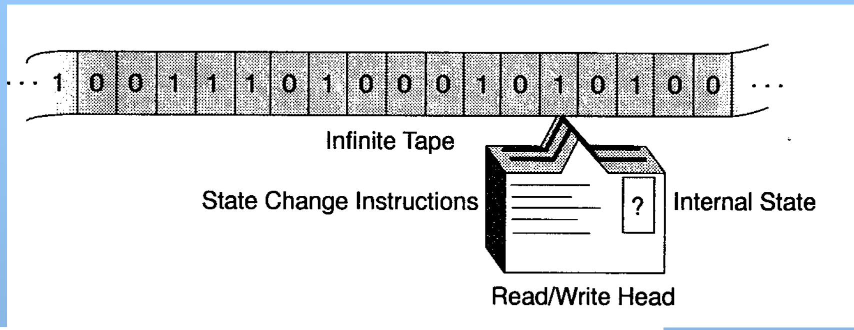
Central concepts

- Superposition: a “blend” of 0 and 1 simultaneously, i.e., quantum parallel mode
- Reversible computing: logical irreversibility implies thermodynamic irreversibility (i.e., heat dissipation)

Charles Bennett

The Capabilities of Computers

(Deterministic)
Turing Machine



Probabilistic
Turing Machine

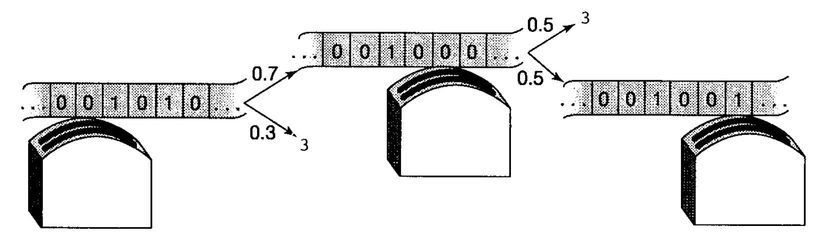


Fig. 2.2 In a probabilistic classical Turing machine there are multiple possible successor states, only one of which is actually selected. Unselected paths are terminated (×). The probabilities of transitioning between various states are shown. Notice that the sum of the probabilities on all the paths emanating from a state is 1.

Quantum
Turing Machine

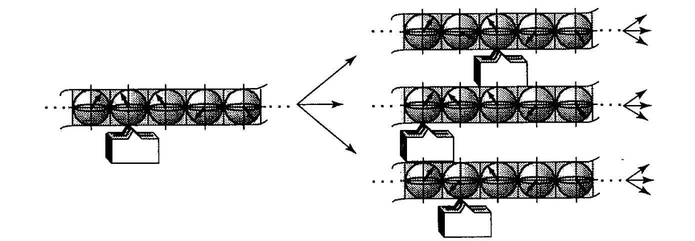
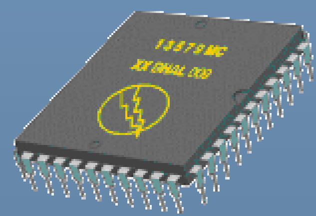


Fig. 2.3 In the quantum Turing machine each cell on the tape can hold a qubit whose state is represented as an arrow contained in a sphere. All paths are pursued simultaneously. Instead of probabilities on each path we now have amplitudes. Amplitudes are complex numbers whose square moduli are probabilities.

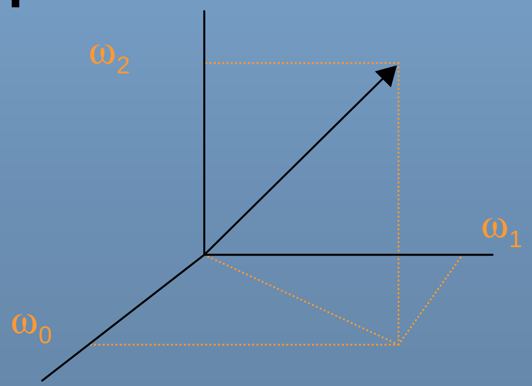
Proving vs. providing proof

- QTM can simulate a TM - QTM universal
- TM provides a proof as the sequence of steps performed
- QTM can provide an answer without a proof trace (worse: if you try to “peek” QTM that would disrupt the proof!)



Bits and Qubits

- Each bit is represented by the state of a simple 2-state quantum system e.g., spin state)
- We need finite dimensional Hilbert space



"Complex linear vector space"

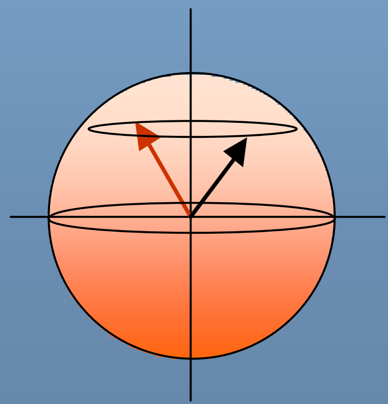
Bra-ket

- For a simple two-state system you can write the state as a “ket (vector)”

$$|\psi\rangle = w_0|\psi_0\rangle + w_1|\psi_1\rangle \equiv \begin{pmatrix} w_0 \\ w_1 \end{pmatrix}$$

- Probability interpretation

$$P(\text{system in state } |\psi_i\rangle) = \frac{|w_i|^2}{\sum_{i=0}^{n-1} |w_i|^2}$$



Unitary operators

- 2-state system has 2 eigenstates called $|\psi_0>$ and $|\psi_1>$ (basis)

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|y\rangle = w_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + w_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} w_0 \\ w_1 \end{pmatrix}$$

Unitary operators continued

- To change the quantum world one needs an operator, e.g. NOT

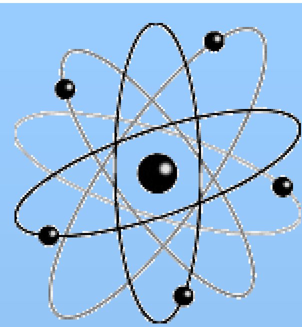
$$\mathrm{NOT}\,|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle,$$

$$\mathrm{NOT}\,|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

NOT is reversible!

- One can also have non-classical gates such as $\sqrt{\mathrm{NOT}}$

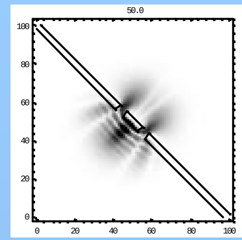
Universality



- In classical computation AND and NOT are enough to build any circuit
- In quantum computing it is enough to use a 2-qubit gate (Barenco et al)

$$\hat{A}(f,a,q) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{ia}\cos(q) & -ie^{i(a-q)}\sin(q) \\ 0 & 0 & -ie^{i(a+q)}\sin(q) & e^{ia}\cos(q) \end{pmatrix}$$

Fundamentals



- One can have quantum interference whenever there is more than one way of obtaining a particular result
- measuring a quantum system:
  - ✓ if the system is in eigenstate the outcome is one of the eigenvalues
  - ✓ if the system is in superposition state the result is given by

$$P(\text{system in state } | y_i \rangle) = \frac{|w_i|^2}{\sum_{i=0}^{n-1} |w_i|^2}$$

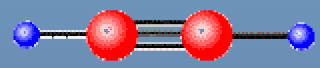
“A good quantum calculation”

- Create a superposition of register elements
- Calculate in “one shot” all function values F(j)
- Do something clever with all the F(j) values

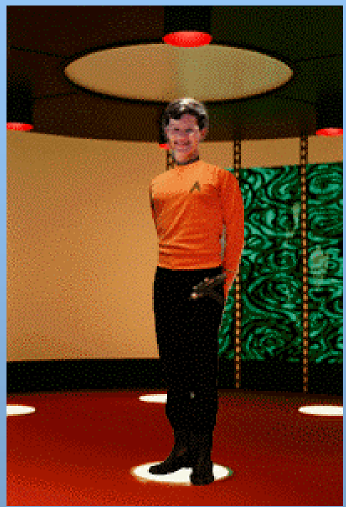
(Use **interference** to increase the amplitudes and thus probabilities of the solution states)

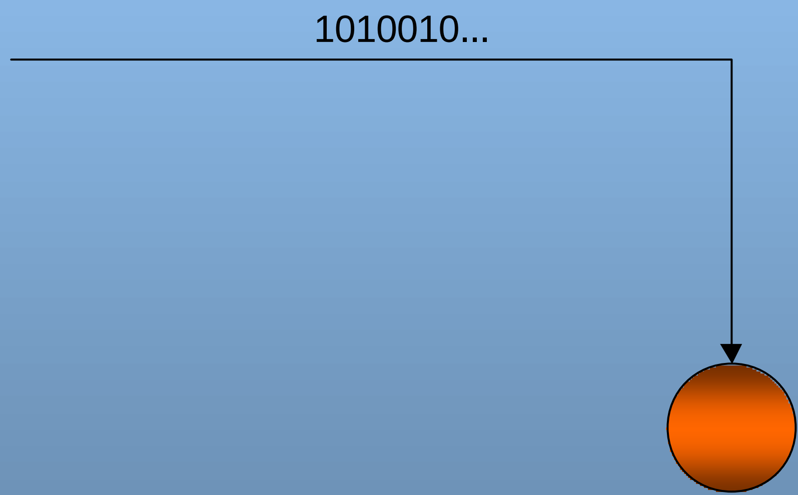
Quantum entanglement (EPR)

- If two systems (particles) are "Quantum correlated" one talks about entanglement
- For entangled particles their joint state is not factorizable as the direct product of two simpler states
- Produced by conservation of some attribute



Teleportation





- dissociation
- information transmission
- reconstitution

Well, at least a qubit ...

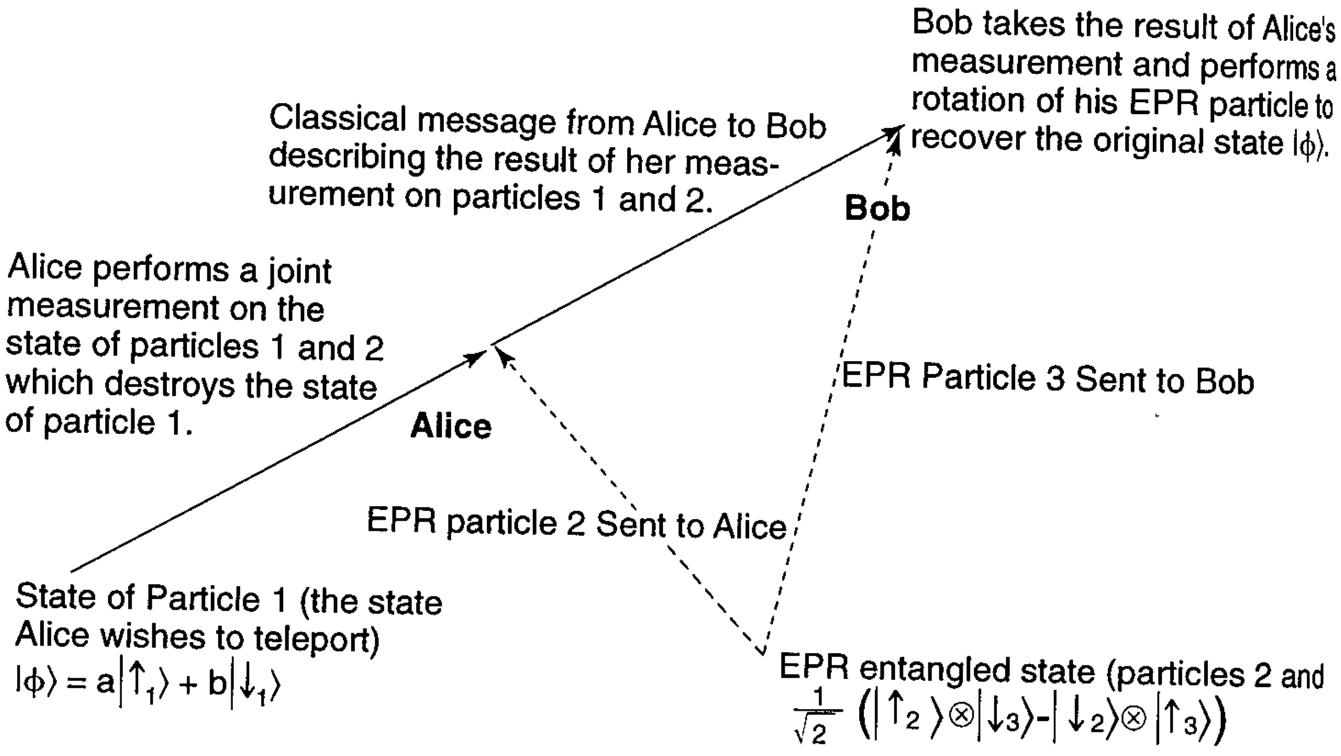


Fig. 9.5 Schematic view of quantum teleportation using EPR.