Short Course in Quantum Information

Prof. Ivan H. Deutsch

Dept. of Physics and Astronomy

Center for Advanced Studies

University of New Mexico

Information Physics Group: http://info.phys.unm.edu

Course Info

- All materials downloadable @ website

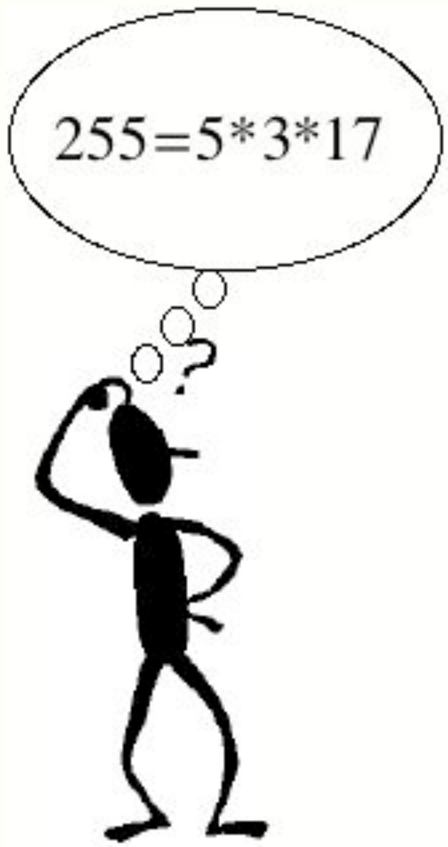
http://info.phys.unm.edu/~deutschgroup/DeutschClasses.html

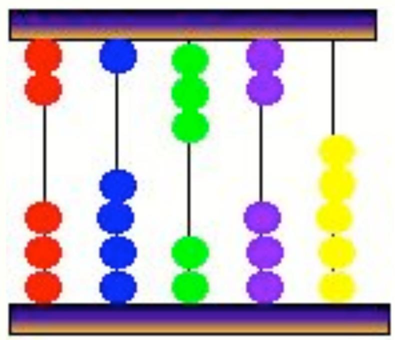
- Syllabus

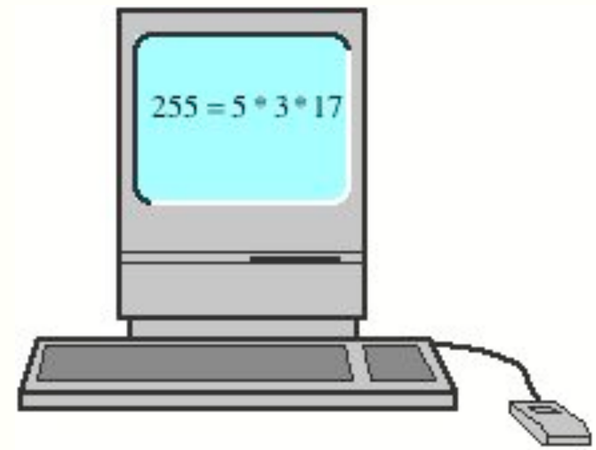
Lecture 1: Intro
Lecture 2: Formal Structure of Quantum Mechanics
Lecture 3: Qubits
Lecture 4: Entanglement
Lecture 5: Algorithms
Lecture 6: Error Correction
Lecture 7: Physical Implementations
Lecture 8: Quantum Cryptography

Why is a Physicist Talking About Information?

Information is Physical

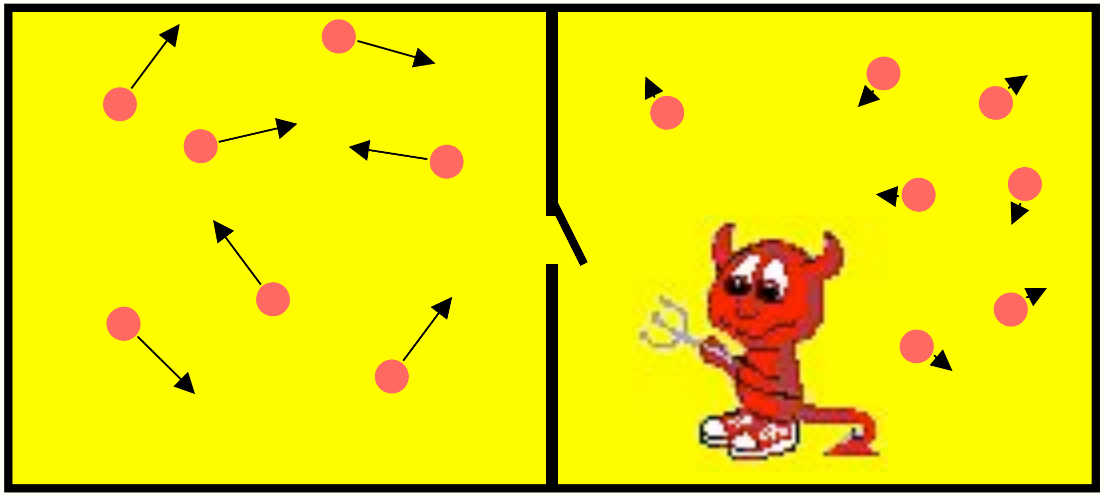






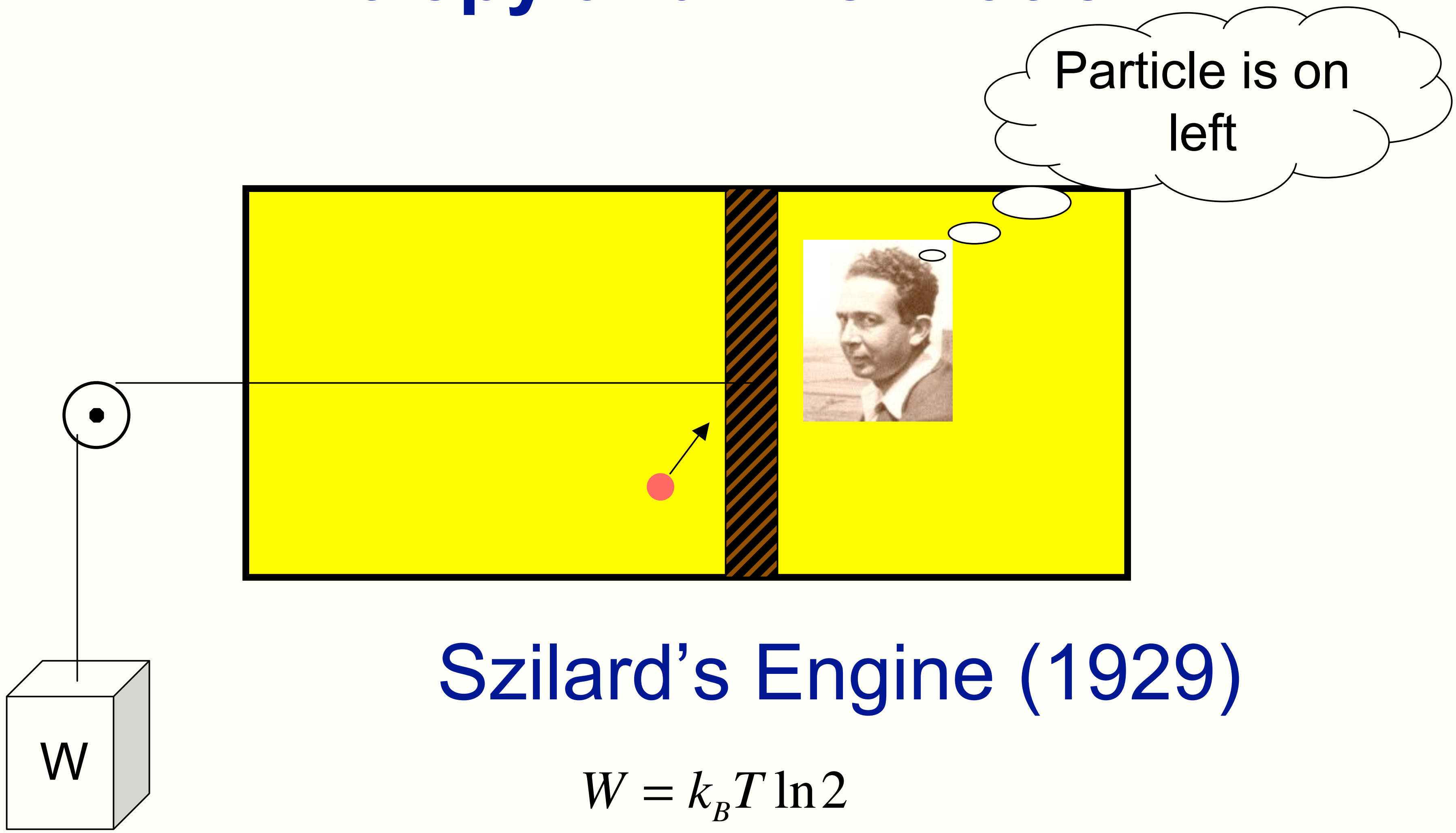
Any computation is constrained by the physical laws governing the "machine" that carries out the operations.

Entropy and Information



Maxwell's Demon (1867)

Entropy and Information



Szilard's Engine (1929)

$$W = k_B T \ln 2$$

Bennett
(1982)

Landauer
(1961)

Benioff
(1985)

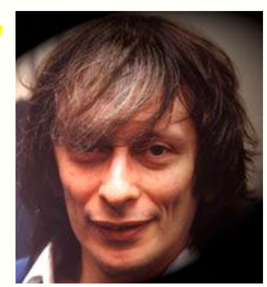
Thermodynamics/reversible computing

Quantum Simulations

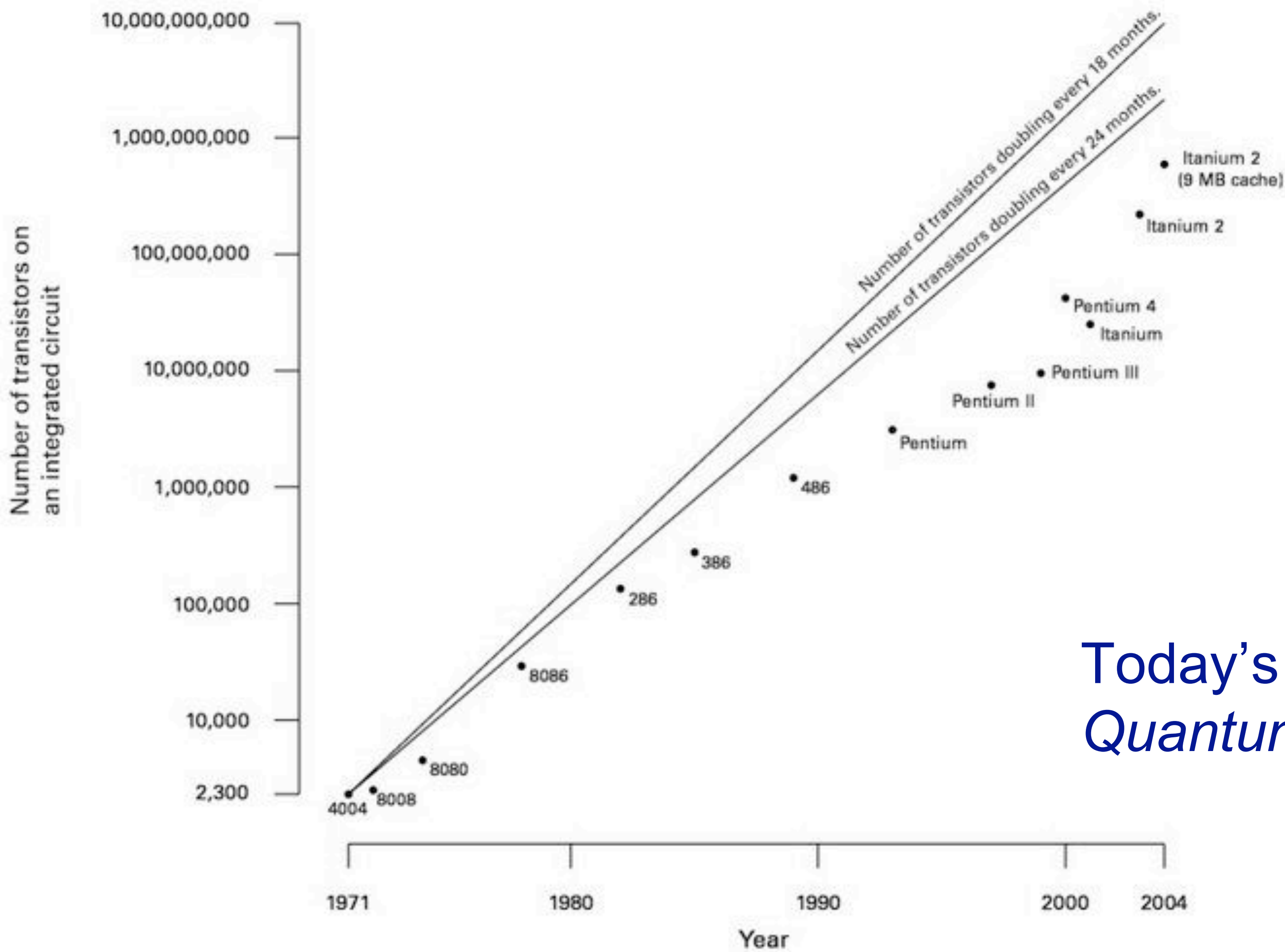
Universal quantum circuit model

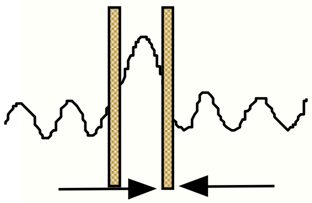
Feyman
(1982)

Deutsch
(1985)



Moore's Law





Today's worry:
Quantum uncertainty

What is Information?


WHEEL OF FORTUNE


A
E
O
EVENT


WHEEL OF FORTUNE


Q
Z
W
EVENT

Information = What we know.

Bayesian view of probabilities: $P\left(x|y\right)$

Prior information

Logic and probability of alternatives:

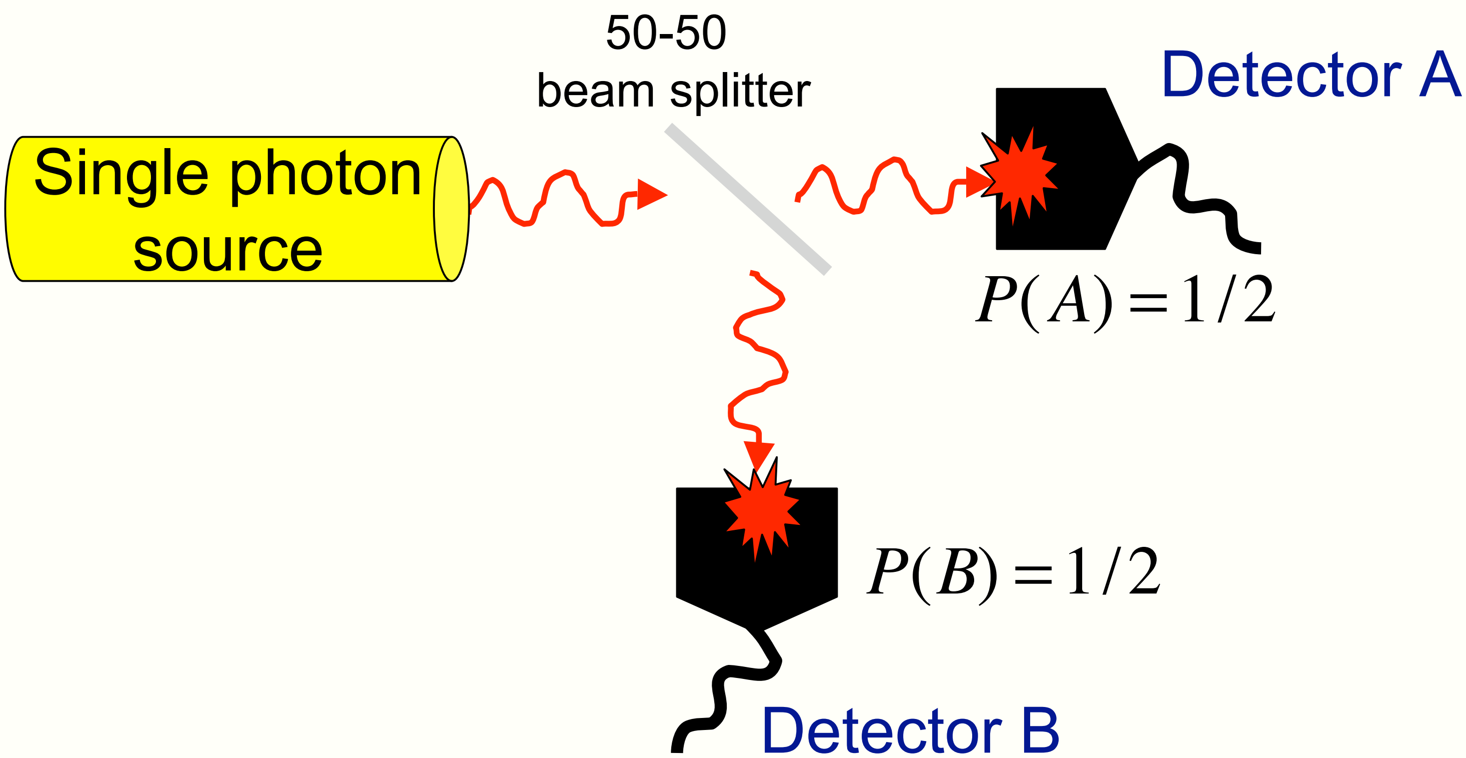
$$P(x) = P\left(x|y_1\right)P(y_1) + P\left(x|y_2\right)P(y_2)$$

Bayes Rule - Updating probabilities given new information:

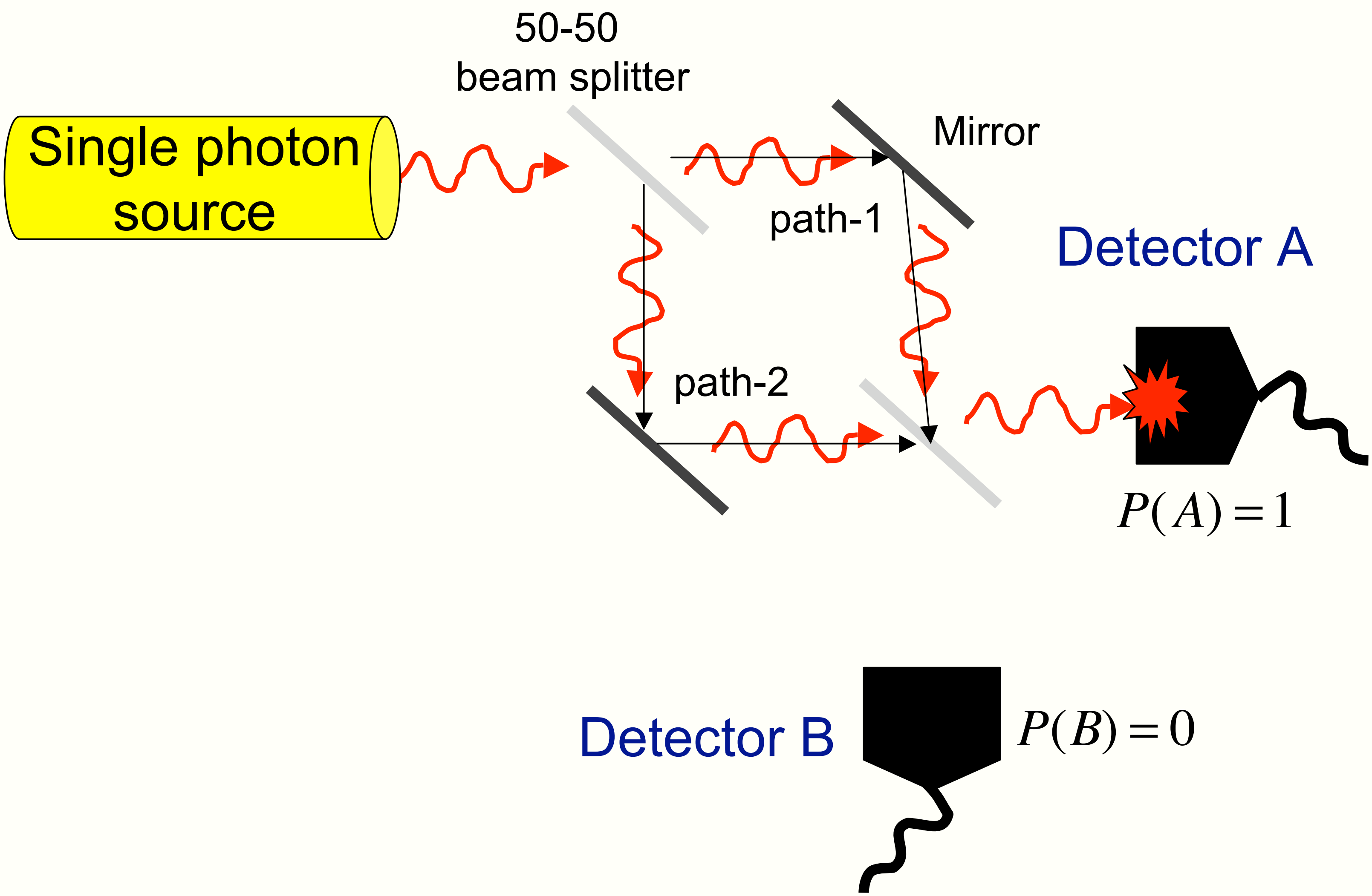
$$P\left(x|y_1, y_2\right) = N \underbrace{P\left(x|y_1\right)}_{\text{prior}} \underbrace{P\left(y_2|x, y_1\right)}_{\text{likelihood}}$$

How Does the Quantum World Differ?

Probabilties of events Quantum World



Probabilties of events Quantum World



Quantum Events Can Define Logic

"Logically":

$$P(A) = \underbrace{P\left(A\middle|1\right)}\underbrace{P(1)} + \underbrace{P\left(A\middle|2\right)}\underbrace{P(2)}$$

probability that *A* fires given path-1

probability of path-1

probability that *A* fires given path-2

probability of path-2

$$P(A) = \underbrace{P\left(A\middle|1\right)}_{1/2}\underbrace{P(1)}_{1/2} + \underbrace{P\left(A\middle|2\right)}_{1/2}\underbrace{P(2)}_{1/2} = 1/2$$

? ? ? ?

The Quantum World Has Its Own Logic

Probability vs. *Probability Amplitude*

To quantum "processes" are associated complex amplitudes, ψ_i

The probability of an even is the square modulus, $P_i = |\psi_i|^2 = \psi_i^* \psi_i$

Feynman's Rule: Add *amplitudes* for *indistinguishable* processes

$$\psi(A) = \psi(A|1)\psi(1) + \psi(A|2)\psi(2)$$

$$P(A) = |\psi(A)|^2 = \psi^*(A)\psi(A)$$

$$= \left(\psi(A|1)\psi(1) + \psi(A|2)\psi(2)\right)^* \left(\psi(A|1)\psi(1) + \psi(A|2)\psi(2)\right)$$

$$= |\psi(A|1)|^2 |\psi(1)|^2 + |\psi(A|2)|^2 |\psi(2)|^2$$

$$+ \psi(A|1)\psi(1)\psi^*(A|2)\psi^*(2) + \psi(A|2)\psi(2)\psi^*(A|1)\psi^*(1)$$

The Quantum World Has Its Own Logic

Probability vs. *Probability Amplitude*

To quantum "processes" are associated complex amplitudes, ψ_i

The probability of an even is the square modulus, $P_i = |\psi_i|^2 = \psi_i^* \psi_i$

Feynman's Rule: Add *amplitudes* for *indistinguishable* processes

$$\psi(A) = \psi(A|1)\psi(1) + \psi(A|2)\psi(2)$$

$$P(A) = |\psi(A)|^2 = \psi^*(A)\psi(A)$$

$$= \left(\psi(A|1)\psi(1) + \psi(A|2)\psi(2)\right)^* \left(\psi(A|1)\psi(1) + \psi(A|2)\psi(2)\right)$$

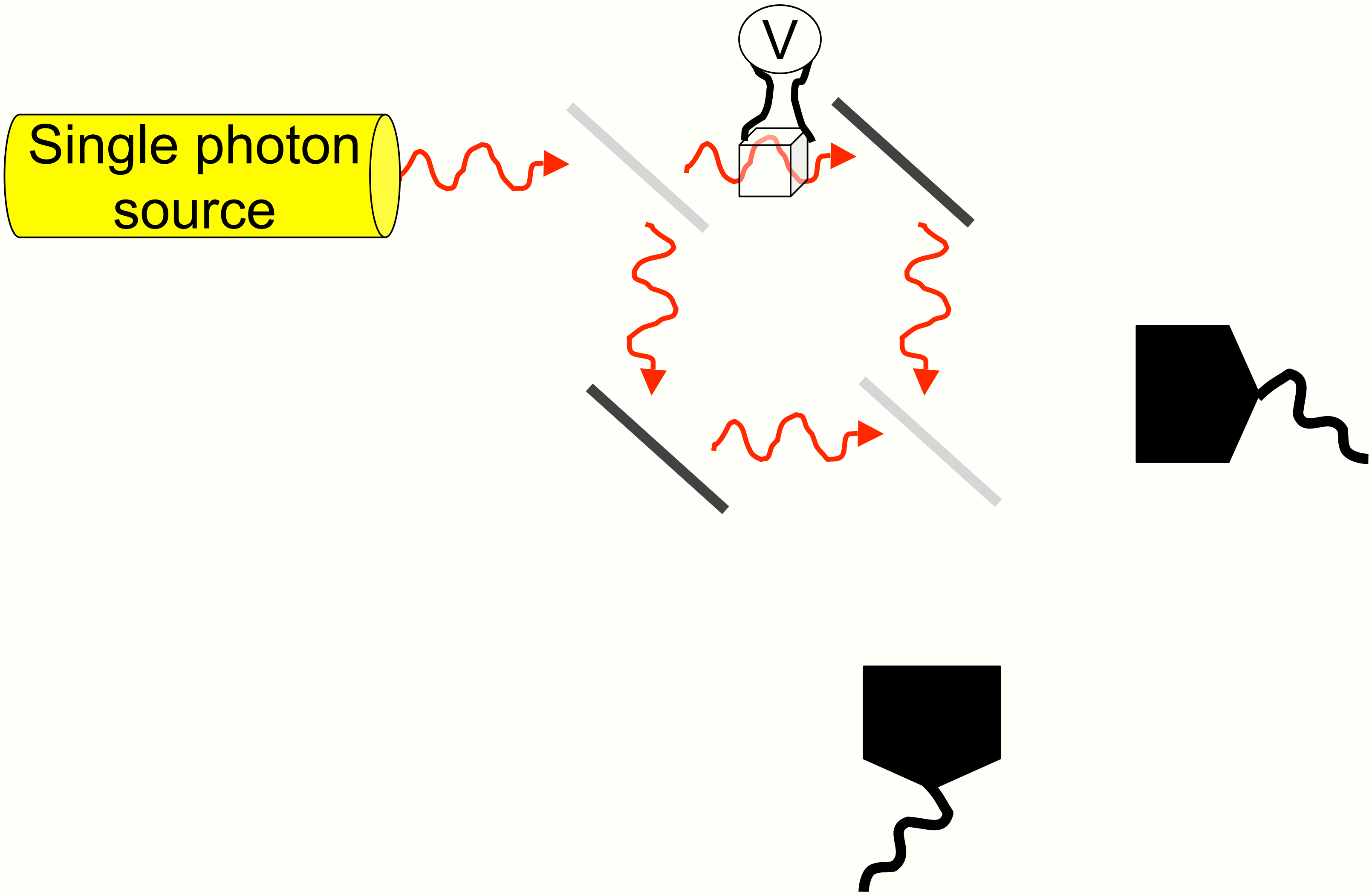
$$= P(A|1)P(1) + P(A|2)P(2)$$

classical logic

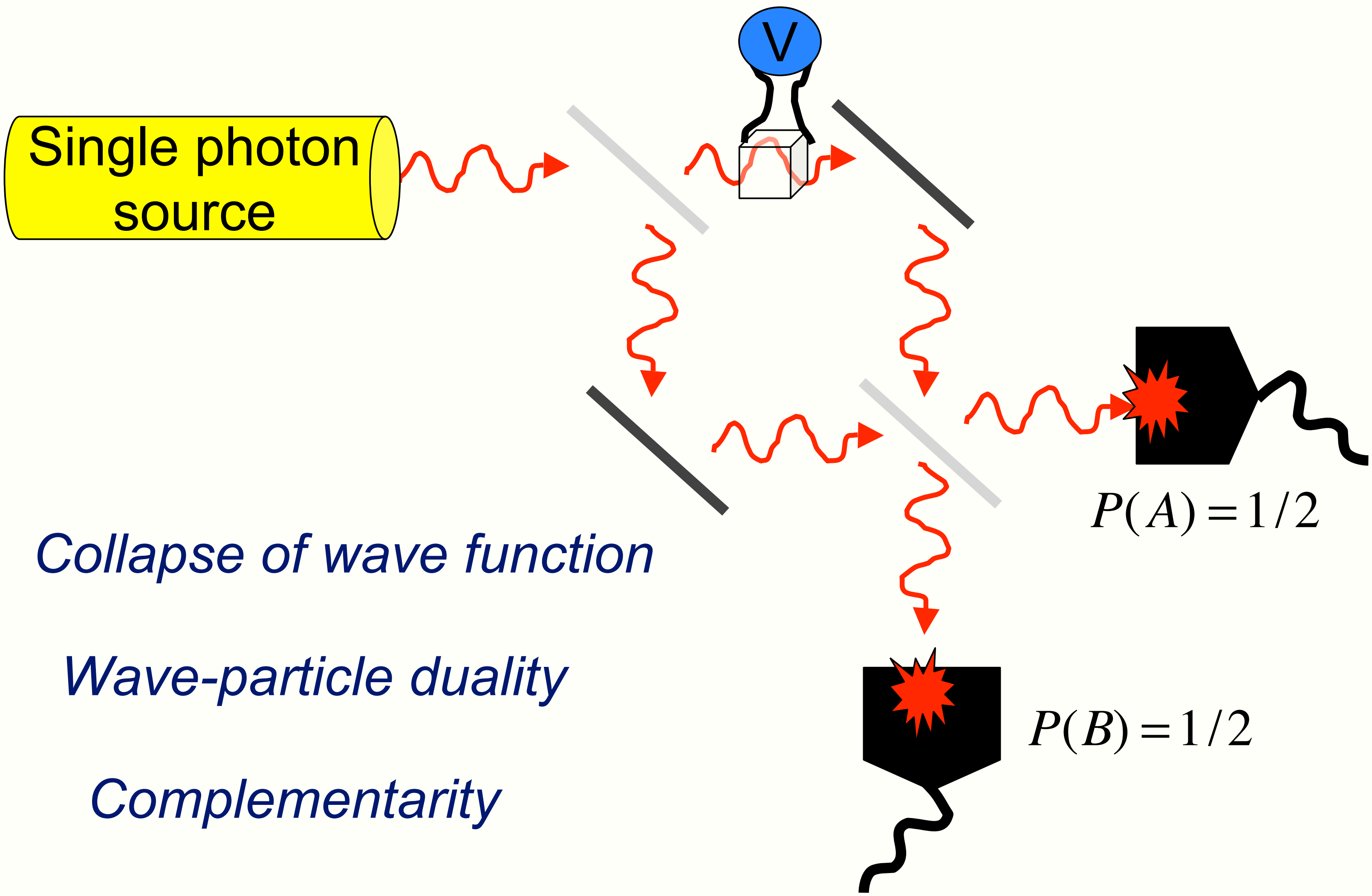
quantum interference

$$+\psi(A|1)\psi(1)\psi^*(A|2)\psi^*(2) + \psi(A|2)\psi(2)\psi^*(A|1)\psi^*(1)$$

Measurement / Irreducible Disturbance



Measurement / Irreducible Disturbance



Collapse of wave function

Wave-particle duality

Complementarity

What Is Collapsing?

What is the probability the coin is heads up?

P=1/2

What Is Collapsing?

What Is Collapsing?

State of knowledge

What is the probability the coin is heads up?

P=1

Hidden Variables?

Classical probability: Incomplete knowledge of state, but can be "completed" by discovering the "hidden information" of an objective, "realistic" property.

Einstein: Quantum mechanics is "incomplete". "Hidden variables" make results appear random.

John Bell: There is no *local* hidden variable (objective value) that can account for correlations in quantum measurements.

Entangled States

The Weird Quantum World

- Interference between indistinguishable processes.
- Heisenberg uncertainty (incompatible observables).
- Information-gain / measurement-disturbance.
- Entanglement: No local realism.

Quantum Information: Putting weirdness to work!

What is Quantum Information Good For?

Quantum Computation:

• Universal Machine (Shor's algorithm)
• Quantum Simulation

Quantum Cryptography:

• Key Distribution (QKD)
• Secret sharing

Quantum Communication:

• Channel capacity
• Distributed computation

Quantum Metrology

• Precision sensors

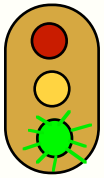
Hardware and Software of Quantum Information

Fundamental Unit of Quantum Information

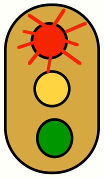
Classical Bit: Two-states which are clear distinguished

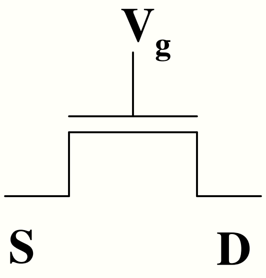
Digital Logic

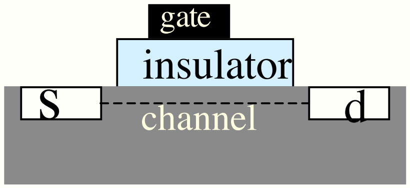
1= *"On"*



0= *"Off"*







MOSFET

Fundamental Unit of Quantum Information

Quantum bit (qubit): Two-states which are "orthogonal" and can exist in superposition.

- Photon paths or polarizations in an interferometer.
- Energy levels of an atom.
- "Spin" directions of an electron.
- Charge states in a quantum dot.
- Mesoscopic currents in a superconductor.

Logical "basis" states:

$|0\rangle$ Port-A of interferometer

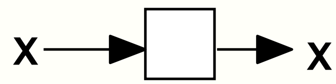
$|1\rangle$ Port-B of interferometer

General superposition: $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$

Transformation on qubits: Logic Gates

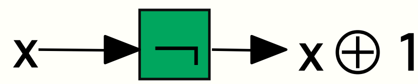
Bit

Identity



IN	OUT
0	0
1	1

NOT



IN	OUT
0	1
1	0

Qubit

NOT

$$|0\rangle \rightarrow |1\rangle$$
$$|1\rangle \rightarrow |0\rangle$$

$\sqrt{\text{NOT}}$

$$|0\rangle \rightarrow (|0\rangle - i|1\rangle)/\sqrt{2}$$
$$|1\rangle \rightarrow (|1\rangle - i|0\rangle)/\sqrt{2}$$

H

$$|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$$
$$|1\rangle \rightarrow (|1\rangle - |0\rangle)/\sqrt{2}$$

Multiple Qubits: The Space Grows Exponentially

E.g. 3-qubits, dim=8

$$|0\rangle = |0\rangle|0\rangle|0\rangle \quad |1\rangle = |0\rangle|0\rangle|1\rangle \quad |2\rangle = |0\rangle|1\rangle|0\rangle \quad |3\rangle = |0\rangle|1\rangle|1\rangle$$

$$|4\rangle = |1\rangle|0\rangle|0\rangle \quad |5\rangle = |1\rangle|0\rangle|1\rangle \quad |6\rangle = |1\rangle|1\rangle|0\rangle \quad |7\rangle = |1\rangle|1\rangle|1\rangle$$

General state: $|\psi\rangle = \sum_{x=0}^{2^n-1} c_x |x\rangle$

n-qubits: 2^n alternatives

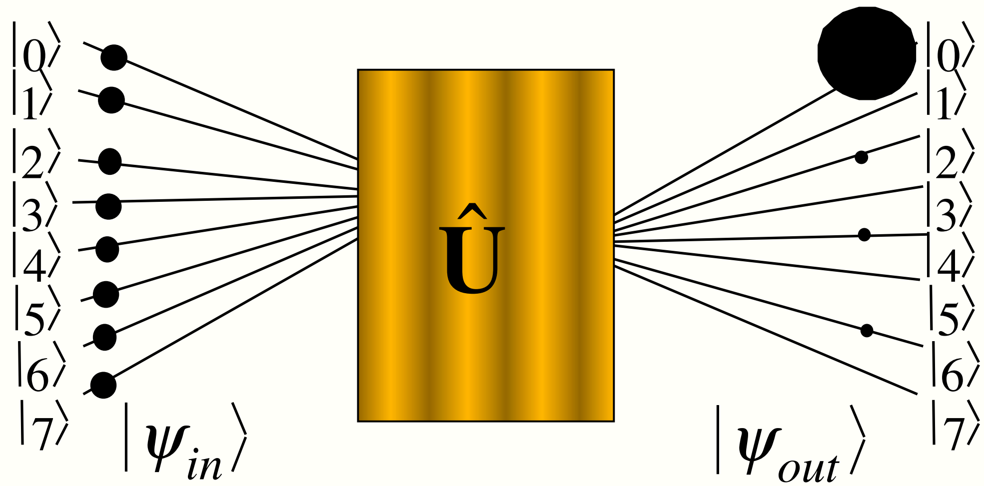
Entangled

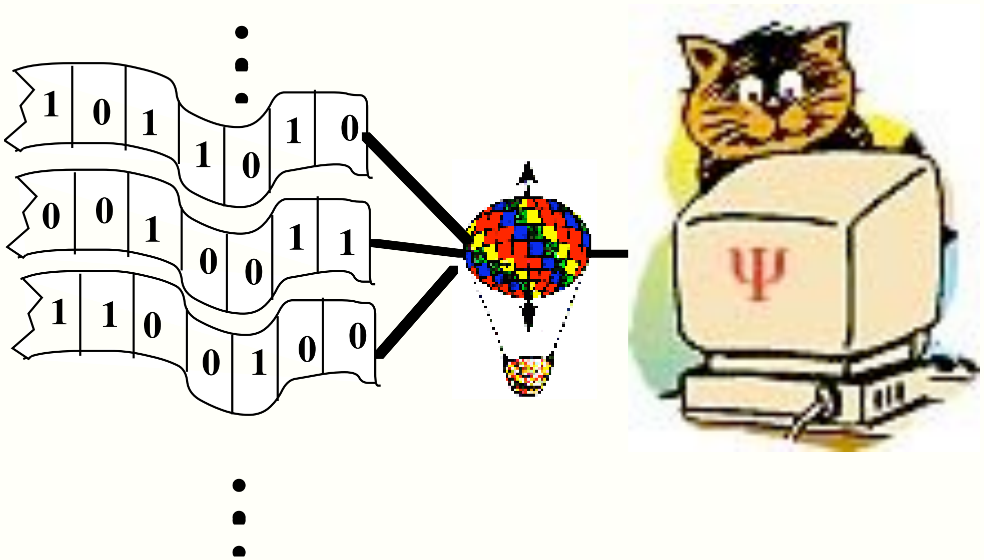
$$|\psi\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_3\rangle$$

Quantum Algorithm

- **Map input-output**

$$|\psi_{out}\rangle = \hat{U}|\psi_{in}\rangle$$



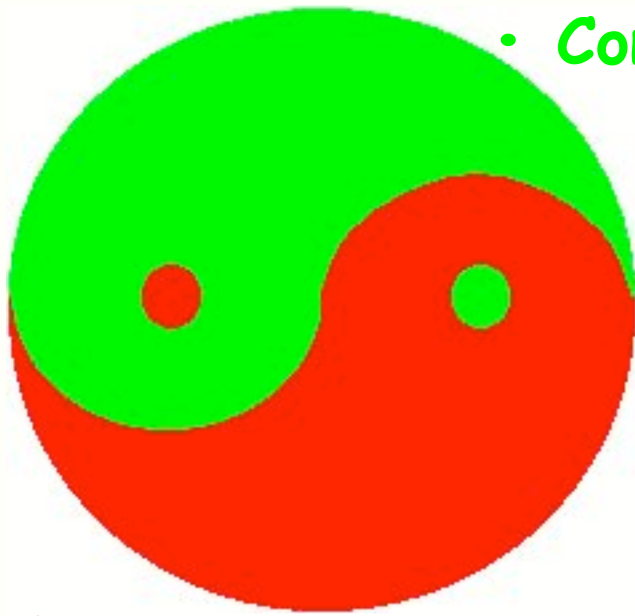


Quantum Parallelism

The Tao of Quantum Computing

- Coupling qubits.
- Control fields.

Coherence



- Coupling to environment.
- Coupling to neglected degrees of freedom.

Decoherence

I. H. Deutsch, *University of New Mexico*
Short Course in Quantum Information