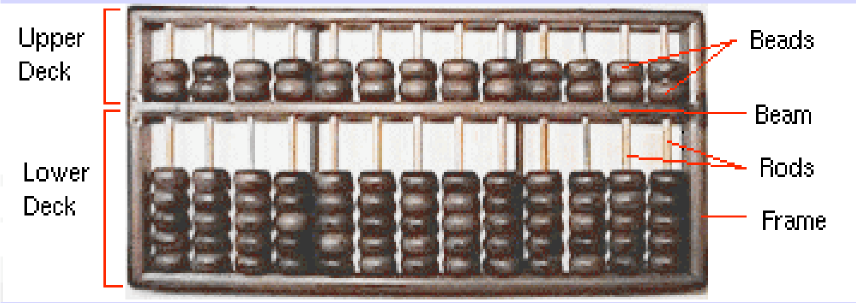
Quantum Computation

Juan Pablo Paz
Departmento de Física, FCEyN,
Universidad de Buenos Aires, Argentina

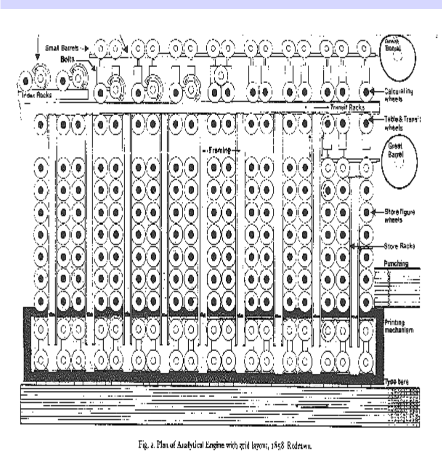
SFI SUMMER SCHOOL
BARILOCHE
December 2008

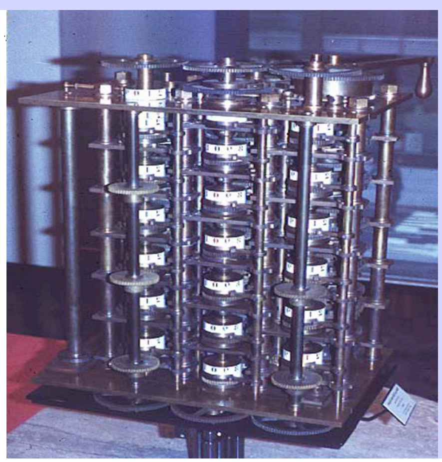
Departamento de Física Juan José Giambiagi
Facultad de Ciencias Exactas y Naturales Universidad de Buenos Aires

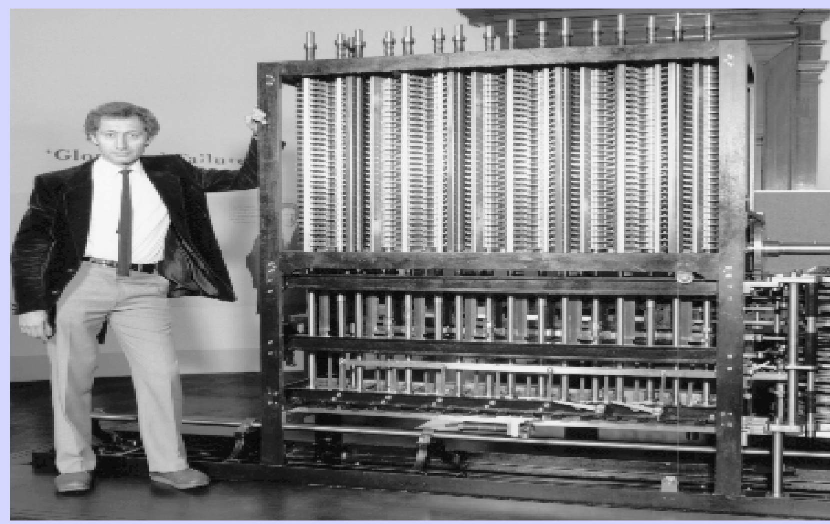
What is a computer?



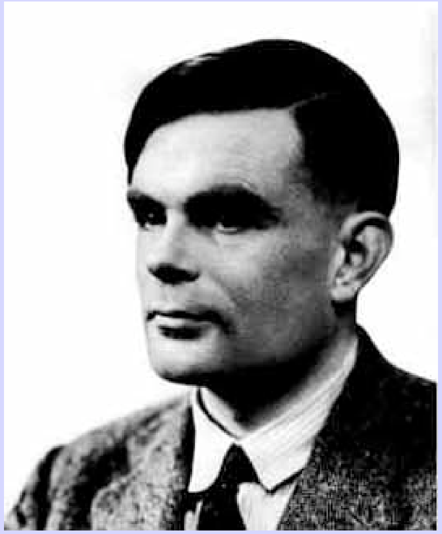
Blaise Pascal (France, 1642).





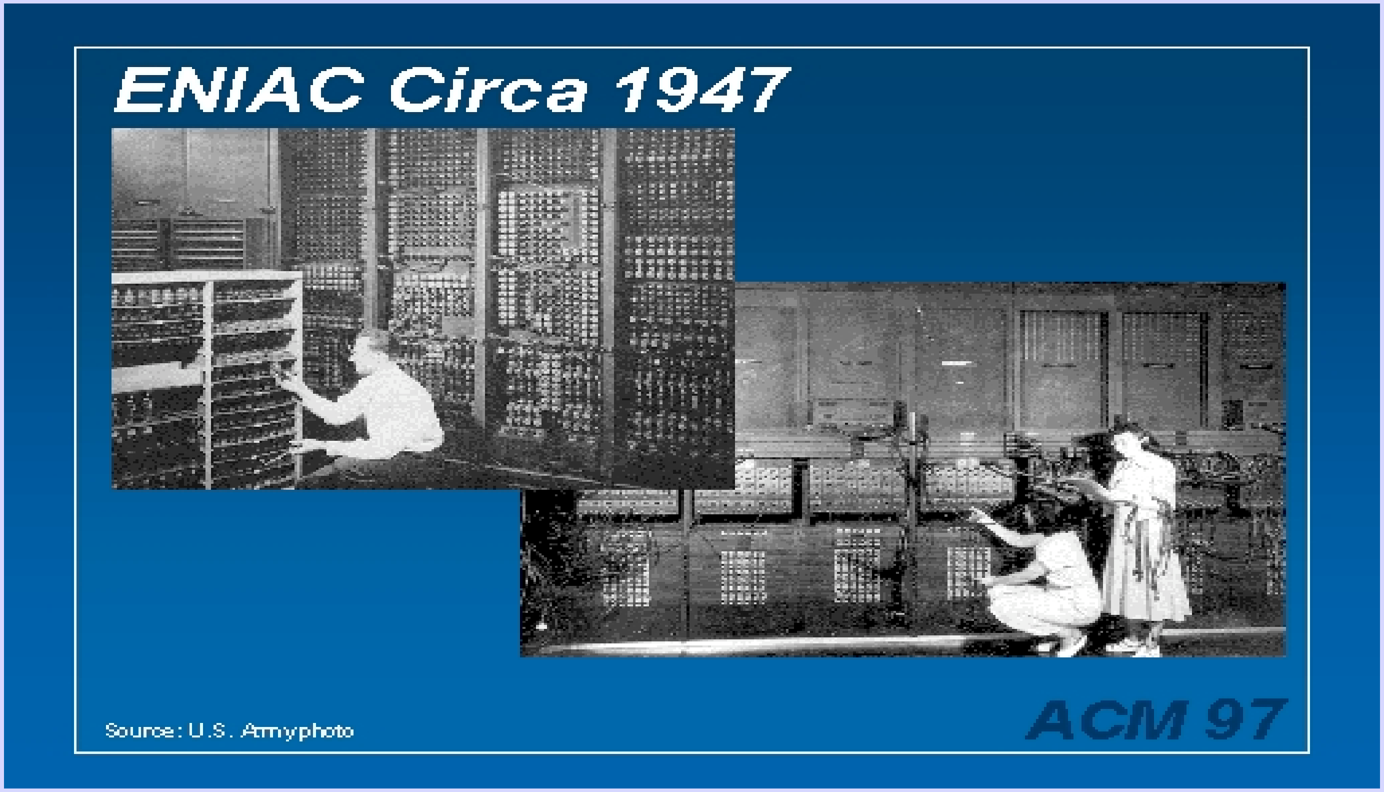


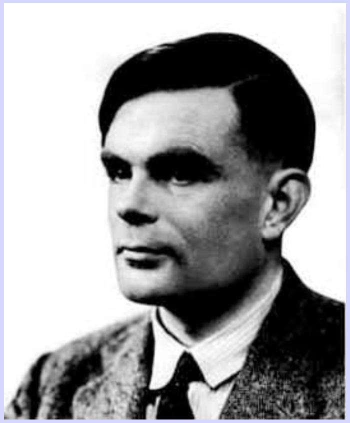
Universal Computer (programmable)



Turing (UK, 1930)

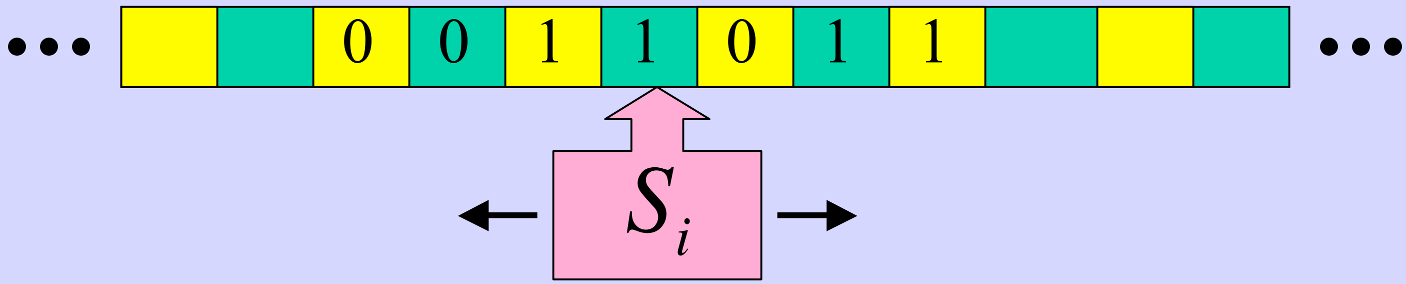
von Neuman (USA, 1940)





Turing (UK, 1930)

COMPUTER= TURING MACHINE



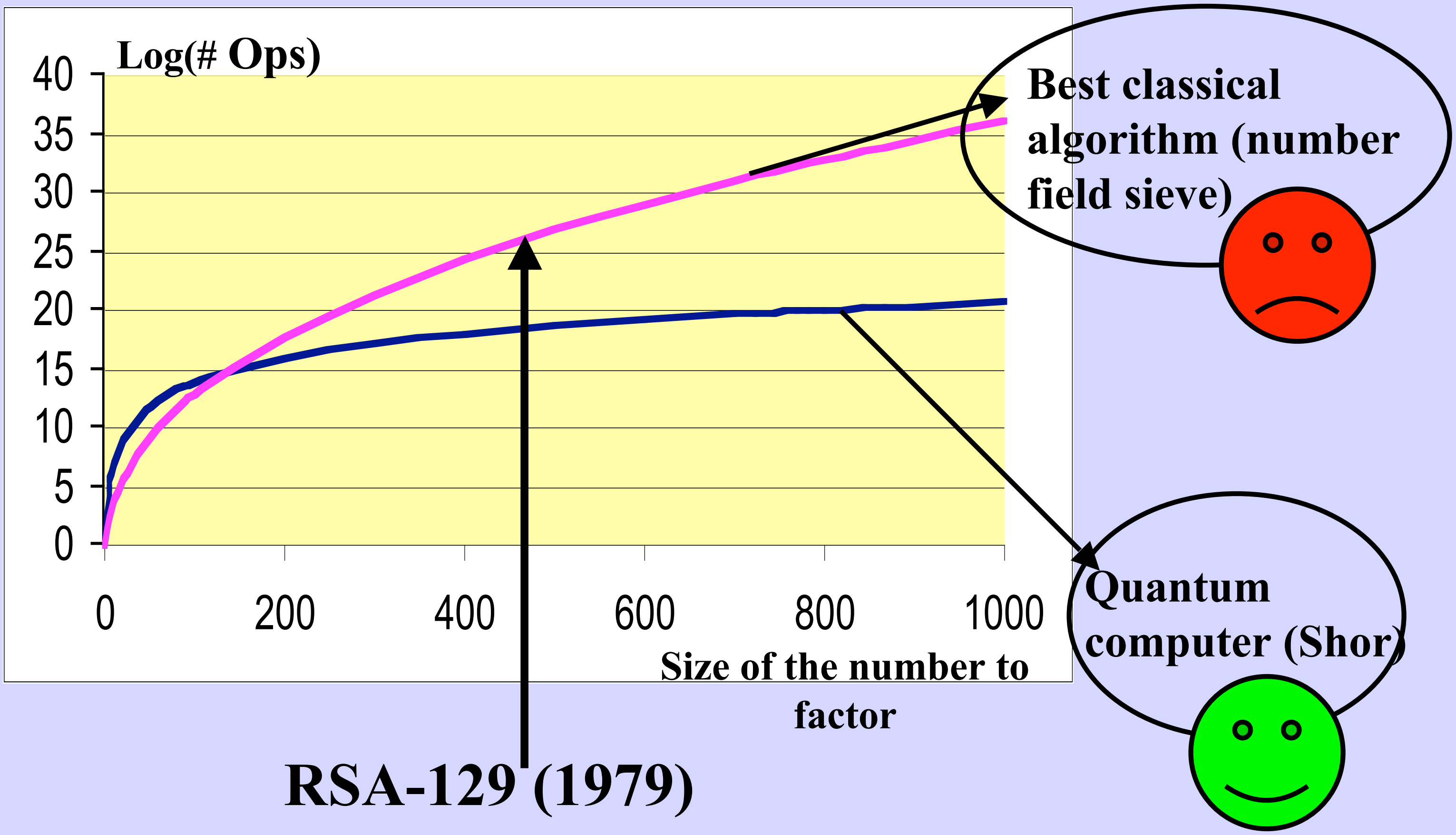
$$\left(X,S_i\right)\Rightarrow\left(X',S_k\right),\left(R,L\right)$$

Church-Turing Thesis: A problemm can be solved in a 'reasonable' computer if and only if it can be solved in a Turing Machine

Strong Church-Turing Thesis: Every 'reasonable' computer device can be simulated "efficiently" in a non--deterministic Turing Machine

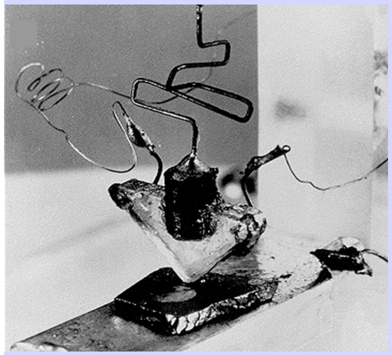
Quantum Computation questions the validity of the Strong Church-Turing Thesis

"Killer application" of quantum computers
Find prime factors of integer numbers: Peter Shor (1994)

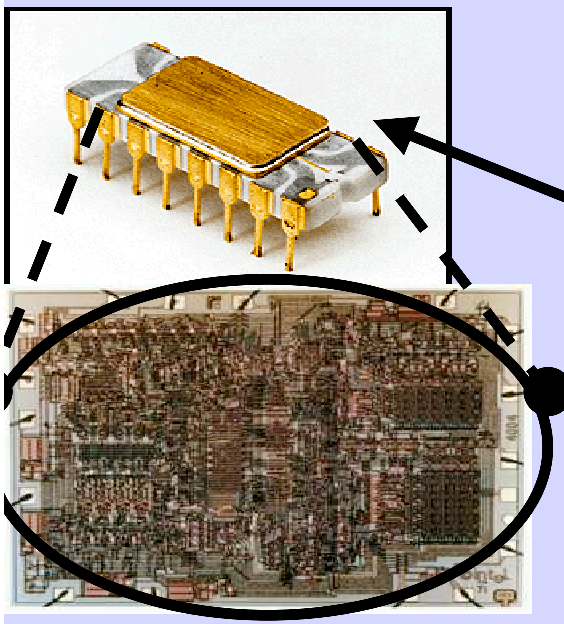


Challenge ($ 10,000): RSA-576 (172 digits), find P and Q such that
P x Q =1881988129206079638386972394616504398071635633794173827007633564229888597152346654853190606065047430453173880113033967161996923212057340318795506569962213051687593076502570 59 **(see details in www.rsa.com)**

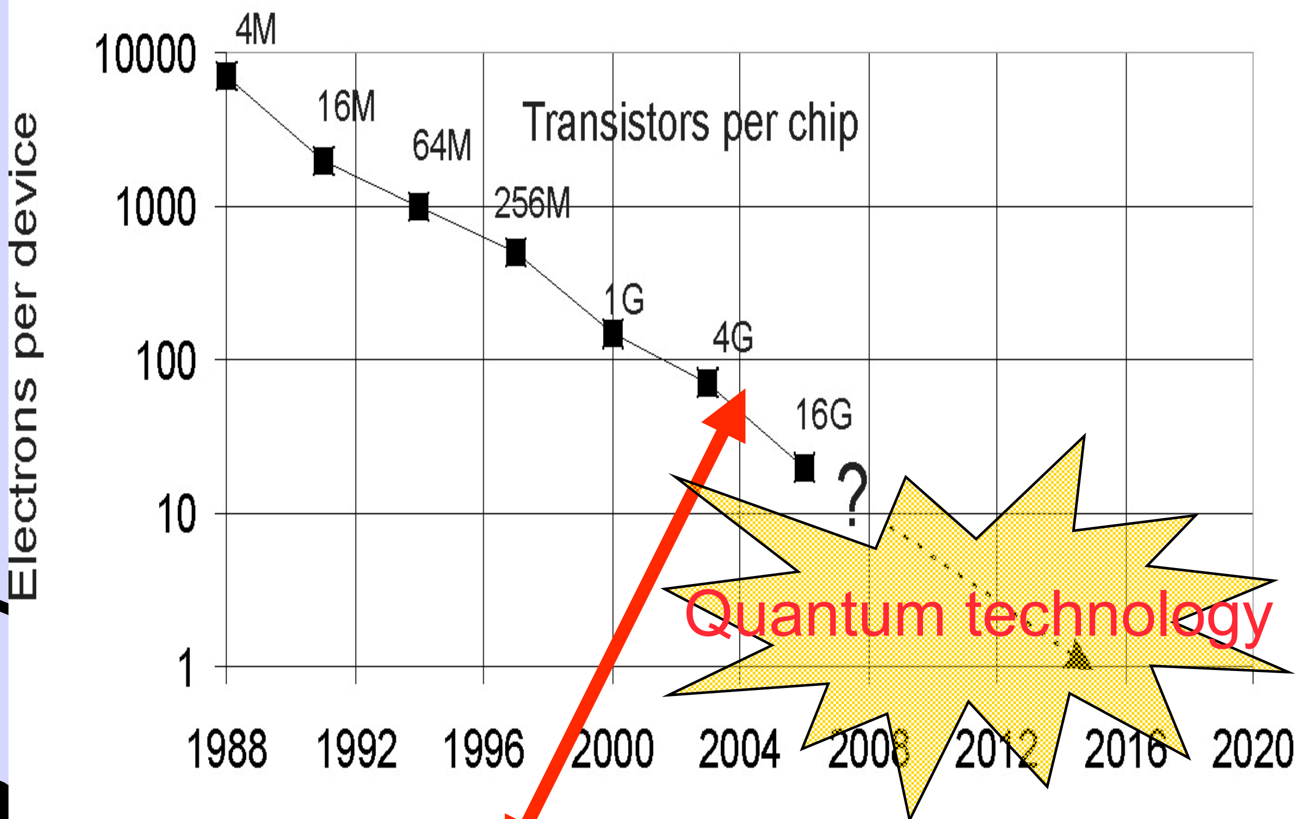
Microelectronics: Trends on the nature of "reasonable" computational devices. Smaller and smaller… Moore's law: Number of transistors per chip doubles every 18 months.



Transistor 1956



Intel 4004: 2500 transistors



What is the limit? Could we store a bit using a single atom? ***Current hard disks store one bit using 100,000,000,000 atoms***

Is it possible to manipulate single atoms? Reality or fiction?

Schrödinger, 1952: ***"…We never perform experiments with single electrons or single atoms. Sometimes we assume this is possible but this leads us to ridiculous conclusions…***

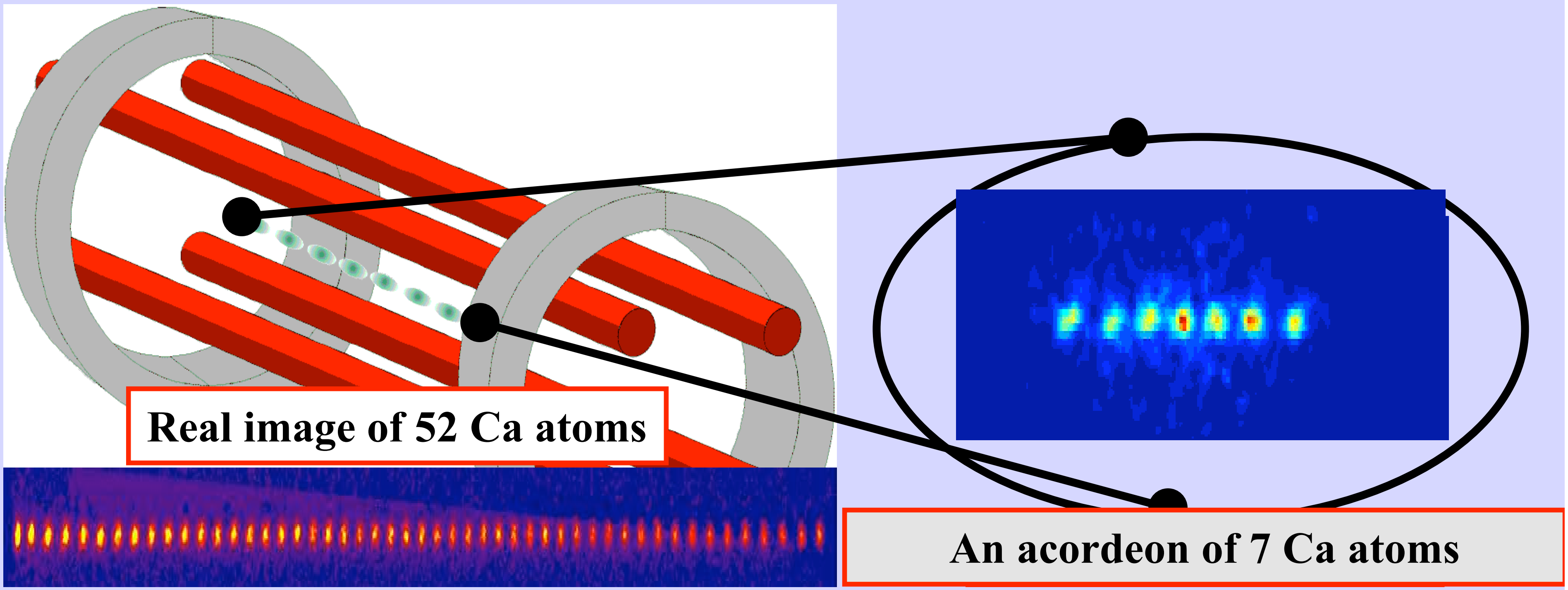
We can say that we do not perform experiments with single particles in the same way that we do not have Ictiosaurios in the zoo…"

(*British Journal of the Philosophy of Sciences, vol. 3, 1952*)

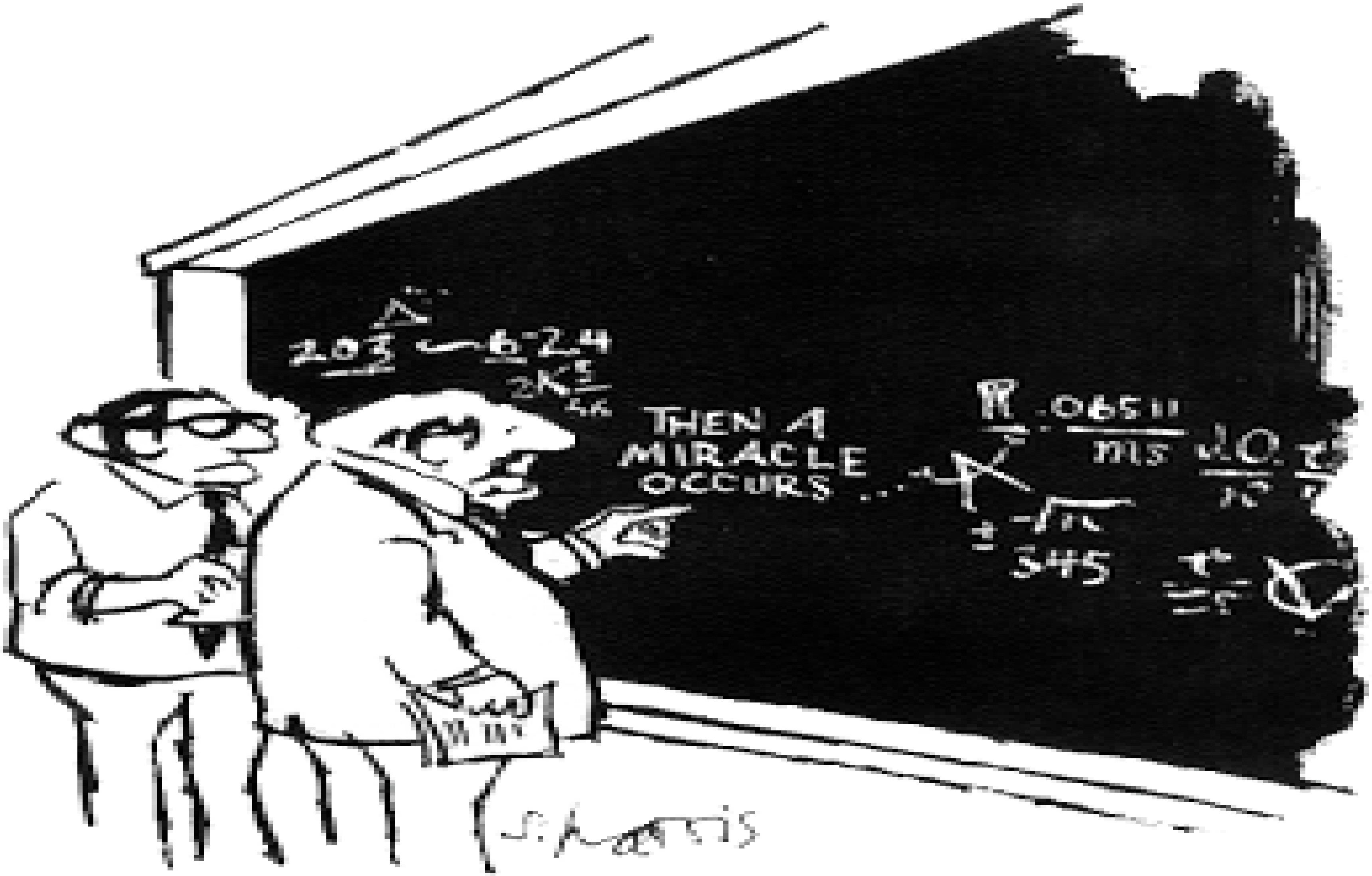
Quantum physics 50 years afterwards: Ictiosaurious in the zoo!

XXI CENTURY: QUANTUM TECHNOLOGIES

Atoms In “traps” controlled and manipulated one by one!!



NEW APPLICATIONS: QUANTUM COMPUTERS (ETC!…)



"I think you should be more explicit here in step two."

QUANTUM COMPUTERS

Richard Feynman

1981

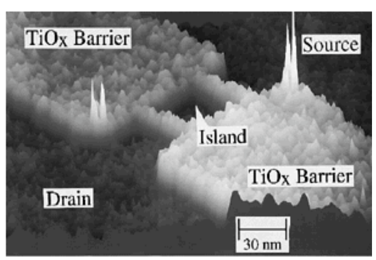
David Deutsch

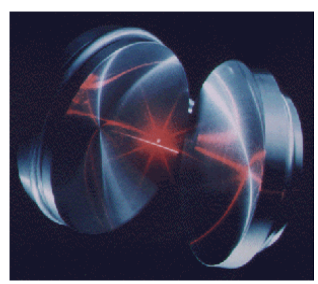
1990

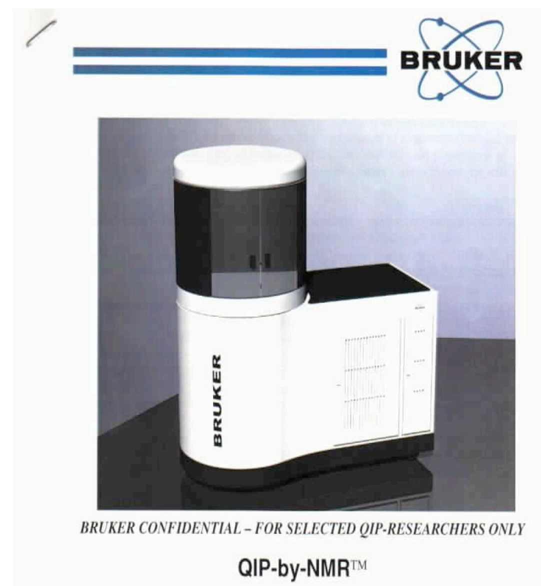
Peter Shor

1994

HOW DO THEY LOOK
(rather primitive…)

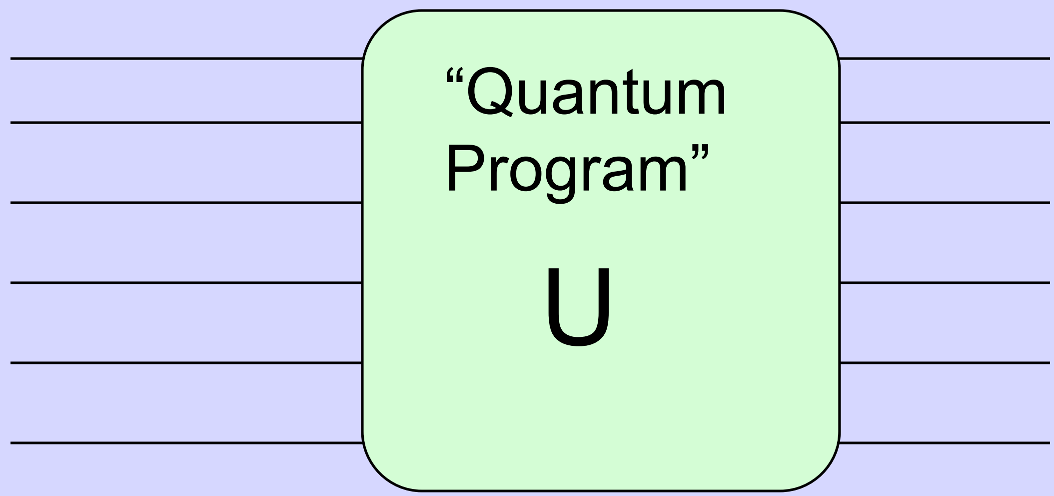






Rules of the game:
Classical computation can be represented in terms of ‘circuits’ (with cables and boxes). Let’s present the quantum version of this

$|\Psi(0)\rangle$



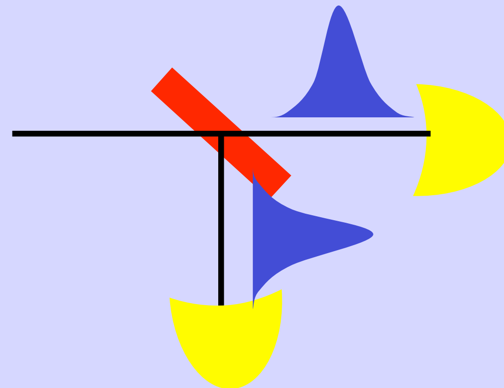
$|\Psi(final)\rangle = U|\Psi(0)\rangle$

- **What are the cables (quantum hardware)**
- **What is inside the black box (quantum hardware and quantum software)**

Quantum physics 101: Strange properties of photons

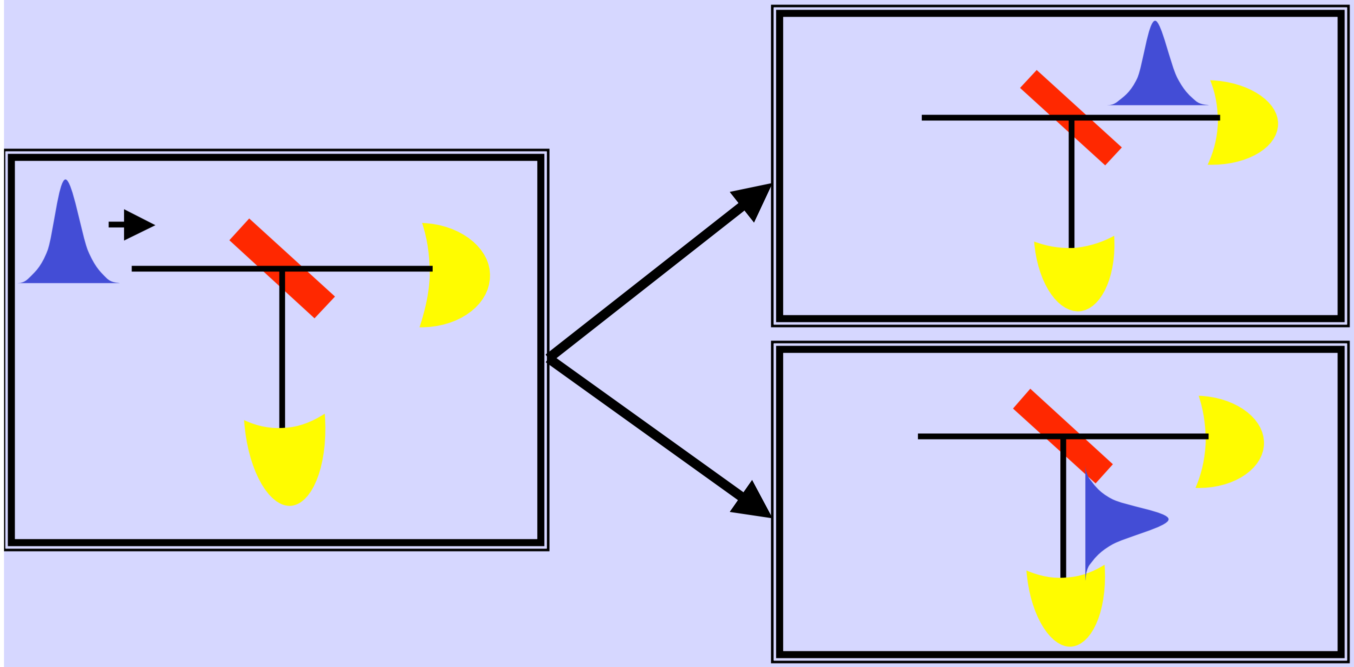
Shile a laser on a half mirror (50% reflected, 50% transmited)

Classical case: intense bea
(laser pointer)



50% of the intensity goes to each detector

Quantum case: atenuated beam, light arrives in 'packets' (photons)

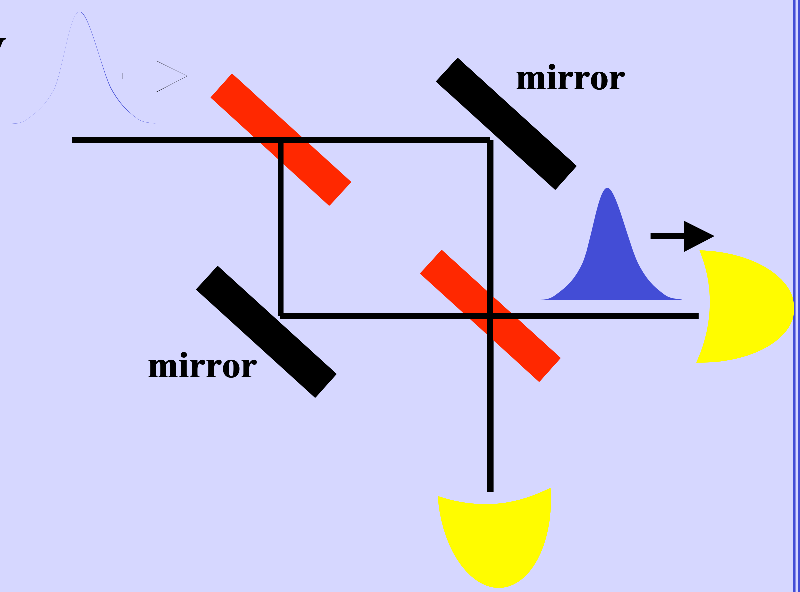


50% of the time one detector "clicks"

50% of the time the other detector "clicks"

Photons arrive one by one. But: what path do they follow?

Quiz: How many photons go to each detector?



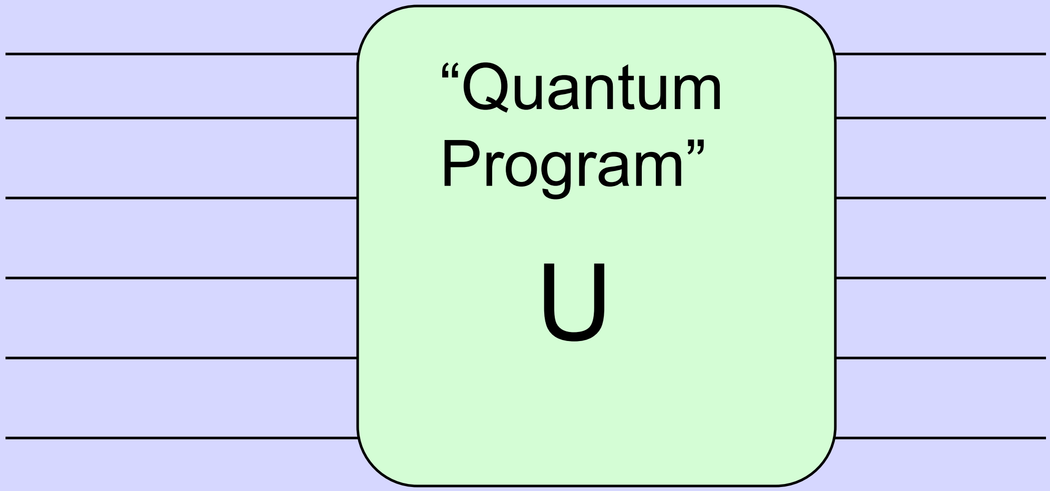
Empirical fact (hard to swallow!): EVERY photon arrives to one of the detectors!! This fact cannot be explained unless we accept that photons do not follow a single trajectory (they follow both!)

During the experiment, the state of the photon is described by a vector that is the superposition (linear combination) of two alternatives "up" and "down"

$$|Photon\rangle = |UP\rangle + |DOWN\rangle$$

Rules of the game:
Classical computation can be represented in terms of 'circuits' (with cables and boxes). Let's present the quantum version of this

$|\Psi(0)\rangle$



$|\Psi(final)\rangle = U|\Psi(0)\rangle$

- **What are the cables (quantum hardwaqre)**
- **What is inside the black box? (quantum hardware and quantum software)**

Basic ingredient for quantum hardware:
I) Quantum Bits (qubits)

A physical system may represent a "classical bit" if it can exist in two distinct (stable) states

A physical system can represent a "quantum bit" if it can exist in any state belonging to a 2-dimensional vector space (complex)

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

Most general state of a qubit (vector in a 2-dim complex vector space)

$$\Pr obability(1) = |\alpha|^2 \qquad \Pr obability(0) = |\beta|^2$$

$$|n - Qubits\rangle = \alpha_0|00...00\rangle + \alpha_1|00...01\rangle + ... + \alpha_{2^n-1}|11...11\rangle$$

Most general state of n qubits (lives in a complex vector space with 2^n dimensions)

QUANTUM MECHANICS

(the most succesfull theory in the history of science)

Randomness is intrinsic to nature: we can only predict probabilities

WE DO NOT predict where each electron lands!

WE DO PREDICT location of fringes, separation, brightness, etc.

How do we predit probabilities? Describe the state of a system as a vector

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

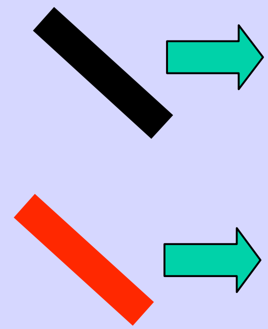
$$\Pr obability(1) = |\alpha|^2 \quad \Pr obability(0) = |\beta|^2$$

State change in time. How? Example: when a photon encounters mirrors, beam splitters, etc …

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

$$|0\rangle = photon\ in\ path\ a$$

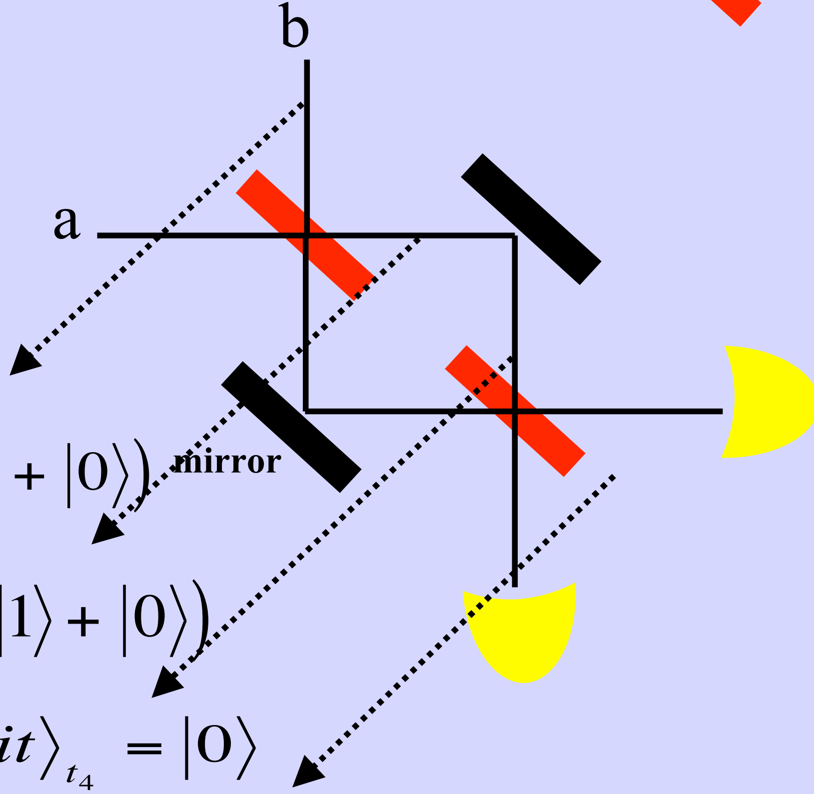
$$|1\rangle = photon\ in\ path\ b$$



$$|0\rangle \rightarrow |1\rangle; \quad |1\rangle \rightarrow |0\rangle$$

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

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$



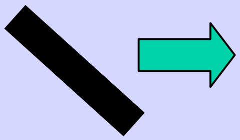
$$|Qubit\rangle_{t_1} = |0\rangle$$

$$|Qubit\rangle_{t_2} = \frac{1}{\sqrt{2}}\left(|1\rangle + |0\rangle\right)$$

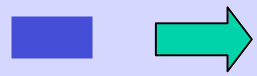
$$|Qubit\rangle_{t_3} = \frac{1}{\sqrt{2}}\left(|1\rangle + |0\rangle\right)$$

$$|Qubit\rangle_{t_4} = |0\rangle$$

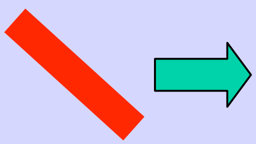
State change in time. How? Example: when a photon encounters mirrors, beam splitters, glass, etc …



$$|0\rangle \rightarrow |1\rangle; \quad |1\rangle \rightarrow |0\rangle$$

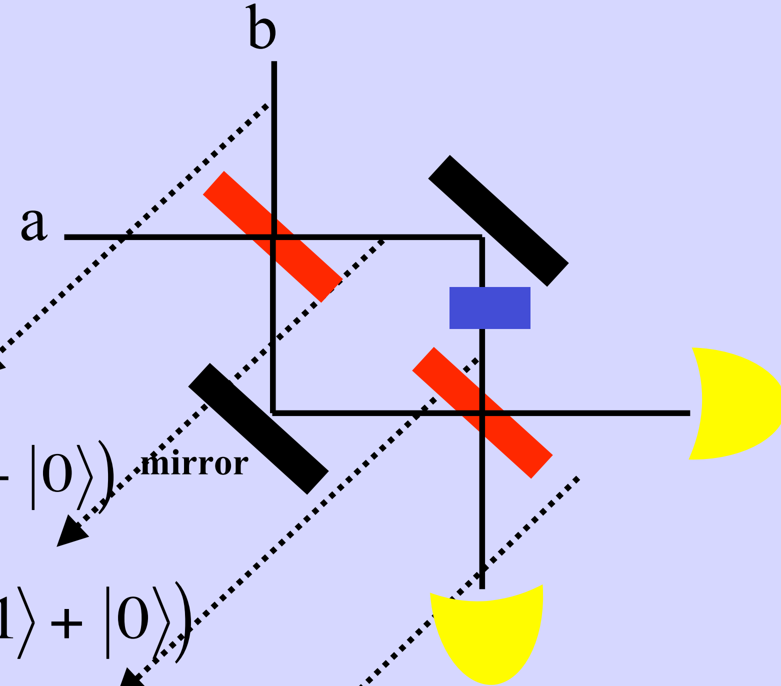


$$|0\rangle \rightarrow |0\rangle; \quad |1\rangle \rightarrow -|1\rangle$$



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

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



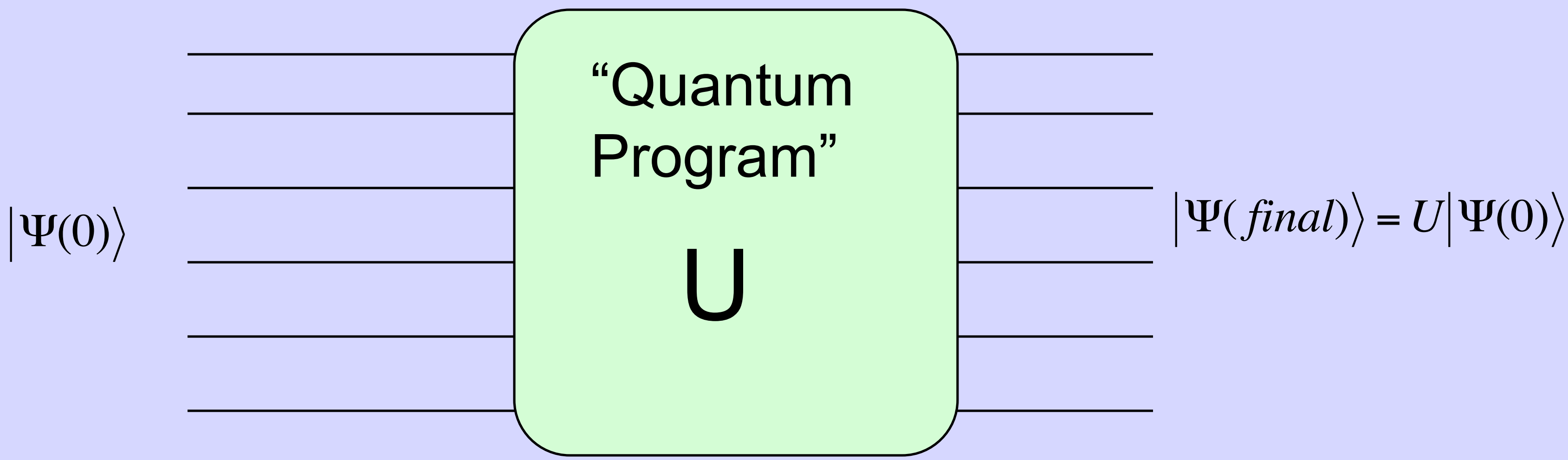
$$|Qubit\rangle_{t_1} = |0\rangle$$

$$|Qubit\rangle_{t_2} = \frac{1}{\sqrt{2}}\left(|1\rangle + |0\rangle\right)$$

$$|Qubit\rangle_{t_3} = \frac{1}{\sqrt{2}}\left(-|1\rangle + |0\rangle\right)$$

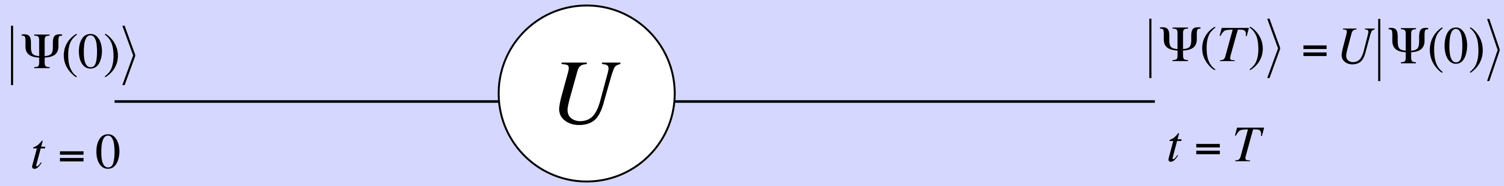
$$|Qubit\rangle_{t_4} = |1\rangle$$

Rules of the game:
Classical computation can be represented in terms of 'circuits' (with cables and boxes).
Let's present the quantum version of this



- **What are the cables (quantum hardware)**
- **What is inside the black box? (quantum hardware and quantum software)**

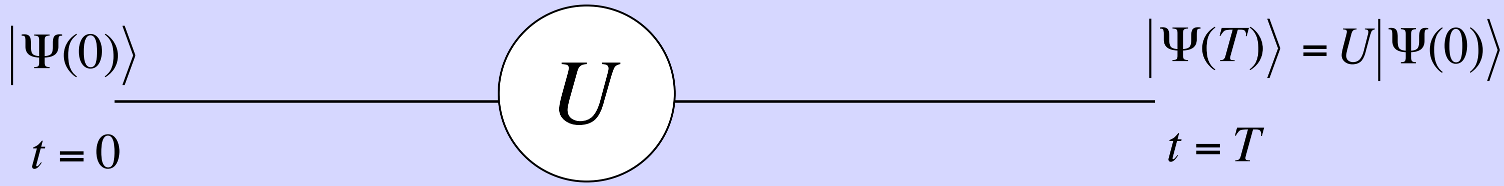
Basic ingredient for quantum hardware: II) Temporal evolution



Evolution is represented by an "evolution operator U"
U is a linear operator (matrix) which is unitary (its inverse is the transpose-conjugate matrix)

U depends on:
a) The qubit, b) Our action on it (remember mirrors, glass, etc)

Basic ingredient for quantum hardware:
Universal computer: Able to reach ANY U



1) A set of qubits can be used to perform any quantum computation if one can "force" them to evolve with an arbitrary U (unitary operator)

2) An arbitrary U on a set of qubits can be attained if we are able to combine a finite set of operators acting on pairs of qubits (analogue to universal gates)

Analogy: A set of classical bits can be used to evaluate any Boolean function if we can implement a set of universal (XOR, NAND, etc) gates on any pair

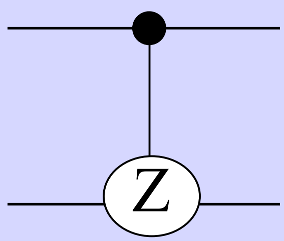
RESULT 1 (IMPORTANT): FOR A SINGLE QUBIT, EVERY UNITARY OPERATOR CAN BE OBTAINED AS A PRODUCT OF THREE ROTATIONS

RESULT 2 (VERY IMPORTANT): FOR A SET OF n QUBITS EVERY UNITARY OPERATOR CAN BE APPROXIMATED ("WITH AN ERROR AS SMALL AS WE WANT") AS A SEQUENCE OF:

a) OPERADORS AFFECTING A SINGLE QUBIT (PREVIOUS CASE)

b) A SIMPLE TWO-QUBIT OPERATOR

CONTROL-Z



$$U_{C-Z}|0\rangle|0\rangle = |0\rangle|0\rangle$$

$$U_{C-Z}|0\rangle|1\rangle = |0\rangle|1\rangle$$

$$U_{C-Z}|1\rangle|0\rangle = |1\rangle|0\rangle$$

$$U_{C-Z}|1\rangle|1\rangle = -|1\rangle|1\rangle$$

NOTATION: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- CONTROL-Z IS OBTAINED FROM "SIMPLE INTERACTIONS" BETWEEN TWO QUBITS

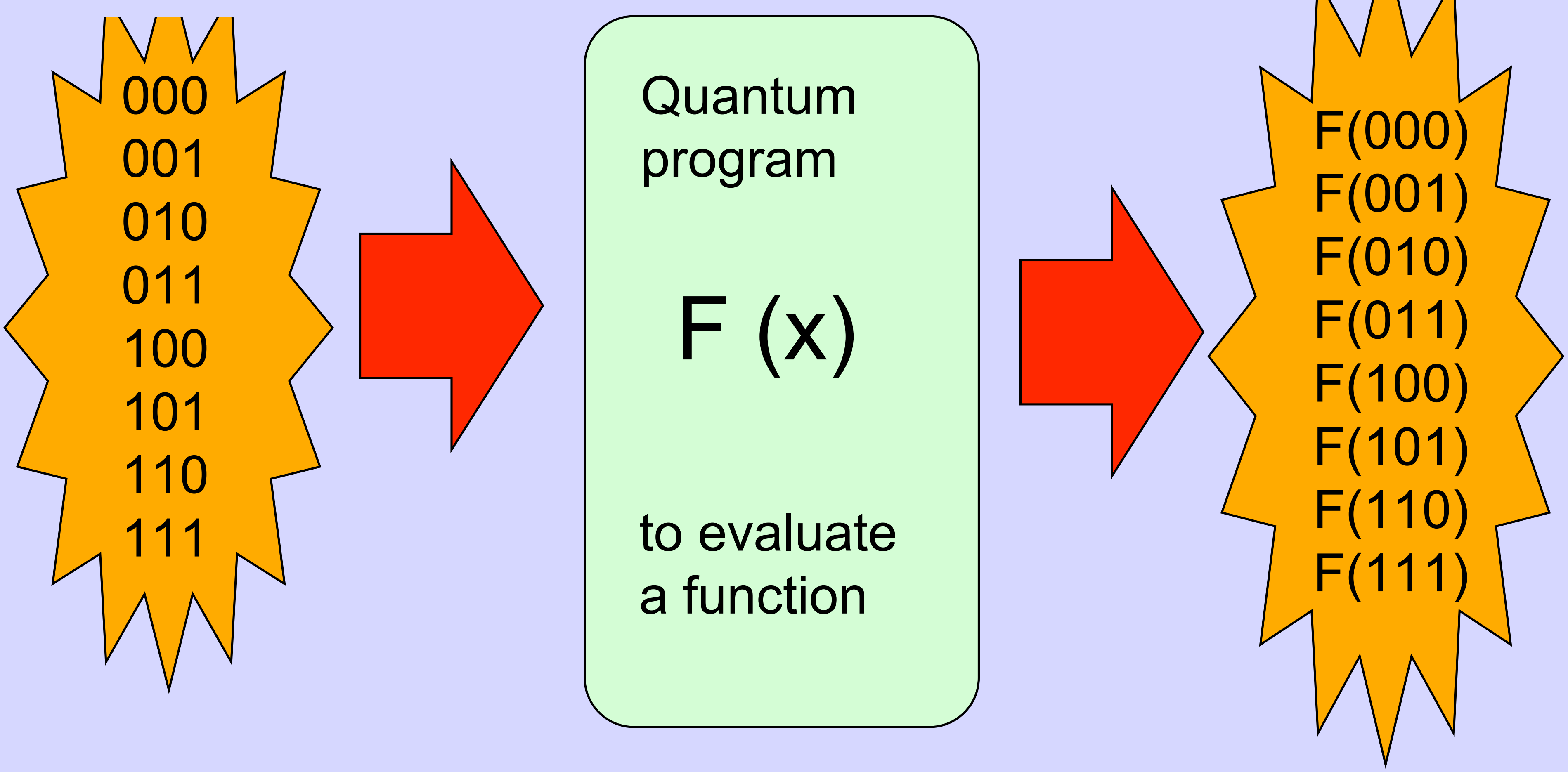
$$U_{C-Z} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

$$U_{C-Z} \approx \exp\left(i\frac{\pi}{4}(I - Z) \otimes Z \right)$$

Evolution of a quantm computer
New paradigm: quantum parallelism (magic version…)

Initial State: Three qubits in a superposition.

Final state: Store the value of the function in all numbers!

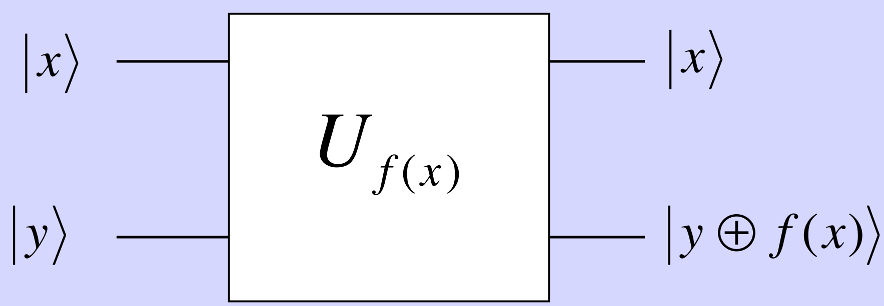


Quantum parallelism

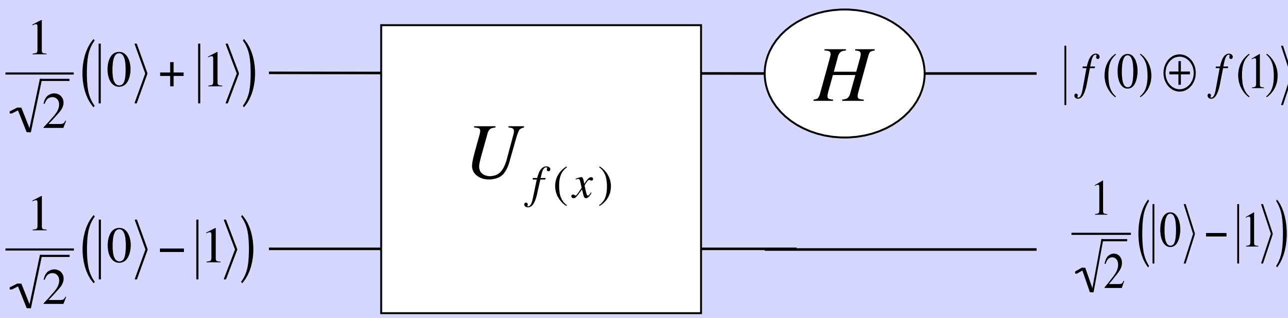
(not so magic version: Detsch-Jozsa algorithm, 1992)

Quantum Program

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



Execute the same program with a different initial state:



Measuring the state of the first qubit we discover if f(0)=f(1) ("global" property) IMPORTANT: We evaluated the function only once!!

$$\frac{1}{2}\Big(|0\rangle\otimes\big(|f(0)\rangle-|1\oplus f(0)\rangle\big)+|1\rangle\otimes\big(|f(1)\rangle-|1\oplus f(1)\rangle\big)\Big)$$

$$\frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle\Big)\otimes\frac{1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)$$

What is the main obstacle?

Extreme sensitivity to interaction with outside environment:

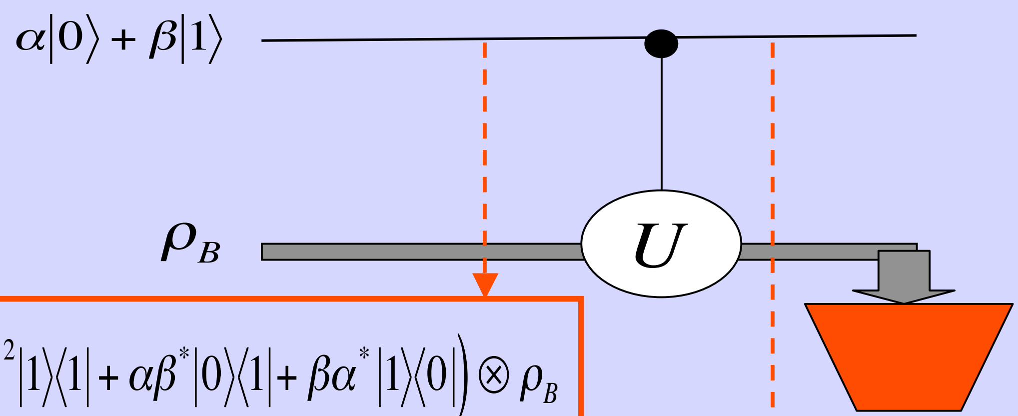
Decoherence: Due to interaction with environment, quantum computer "colapses" into a classical one (loosing all its advantadges).

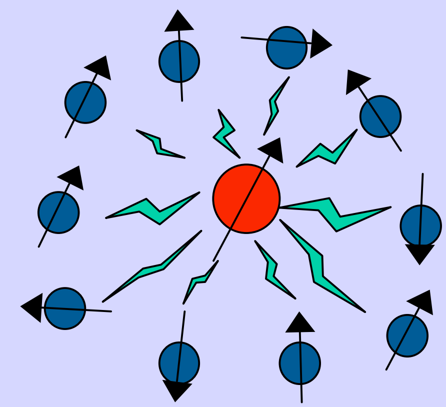
This can be fixed (possible but not easy)

Quantum error correcting codes

Fault tolerant quantum computation

DECOHERENCE IS THE ENEMY OF QUANTUM INFORMATION PROCESSING





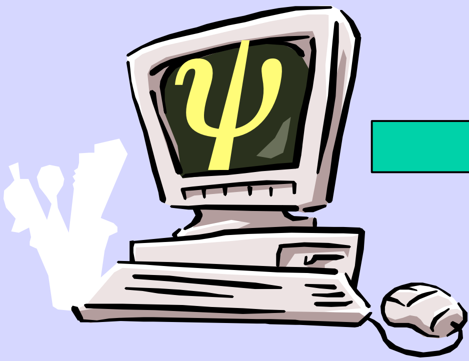
$$\rho_{AB} = \left(|\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| + \alpha\beta^*|0\rangle\langle 1| + \beta\alpha^*|1\rangle\langle 0|\right) \otimes \rho_B$$

$$\rho_{AB} = |\alpha|^2|0\rangle\langle 0| \otimes \rho_B + |\beta|^2|1\rangle\langle 1| \otimes U\rho_B U^+ + \alpha\beta^*|0\rangle\langle 1| \otimes \rho_B U^+ + \beta\alpha^*|1\rangle\langle 0| \otimes U\rho_B$$

$$\rho_A = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| + \alpha\beta^*|0\rangle\langle 1| Tr_B(\rho_B U) + \beta\alpha^*|1\rangle\langle 0| Tr_B(\rho_B U)$$

QUANTUM BIT + DECOHERING ENVIRONMENT = CLASSICAL BIT

BUILDING A QUANTUM COMPUTER IS VERY HARD



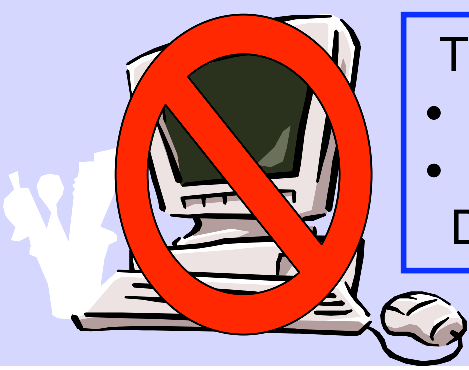
"DiVincenzo commandments"

I. Scalable set of qubits
II. Easy initialization
III. Universal operations
IV. Long decoherence time
V. Easy final readout

2030??

Feynman: We need quantum computers to simulate the behavior of physical systems

Simulate quantum systems in classical computers is hard!
40 spin 1/2 particles requires $O(2^{40})$ bits of memory



THE BEST WE CAN DO WITH CLASSICAL COMPUTERS:

- Deterministic algorithms: 32 spins!
- Non-deterministic algorithms: 100 x 100 spins!

DYNAMICS OF A QUANTUM SYSTEM IS REALLY HARD

Quantum Computers

US Roadmap: http://www.qipc.lanl.gov.

EU Roadmap: ftp://ftp.cordis.lu/pub/ist/docs/fet/qip2-34.pdf

QC ROADMAP

time

- (physical) qubit
  - creation and readout
- single qubit operations
  - Rabi flops, decoherence
- two-qubit operations
  - two qubit gate, decoherence, gate tomography, [Bell]
- operations 3-10 qubits
  - simple quantum algorithms, error correction, decoherence free subspace, [GHZ, teleportation]
- 2007 — one logical qubit
- 3-10 logical qubits
  - 2012 — fault tolerant operations

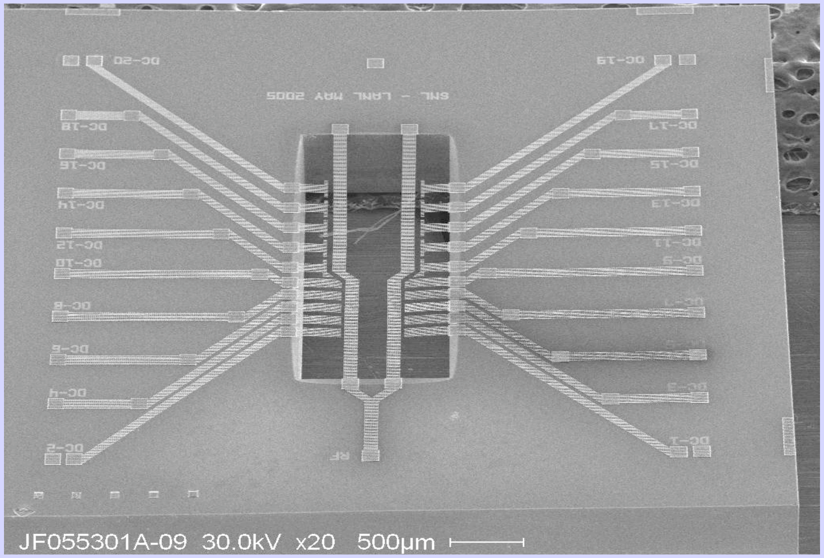
criteria:

✓ achieved in lab

✓ expected to work

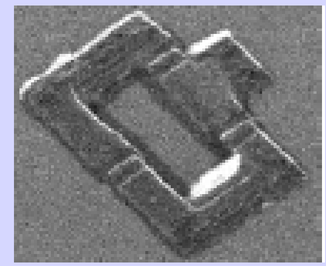
✓ not know how to (road block)

CANDIDATES FOR QUANTUM COMPUTERS

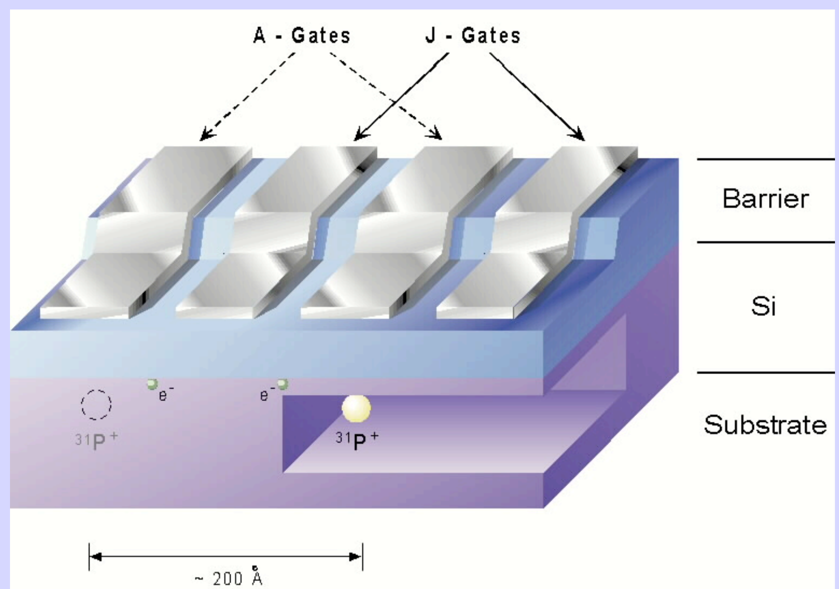


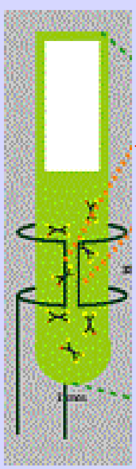
New micro-fabricated ion traps

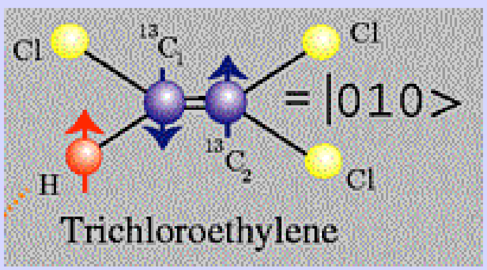
Superconductors



Silícon based ideas (P in Si)



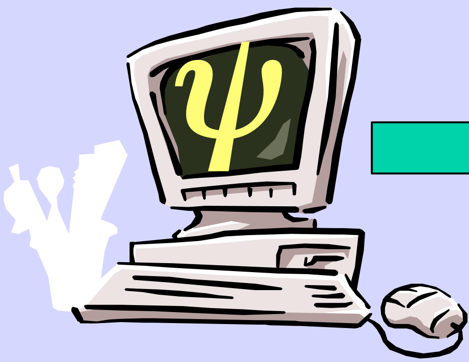




Nuclear Magnetic Resonance

THERE IS AN INTERMEDIATE STATION

Solve interesting quantum physics problems using controllable quantum hardware
QUANTUM SIMULATORS: Controllable system that can imitate/simulate others



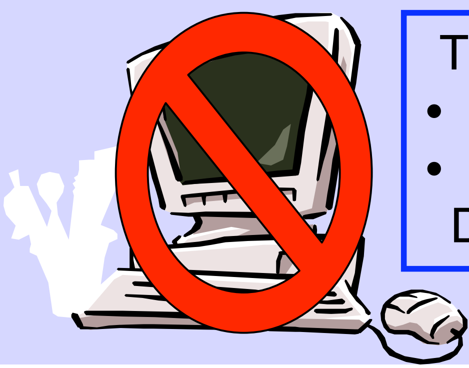
"DiVincenzo commandments"

I. ~~Scalable~~ set of qubits
II. Easy initialization
III. ~~Universal~~ operations
IV. Long decoherence time
V. ~~Easy~~ final readout

2030??

A QUANTUM SIMULATOR IS NOT A UNIVERSAL QUANTUM COMPUTER
BUT CAN SOLVE INTERESTING PROBLEMS. WHICH ONE?

Simulate quantum systems in classical computers is hard!
40 spin 1/2 particles requires $O(2^{40})$ bits of memory



THE BEST WE CAN DO WITH CLASSICAL COMPUTERS:

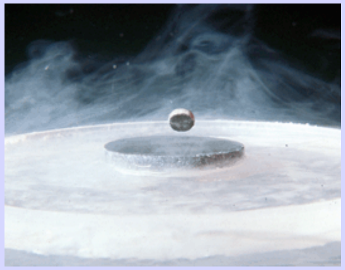
- Deterministic algorithms: 32 spins!
- Non-deterministic algorithms: 100 x 100 spins!

DYNAMICS OF A QUANTUM SYSTEM IS REALLY HARD

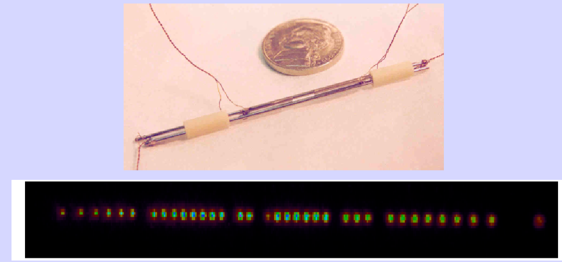
WHAT IS A QUANTUM SIMULATION?

A process that is ultimately implemented in a specific hardware

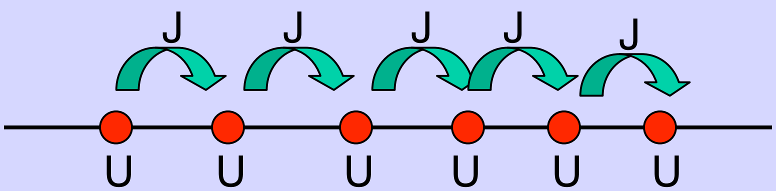
Physical problem



Quantum simulator hardware: Ion trap

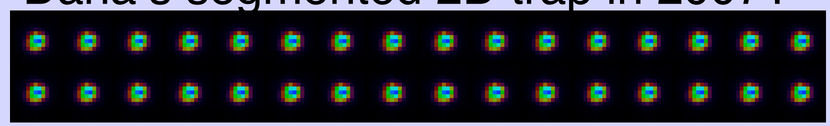


Model (caricature!): Hubbard



Real World

Dana’s segmented 2D trap in 2007?

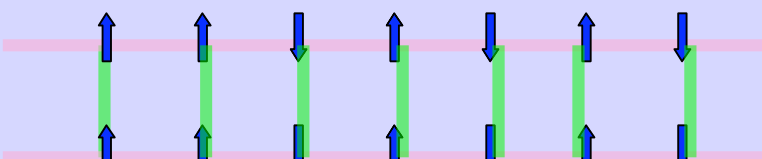


Simulation algorithm:

Mapping onto different model adapted to hardware

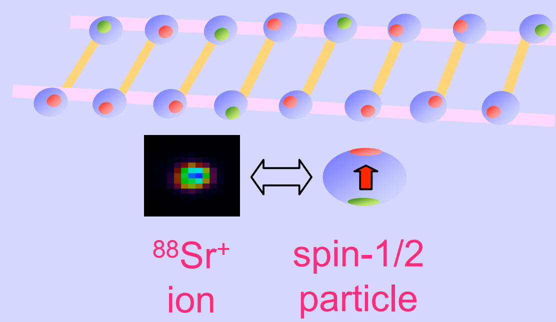
Physical implementation:

Ions & lasers



1D Hubbard = Ladder of spin 1/2’s

(Ortiz-Batista, LANL)



Perspectives on Quantum computation (or why is this interesting?)

- **Shift in computational paradigm: A new way to compute (inspired by physics). New algorithms? (other than factoring).**

- **Use most counterintuitive aspects of quantum physics.**
- **Experiments probe the boundary between quantum and classical worlds as never before.**
- **Experiments require amazing control over individual quantum systems (single atoms, etc).**

- **Quantum Technology. Is it realistic?**
  A big effort is under way.
  Motivation? Factoring: Code breaking…
  Timescale: >20 years? INTERMEDIATE STEPS!

computers: Status of the race…

New Frontiers in Quantum Information With Atoms and Ions

Both the precision control of trapped-ion systems and very large samples of cold neutral atoms are opening important new possibilities for quantum computation and simulation.

J. Ignacio Cirac and Peter Zoller

during recent years. Those systems include single photons, nuclear spins of donor atoms in doped silicon, superconducting Josephson junctions in both the charge- and flux-quantization regimes, semiconductor quantum dots, nuclear magnetic resonance samples, and electrons floating on liq-

38 March 2004 Physics Today

A big effort is under way.
Motivation? Factoring: Code breaking…
Timescale: >20 years? INTERMEDIATE STEPS!