Quantum Information and Quantum Computation

http://www.qubit.org/

Jonathan Jones

Jonathan.jones@qubit.org

Information

The Information Age

Communication

Shannon

Computation

Turing

Current approaches are essentially classical

which is wrong "…because Nature isn't classical dammit!" (Feynman)

Classical Information

- Classical information is made up of bits, which can be in either of two states, 0 and 1

- Bits can (in principle) be measured perfectly
- Bits can be measured without disturbance
- Bits can be copied without restriction
- Local manipulations cannot affect other distant bits

Qubits

- Bits can be mapped to the energy levels ("eigenstates") $|0\rangle$ and $|1\rangle$ of a two state quantum system (a qubit)
- If a qubit is confined to its eigenstates then it behaves just like a classical bit
- But qubits are not confined to eigenstates: they can exist in superpositions of these states opening up entirely new forms of information processing!

Quantum Information

- Qubits can be in two different states at the same time
- Qubits cannot be measured perfectly
- Qubits cannot be measured without disturbance
- Qubits cannot be copied
- Local manipulations on one qubit can affect other distant qubits (the EPR "paradox")

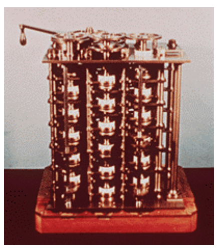
Quantum "technologies"

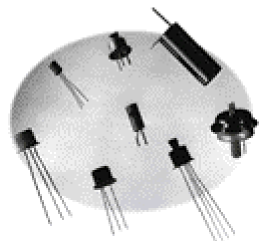
- Quantum Communication: quantum dense coding, quantum cryptography, quantum teleportation
- Quantum Computing: surpassing the classical limits
- Quantum Mechanics: insights into the foundations of quantum theory

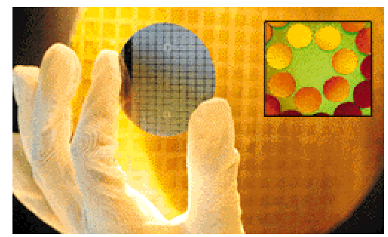
Quantum Computing: Outline

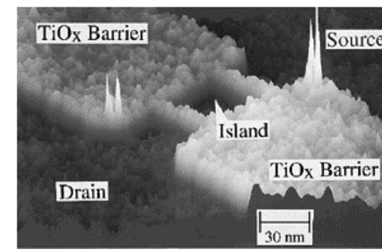
- What's wrong with classical computing?
- What could quantum computing offer?
- How can we build a quantum computer?
- What have we achieved so far?
- How far can we go?

Moore's law









1 m

100 nm

Every eighteen months computers double in speed (tenfold every five years!)

But faster computers must be smaller

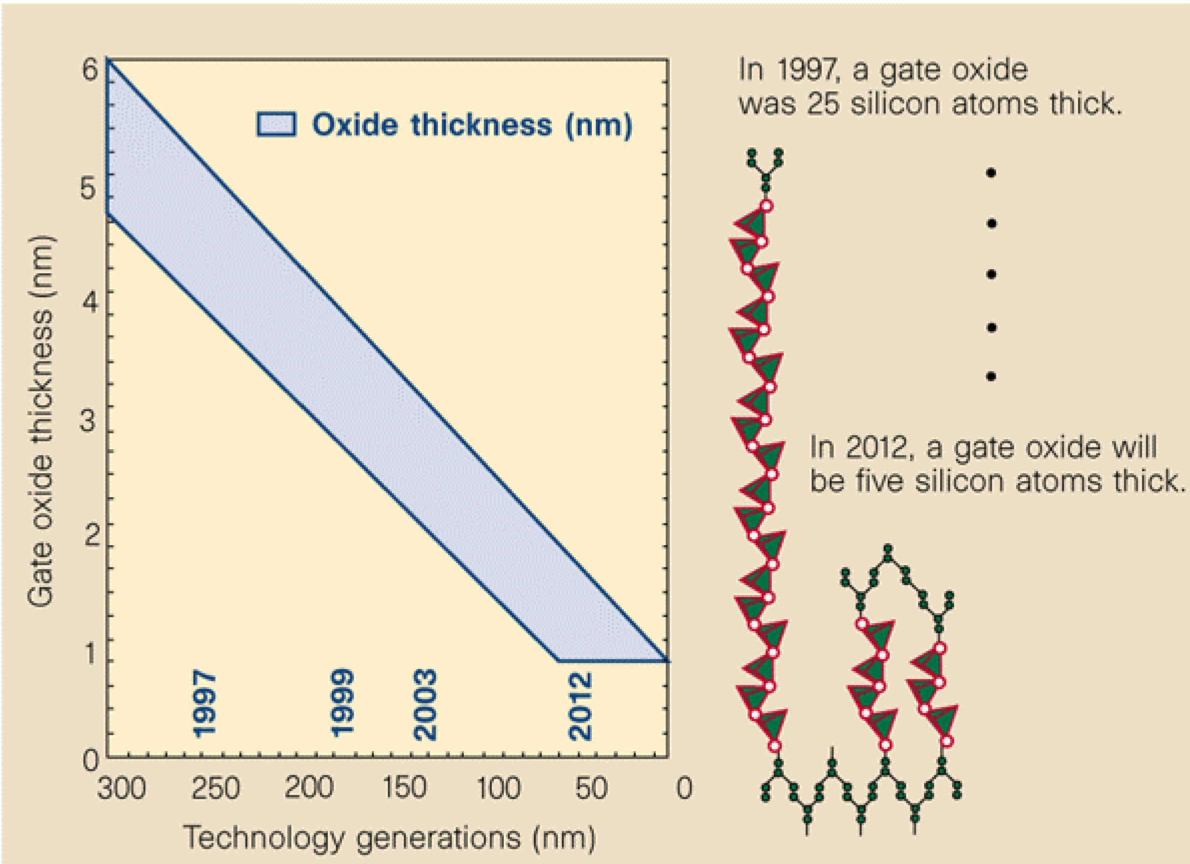
The Semiconductor Roadmap

Year	1999	2002	2005	2008
DRAM half pitch	180	130	100	70
Accuracy	65	45	35	25
Gate length	140	85–90	65	45
Accuracy	14	9	6	4
Oxide layer	1.9–2.5	1.5–1.9	1.0–1.5	0.8–1.2
Junction depth	42–70	25–43	20–33	16–26

1999 SIA Roadmap: from *Nature* **406** 1023 (2000)

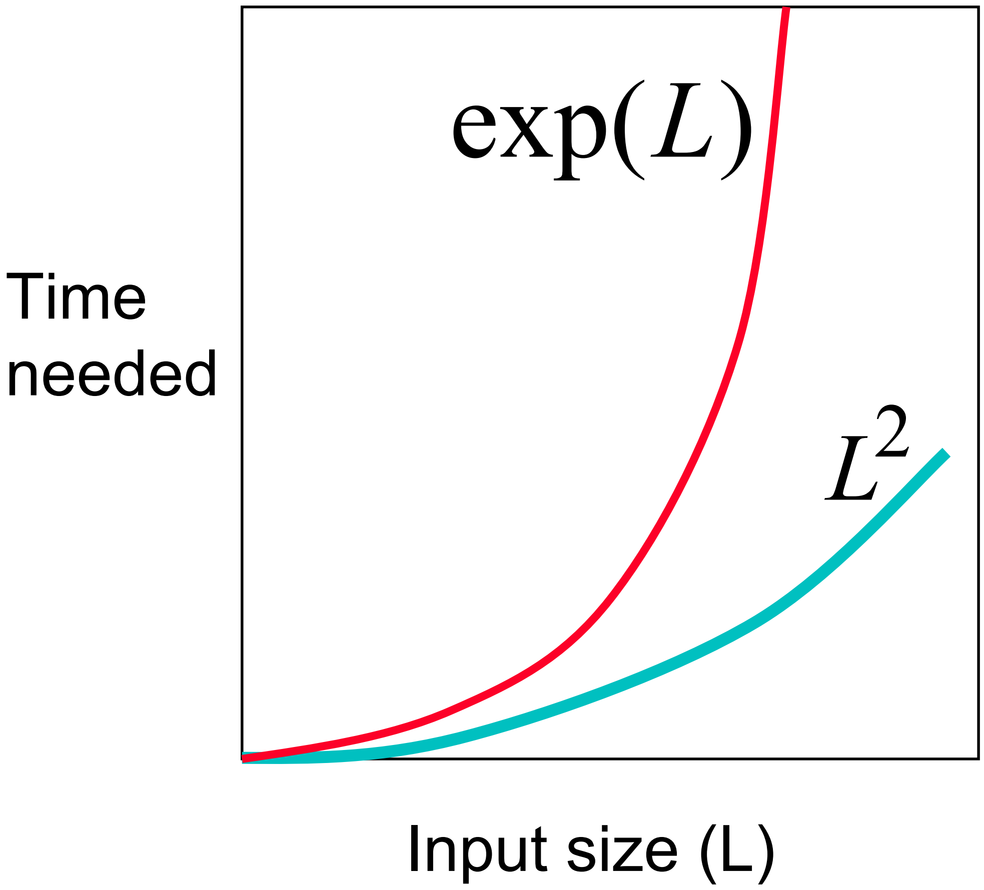
At some point in this decade current approaches to building computers will run into major problems.

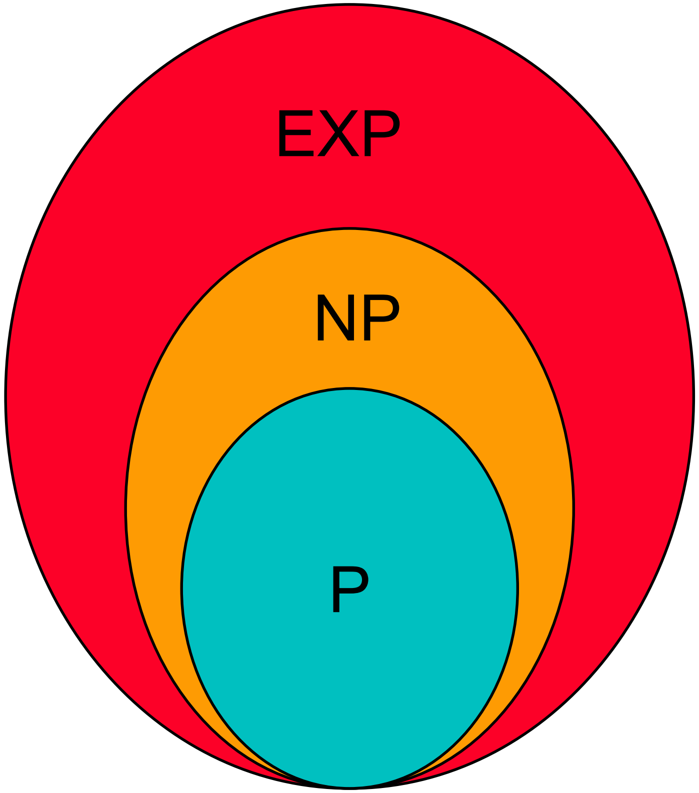
The end of the road?



By 2012 (?) our current approach will run into major problems

Computational complexity



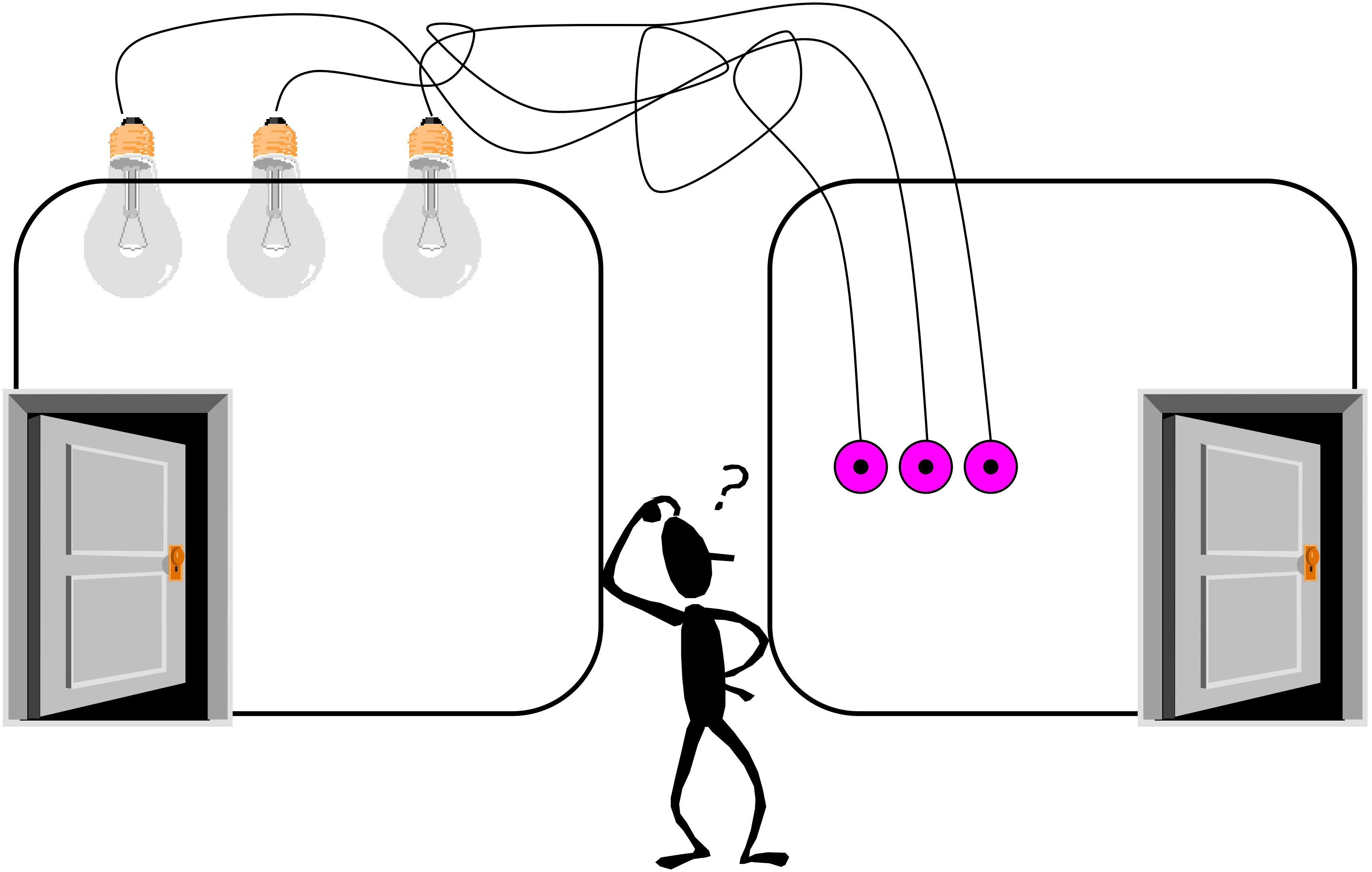


Turing, Church, Feynman

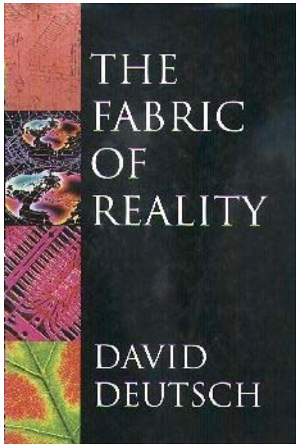
- All reasonable models of computation are equivalent to Turing machines
- Computation is an abstract process whose limits are set by mathematics

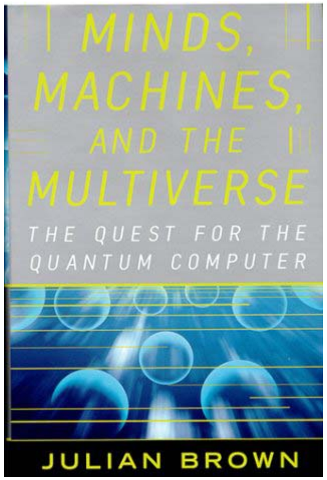
- Computation is a real physical process: the limits to computation are set by physics
- Quantum and classical physics are *different*

Computation is physical!



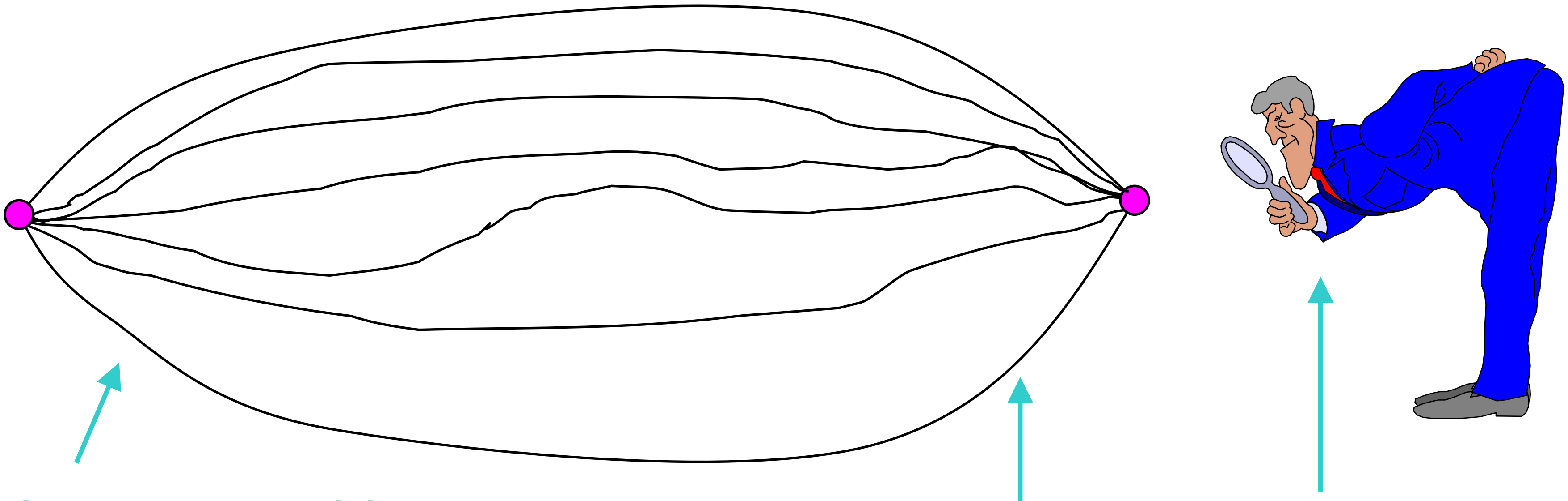
Parallel universes





- When a quantum object can do two things it does both—in different universes
- Parallel universes can evolve separately and then be brought back together (interference)
- Makes quantum mechanics difficult and makes quantum information interesting!

Quantum complexity leads to

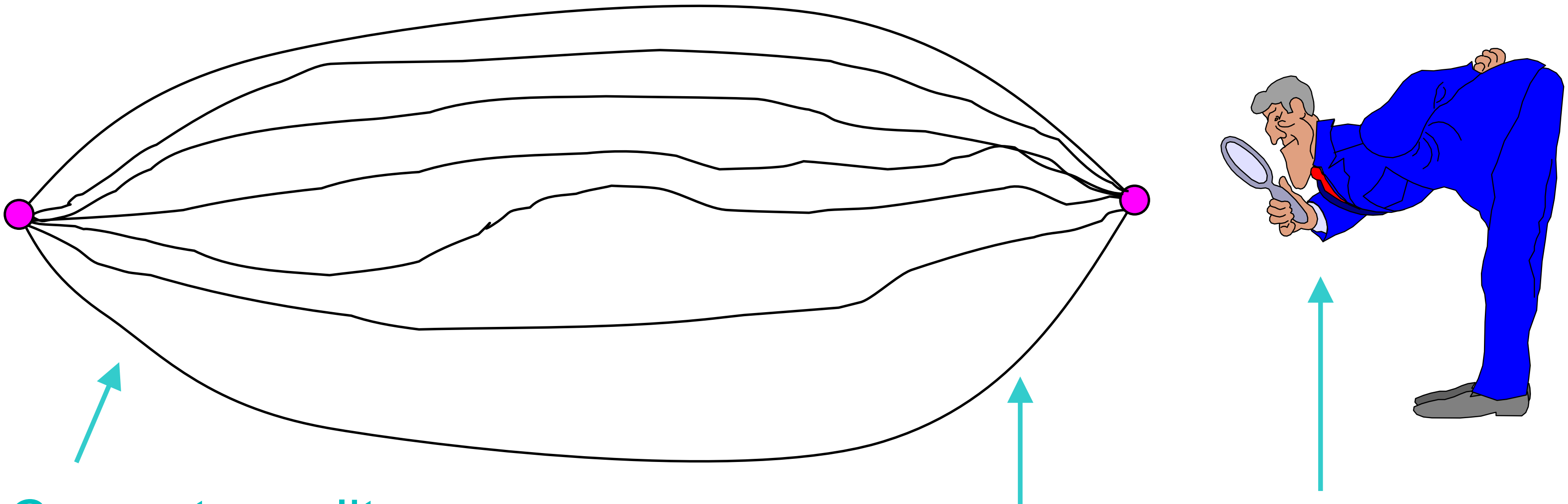


A quantum object splits up into many different parallel universes, each of which behaves differently

Parallel universes recombine and interfere to produce the final result

Look at it!

… quantum parallelism



Computer splits up into many different parallel universes, each of which does a computation

Parallel universes recombine and interfere to produce one answer

Look at final answer!

Qubits & quantum registers

Classical Bit

0 or 1

Quantum Bit

0 or 1 or 0 1

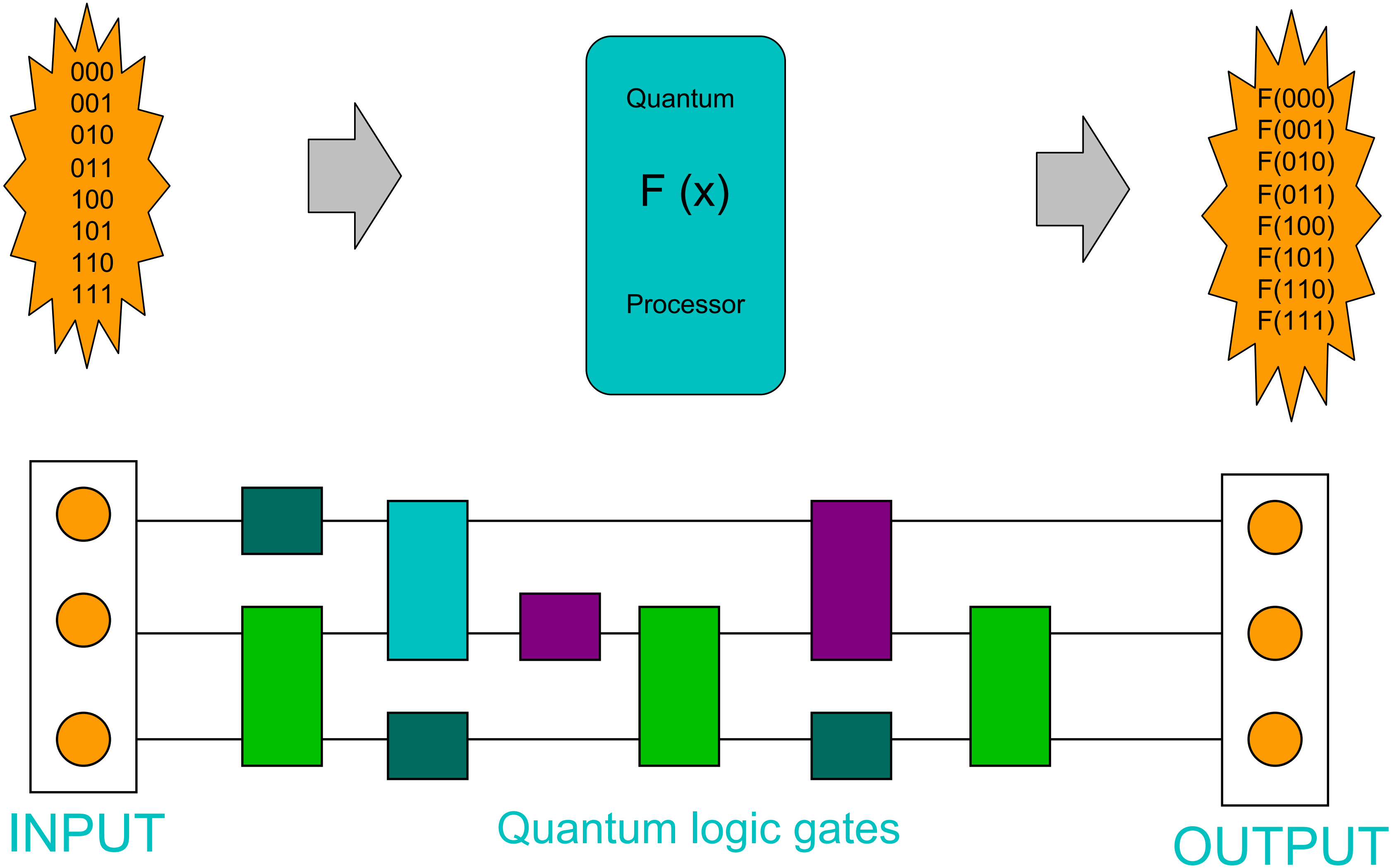
Classical register

101

Quantum register

000 001 010 011
100 101 110 111

Quantum parallel processing



The science bit

- *From Cbits to Qbits: Teaching computer scientists quantum mechanics*, N. David Mermin, *Am. J. Phys.* **71,** 23-30 (2003)

http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html

The science bit

- *From Cbits to Qbits: Teaching computer scientists quantum mechanics*, N. David Mermin, *Am. J. Phys.* **71**, 23-30 (2003)

Table I.

CLASSICAL versus QUANTUM BITS	Cbits	Qbits
States of n Bits	$\|x\rangle_n$, $0 \le x < 2^n$	$\sum \alpha_x \|x\rangle_n$, $\sum \|\alpha_x\|^2 = 1$
Subsets of n Bits	Always have states	Generally have no states
Reversible operations on states	Permutations	Unitary transformations
Can state be learned from Bits?	Yes	No
To get information from Bits	Just look	Measure
Information acquired	x	x with probability $\|\alpha_x\|^2$
State after information acquired	Same: still $\|x\rangle$	Different: now $\|x\rangle$

Exponential growth

Qubits	*Universes (Calculations)*
1	2
2	4
4	16
8	256
16	65536
32	4294967296
64	18446744073709551616
128	340282366920938463463374607431768211456
256	1.16×10^{77}
512	1.34×10^{154}

Getting the answer out…

- Quantum computers could perform vast numbers of computations in parallel
- But we can't access all that power directly! At the end of the day we can only read out a single result
- Quantum algorithms are all about extracting small pieces of useful information which are hard to compute in other ways

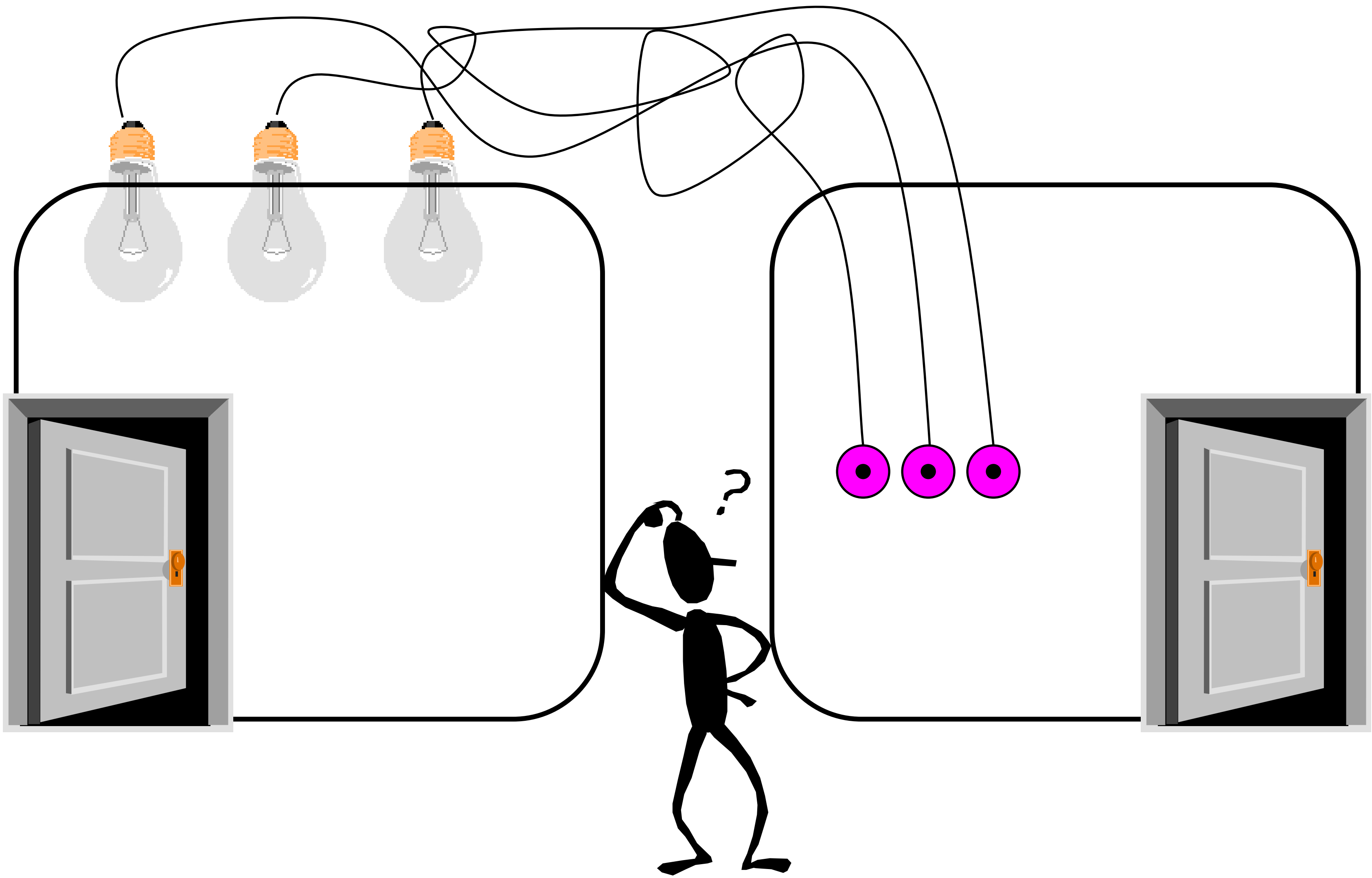
Deutsch's algorithm

- Suppose we have a coin which is either a real coin (with a head and a tail) or a trick coin (with two heads or two tails)
- To distinguish real and trick coins we would normally need to look at both sides separately and compare the two results
- Using quantum methods we can look at both sides in a single glance!

What could we do with one?

- Simulate quantum mechanics in complex systems: from astrophysics to zoology
- Factorise big numbers with Shor's algorithm: the end of classical cryptography?
- Speed up searches: Grover's algorithm
- Quantum computing is not the answer to everything

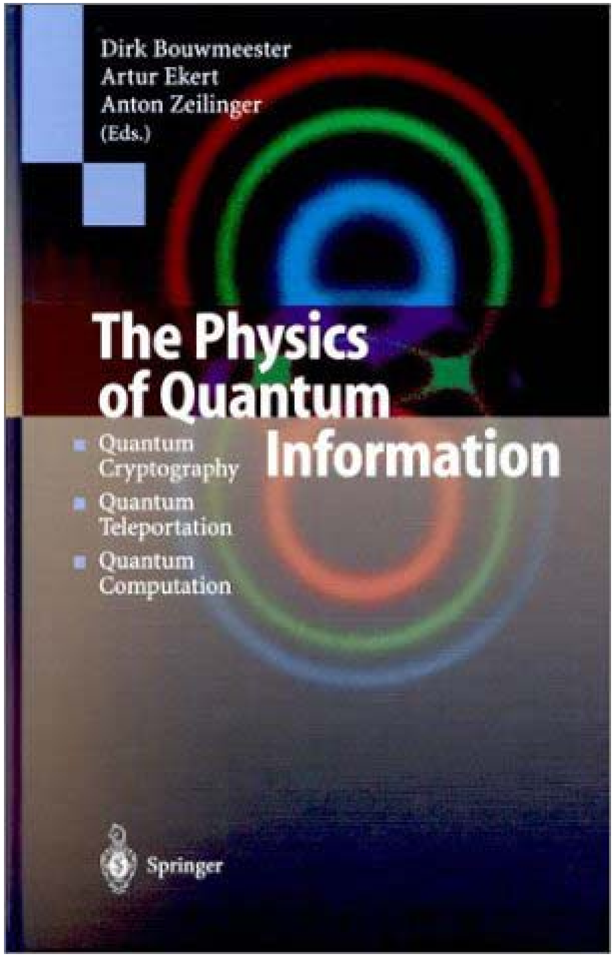
Computation is physical!



How might we build one?

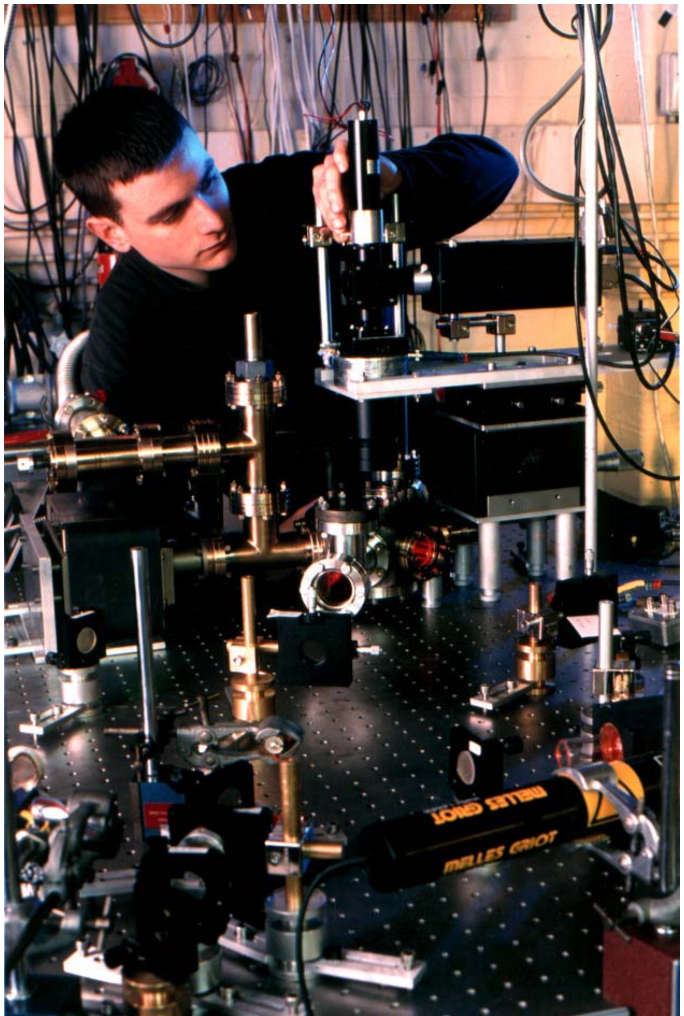
- To build a quantum computer you need
- Quantum objects (to act as qubits),
- Interacting strongly with one another (to build logic gates),
- Isolated from the environment (stable), but
- Accessible from the outside world for input, output and control
- Small quantum computers (2–7 qubits) already exist!

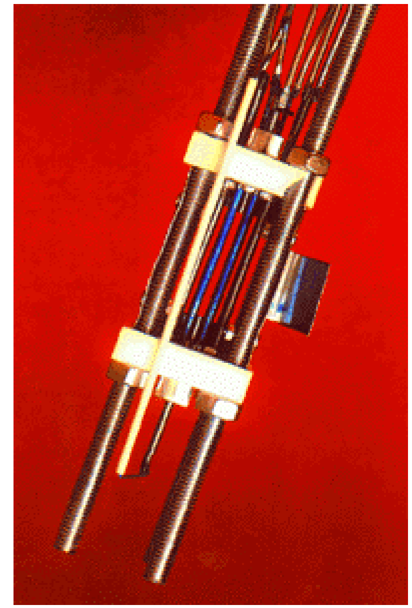
Experiments



- Photons: communication
- Ion traps: early promise
- NMR: current leader
- Solid state: many blue skies proposals—the way of the future?

Ion experiments





NMR experiments

Solid state proposals

- Widely felt that any “real” quantum computer will be a solid state device
- Huge range of proposals involving quantum dots, SQUIDs, single spin NMR/ESR, etc.
- Some schemes have demonstrated single qubit devices; others are just paper proposals
- All extremely speculative, but we should have a better idea in 5-10 years time

Scaling systems up

- NMR is fine for small demonstration systems, but hard to scale up beyond 10-20 qubits
- Limits of ion traps are similar but less clear
- Estimates suggest that quantum computers with about 300-1000 qubits could outstrip classical designs
- Error correction schemes seem to impose an overhead of 10-100, raising the size to 3000+
- We need better technologies

Summary

- Quantum mechanics provides a new way of looking at information (technologies)
- Classical computation runs out quite soon, but quantum computation might allow us to go beyond current limits
- NMR provides a fine technology for building small quantum computers, but we will need new approaches to build quantum computers large enough to be really interesting