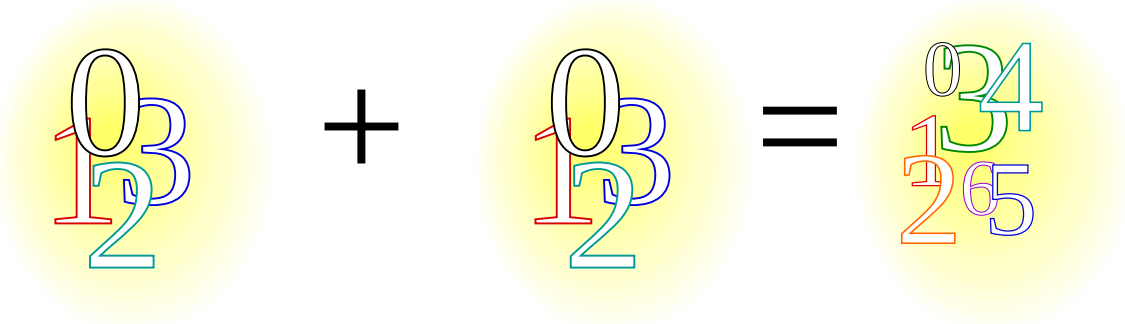
Quantum Information Seminar
Centre for Quantum Information
Department of Physics

Loughborough University



What is Quantum Computation?

John Samson, Department of Physics

Quantum Information

Transistors in classical computers rely on quantum mechanics for their operation. *This does not make them quantum computers!*

Processor has limited knowledge of information being processed.

Quantum computing

- n-bit register in superposition of states: massively parallel computation on 2^n numbers simultaneously
- Only n bits of information can be extracted
- Toy quantum computer exists

Quantum communication and cryptography

- Secure communication protocols
- Secure key distribution; eavesdropping evident
- Now a working technology

Quantum teleportation

- Transfer of quantum state from one photon or atom to another
- Neither sender nor receiver can know state
- Verified experimentally

Outline

Classical computer architecture, complexity of algorithms
Quantum information, qubits, superposition, measurement
Quantum computers, gates, algorithms, requirements

Department of Philosophical Engineering

A prehistory

1900 Planck radiation law

1905 Einstein proposes photon as quantum of em radiation

1925 Heisenberg matrix mechanics

1926 Schrödinger wave mechanics

1927 Copenhagen interpretation of quantum mechanics:
QM predicts observations; does not describe what is

1930 Einstein-Bohr debates: “God does not play dice”

1935 EPR Gedankenexperiment to show QM incomplete

1957 Everett “many worlds” interpretation

1964 Bell inequalities: QM incompatible with local reality

1982 Aspect performs EPR experiment: QM √, reality ×

1982 Feynman proposes quantum computer

1989 Penrose hypothesises brain as quantum computer

1994 Shor algorithm for factorisation on quantum computer

1997 Grover algorithm for database search

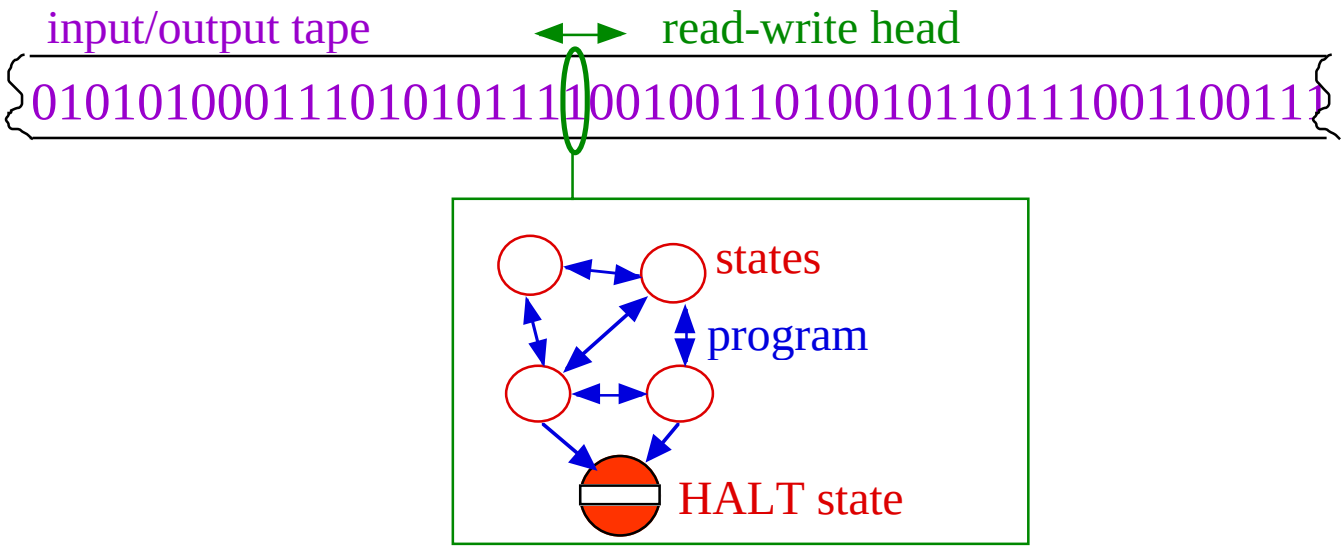
1997 Quantum key distribution demonstrated over 27 km

1997 Quantum teleportation of photon

2001 IBM reports factorisation of 15 on 7-qubit quantum computer

Classical computer

Turing machine



Church-Turing thesis: A Turing machine can perform any algorithm.

Any classical computer can be simulated by a Turing machine.

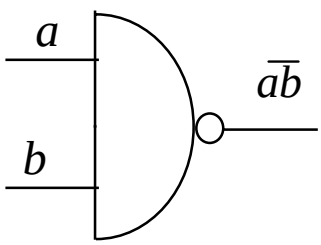
Brain can (Turing)/cannot (Penrose) be simulated by a Turing machine.

Quantum computer cannot be simulated by a Turing machine.

Architecture

- Unit of classical information is the **bit**, b = 0 or 1.
- n-bit register can hold one of 2^n numbers, N = 0 or 1 or … or 2^n–1.
- Bits manipulated by logic **gates**, e. g., NAND:

a	b	$\overline{ab}$
0	0	1
0	1	1
1	0	1
1	1	0



Complexity

Some algorithms take longer than others. To perform an operation on n bits on a *classical* computer:

Class P: Algorithm takes polynomial time

$$T < A\, n^k,$$

where A and k are fixed constants.

E. g., multiplication of two n-bit numbers.

- Long multiplication is polynomial with k=2.
- FFT algorithm for multiplication with $k = 1 + \varepsilon$, any $\varepsilon > 0$.

Class NP: (nondeterministic polynomial)
Proposed solution can be verified in polynomial time, but there may be no general polynomial time algorithm to find it. Used for public key cryptography.

E. g., factorisation of n-bit prime product.

- Exhaustive search takes time ~ $2^{n/2}$
- No (known) polynomial time algorithm
- Factors can be verified in polynomial time

Undecidable: No algorithm exists.

E. g., halting problem: does a given Turing machine halt?

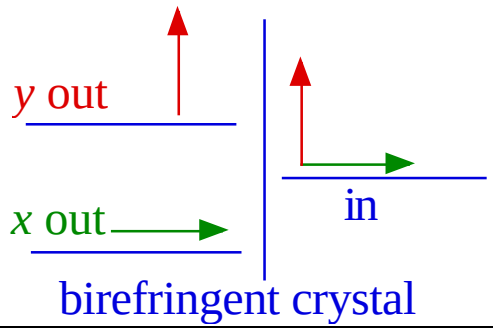
A quantum computer can do certain NP problems in polynomial time. It can't solve undecidable problems.

Quantum Information

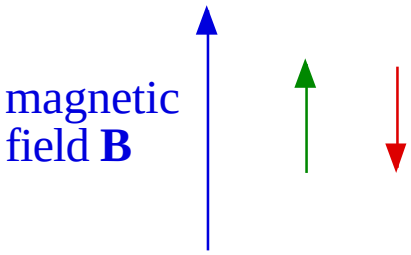
Unit of quantum information is the **qubit** (pronounced *'kju: bɪt*), aka **two-state system**.

Two basis states $|1\rangle$ and $|0\rangle$:

Polarisation state of single photon
horizontal or vertical
$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$



Spin projection of electron
$S_z = +\frac{1}{2}\hbar$ or $S_z = -\frac{1}{2}\hbar$



Atom in ground state or excited state
Current in mesoscopic ring clockwise or anticlockwise
Charge distributions in quantum dots
…

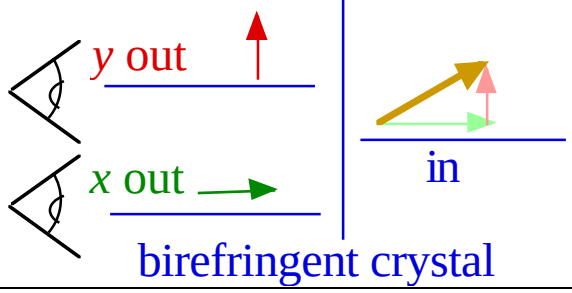
Superposition and interference

Fundamental difference between bits and qubits:

A qubit can be in a superposition of the two basis states

Linear polarisation

$$\begin{pmatrix} \cos\ \theta \\ \sin\ \theta \end{pmatrix}$$

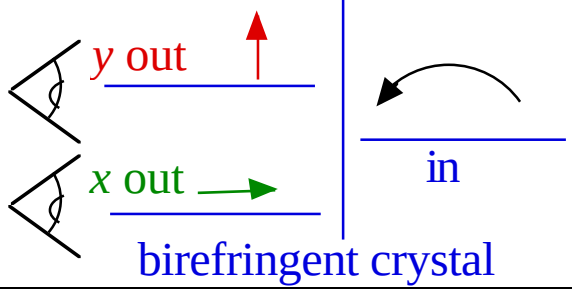


Input beam of light of intensity I:
intensity $I \cos^2 \theta$ in x channel, $I \sin^2 \theta$ in y channel.

Single photon, detectors in each channel: Photon observed in x channel with probability $\cos^2 \theta$, in y channel with probability $\sin^2 \theta$
$\cos^2 \theta + \sin^2 \theta = 1$

Circular polarisation

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$$



Photon observed with probability 1/2 in either channel

Interference

If channels are recombined without measurement, original state reconstructed

Photon follows both paths! (Parallelism)

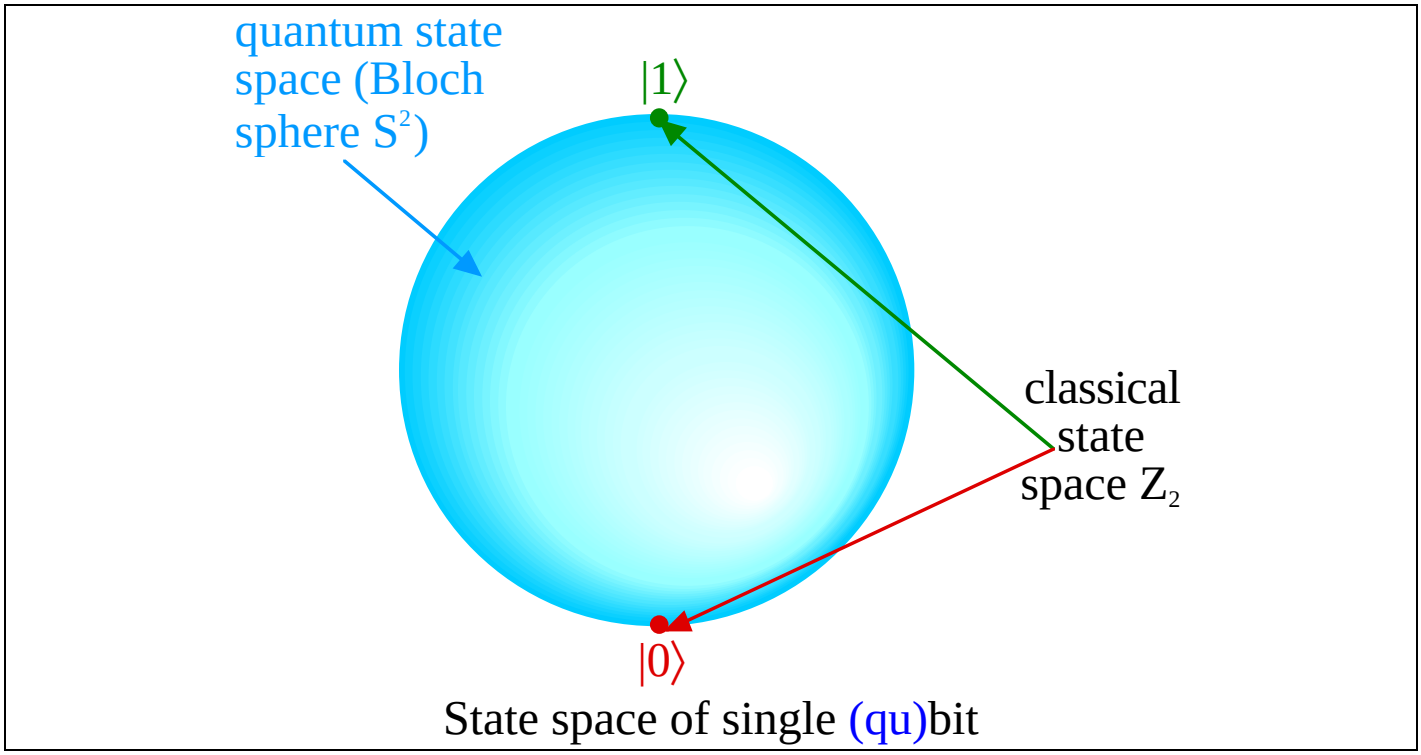
General state (elliptical polarisation)

$\begin{pmatrix} a \\ b \end{pmatrix}, |a|^2 + |b|^2 = 1$

a, b complex, overall phase arbitrary

Represented as point on Bloch sphere (living in Hilbert space)

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{1}{2}\theta\right) \\ \sin\left(\frac{1}{2}\theta\right) e^{i\varphi} \end{pmatrix}$$



State space of single (qu)bit

☺ Much more information in qubit than c-bit

☹ Measurement can only yield one classical bit

- Choose basis (x/y, left/right, etc) representing orthogonal polarisations (antipodal points on Bloch sphere)
- Find photon in one or other channel with certain probability

Postulates of quantum mechanics

Quantum information

State vector (with N complex components) contains all the information about the system

Quantisation

Measurement of any quantity can only give N different outcomes (extract $\log_2 N$ bits of information)

Probability

Probability of result of measurement determined by state vector

Wave function collapse

After measurement state is known (but might have been changed)

Schrödinger

Time evolution is given by a unitary matrix $U(t)$
(i. e., $N \times N$ matrix with $UU^\dagger = 1$, or complex rotation)

Quantum Computer

Multi-qubit states

1 qubit: 2 complex amplitudes (for 0 and 1)
2 qubits: 4 complex amplitudes (for 00, 01, 10 and 11)
n qubits: 2^n complex amplitudes (for 00…0, 00…1 to 11…1)

(Direct product of *n* Hilbert spaces, $\mathbb{C}^{2^n}$)

Vast amount of information!

↗: equal amplitude of 0 and 1

↗↗: equal amplitude of 00, 01, 10 and 11

↗↗…↗: equal amplitude of 2^n numbers

Moore's law: power of a typical computer doubles every 18 months.
To satisfy this you only need add one bit every 18 months!

20-qubit computer can operate on 1M numbers in parallel…
…but you can only ask twenty questions of the output

- How to implement operations?
- What algorithms are suitable?

Quantum gates

Any *classical* Boolean logic operation on n classical bits
f: $\{0,1\}^n \rightarrow \{0,1\}$
can be implemented using combinations of 2-bit NAND gates.

Any *quantum* computation on n qubits is a unitary transformation (rotation) in 2^n-dimensional space. It can be implemented using combinations of

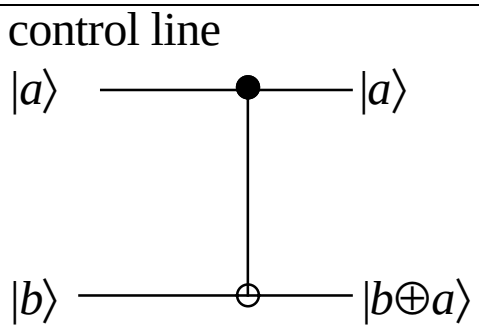
- arbitrary one-qubit transformations (rotate/reflect Bloch sphere)
  e. g. **NOT gate** and **Hadamard gate** ("square root of NOT")

$$\text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- certain two-qubit transformations, e. g. **controlled NOT**
  inverts qubit b iff qubit a is 1

IN		OUT	
a	b	a	$b \oplus a$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$\text{c–NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



(Gates must be reversible — can't lose information)

c-NOT results in entanglement of input bits — central resource in quantum communication: $|a\rangle|0\rangle \rightarrow |a\rangle|a\rangle$

Quantum algorithms

Shor (1994) algorithm to factorise integer N

1. Choose an x, $1 \leq x < N$, such that x and N have no common factors.
2. Find smallest positive r such that $x^r = 1 (\text{mod } N)$
3. One of $\gcd(x^{r/2} \pm 1, N)$ may be a factor of N

e. g. $N = 15$

1. Try $x = 4$
2. $4^1 = 4$, $4^2 = 16 = 1 \text{ mod } 15$, so $r = 2$
3. $4^{2/2} + 1 = 5$, $4^{2/2} - 1 = 3$: both are factors

Difficult step is step 2 (discrete logarithm problem, classically NP).
Solved by quantum Fourier transform: find period in time $O((\ln N)^3)$.

Implemented by IBM in Dec 2001 on 7-qubit computer to factorise 15

Grover (1997) database search

N bits, only one of which is 1. Find it.
Classical algorithm requires time of order N.
Quantum algorithm requires time of order $N^{1/2}$.

Simulations of quantum systems

Quantum computers may be most efficient way to simulate other quantum systems.

What is needed?

A quantum computer must satisfy the DiVincenzo checklist:

Physical system must have

- well-characterised qubits
- means of initialisation, say to 00…0
- quantum gates
- means of readout
- weak coupling to environment (slow decoherence)

Many proposed architectures:

- Quantum dots
- Josephson junctions
- Nuclear Magnetic Resonance
- Ion traps
- Atoms in optical cavities
- Nonlinear optics

Further reading

DiVincenzo D P, “The physical implementation of quantum computation”, *Fortschritte der Physik* **48**, 771 (2000)

Feynman R P, “Simulating Physics with Computers”, *Int J Theor Phys* **11**, 467 (1982)

Grover LK, “Quantum mechanics helps in searching for a needle in a haystack”, *Phys Rev Lett* **79**, 325 (1997)

Nielsen M A and Chuang I L, *Quantum Computation and Quantum Information* (CUP, 2000)

Shor P, *Proc 35th Annual Symposium on the Foundations of Computer Science*, ed Goldwasser S, 124 (IEEE Computer Society Press, Los Alamitos, 1994)

Vandersypen L M K *et al*, “Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance” *Nature* **414**, 883 (2001)

Centre for Quantum Information, Oxford http://www.qubit.org
Links http://www.physics.uq.edu.au/people/nielsen/info/index.html
Loughborough QI page http://www.lboro.ac.uk/departments/ph/qi.html