August 27, 2014

History of Quantum Computing

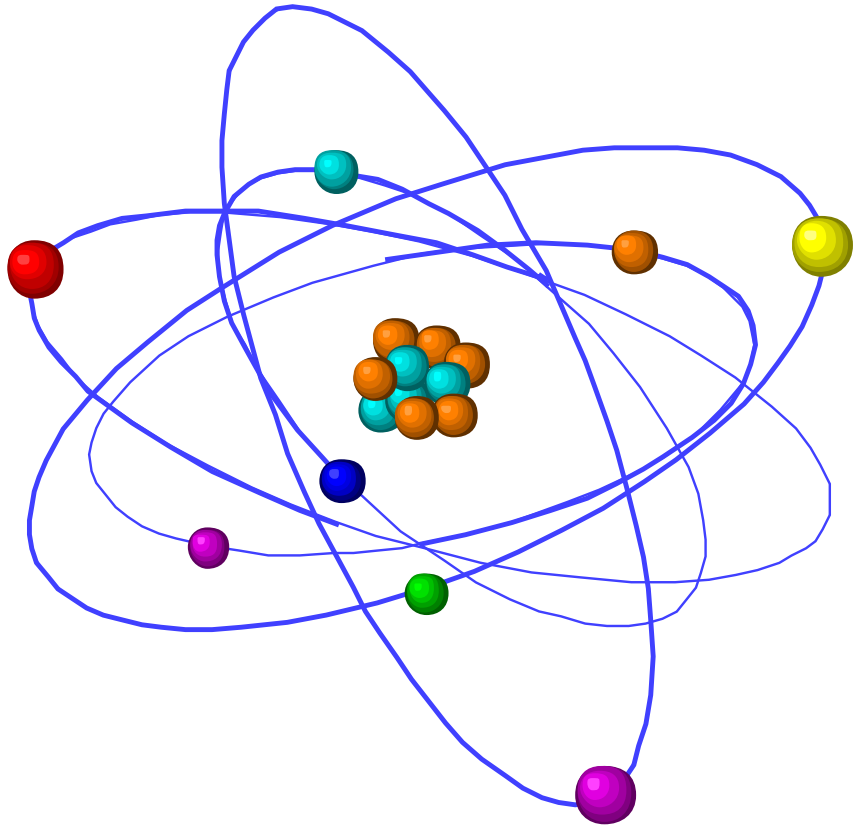
Dr Marie Ericsson,
Uppsala University

What is Quantum Mechanics?

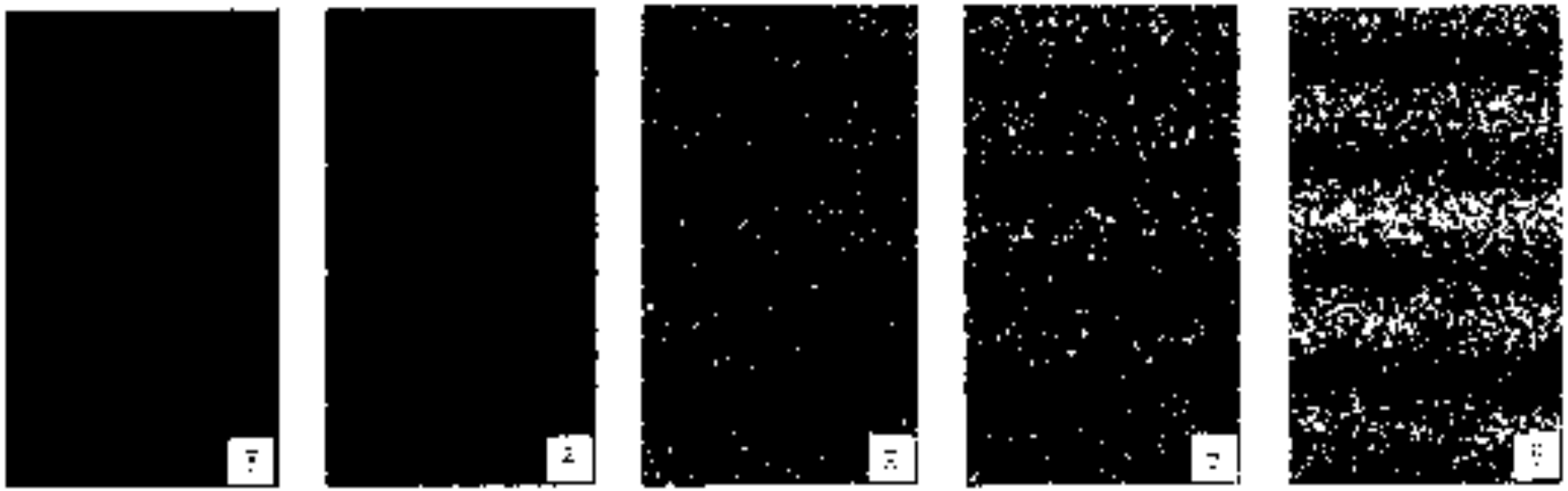
It tells us how the world looks like from an electron's perspective…

Picture from "Alice in Quantumland" by Robert Gilmore.

…. how atoms, electrons, photons and other microscopic particles behave.

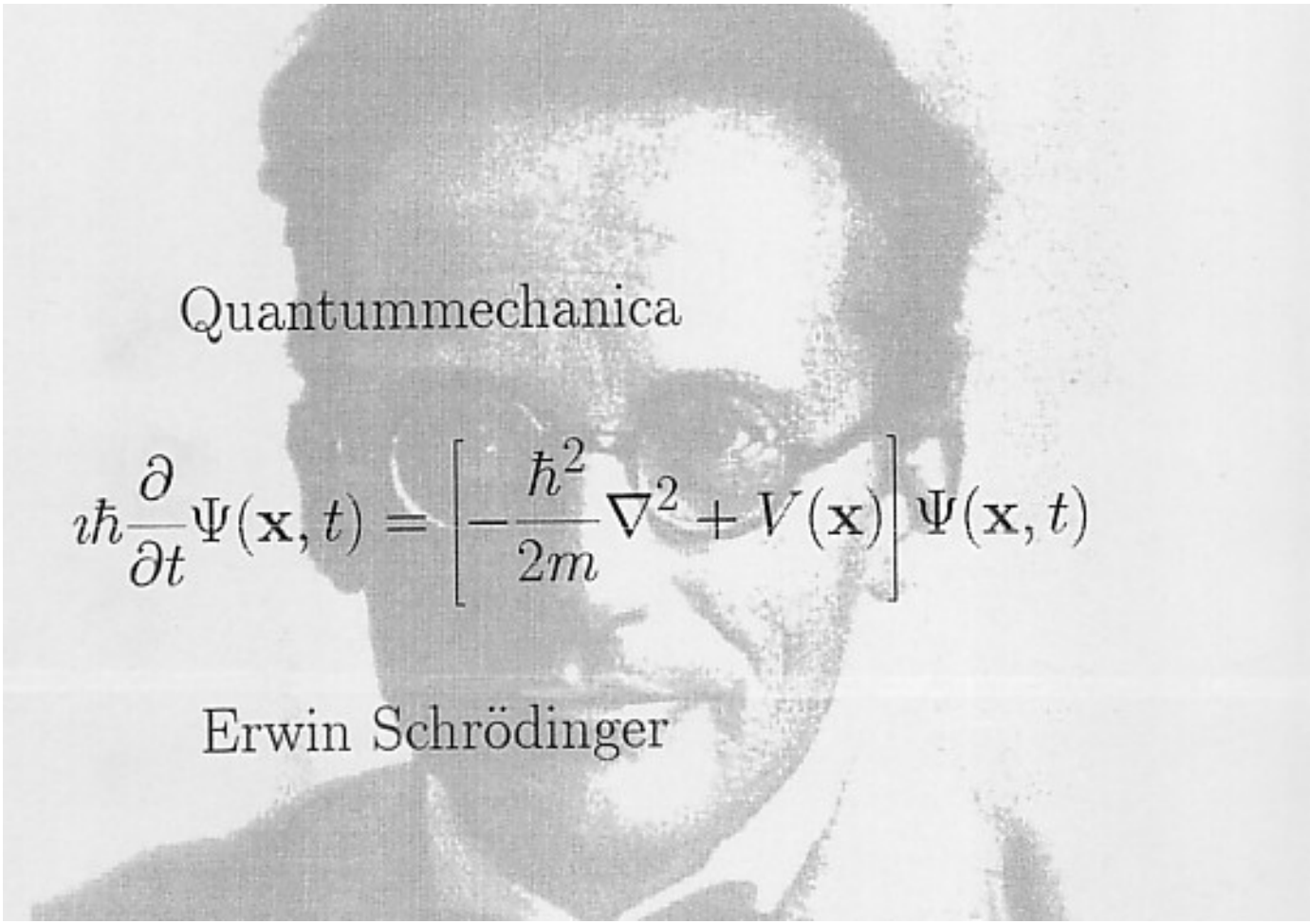


Matter particle-wave duality



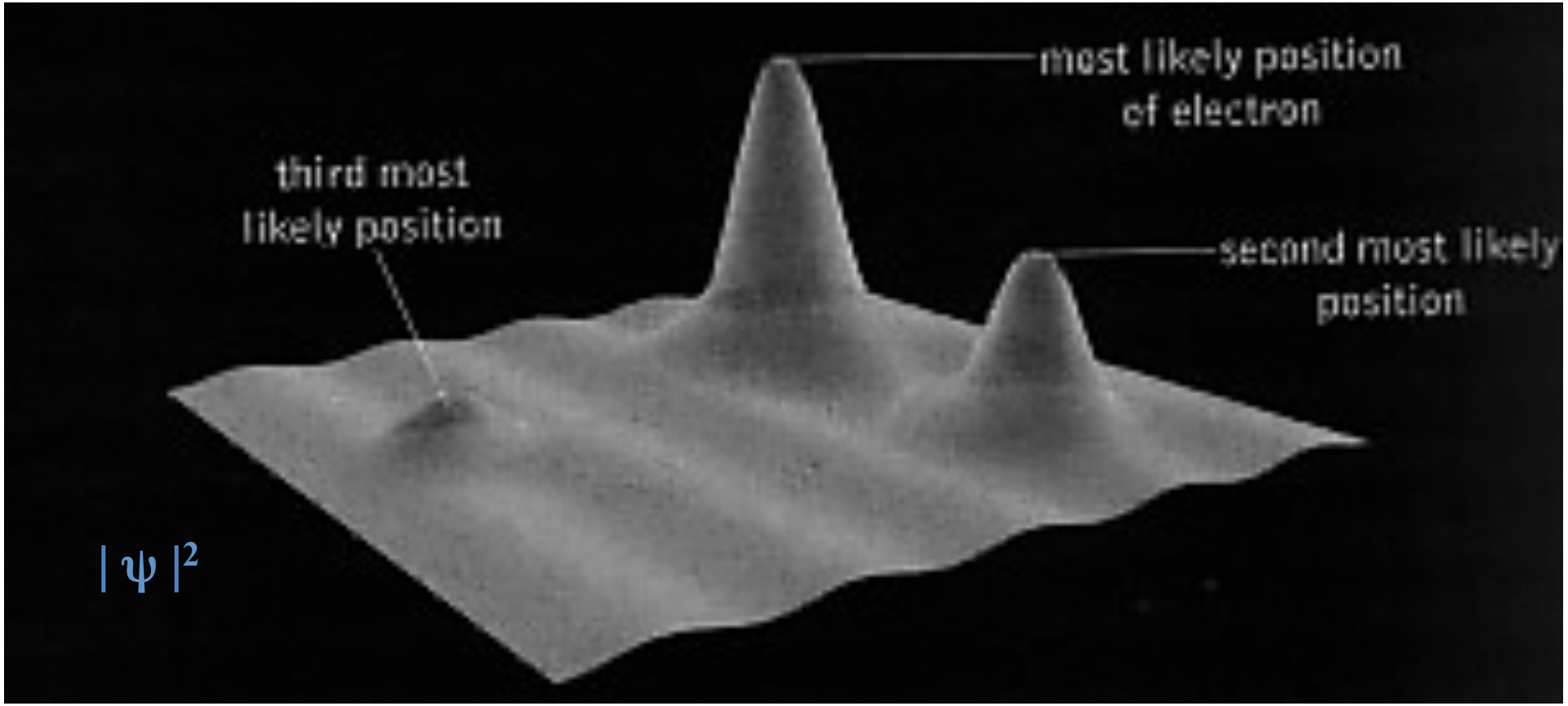
Double slit experiment with single electrons gives wave like interference pattern, like water waves going around two slits.

Schrödinger's Equation (1926)



$\Psi(\mathbf{x},t)$ is describing the quantum system, for example an electron.

But we don't see $\psi(x,t)$ in nature! $|\psi|^2$ gives the probability of finding the particle in a Particular position.



Measurement problem

Until an observation is made the position of a particle is described in terms of probability waves ψ, but after the particle is observed, it is described as a fixed value. Probabilistic theory!

Compare: is there a mirror image if no one is looking…

Strange features of quantum mechanics

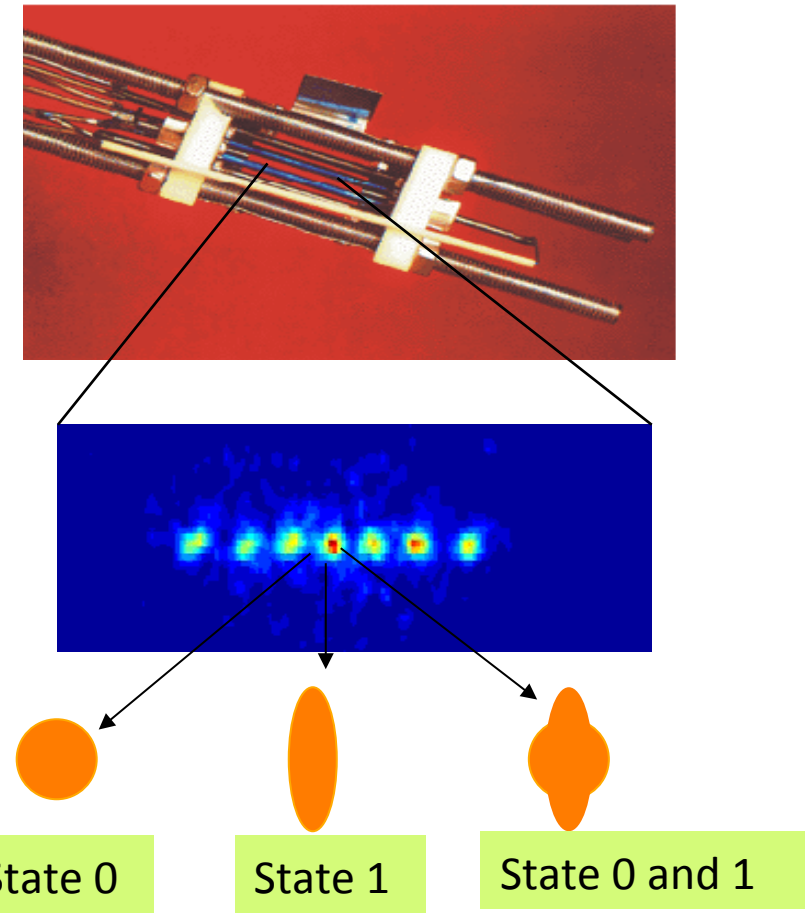
1. Probabilistic theory (if you don't believe in many worlds…). Even if all parameters of a system are known, it is impossible to predict the outcome of certain experiments. Einstein's objection "God does not play dice"

2. Quantum superpositions, being in two or more places at the same time! Can also include being in different energy states at the same time.

Superposition 1

An old woman smiling or a young lady with her head turned?

Superposition 2

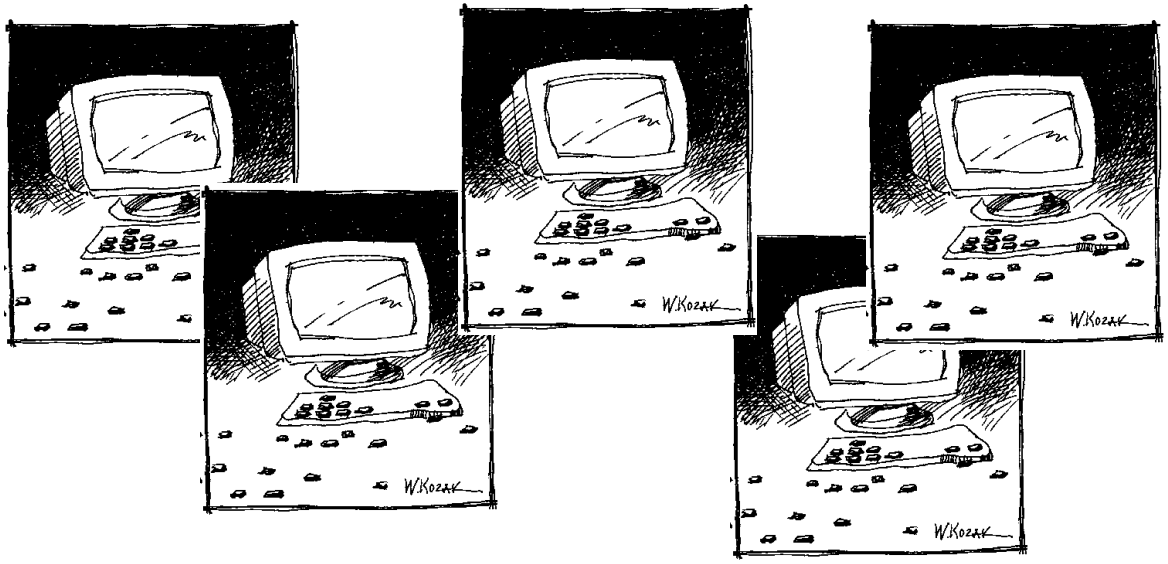


3. Entanglement. “Spooky action at a distance.” Correlation between two or more particles.

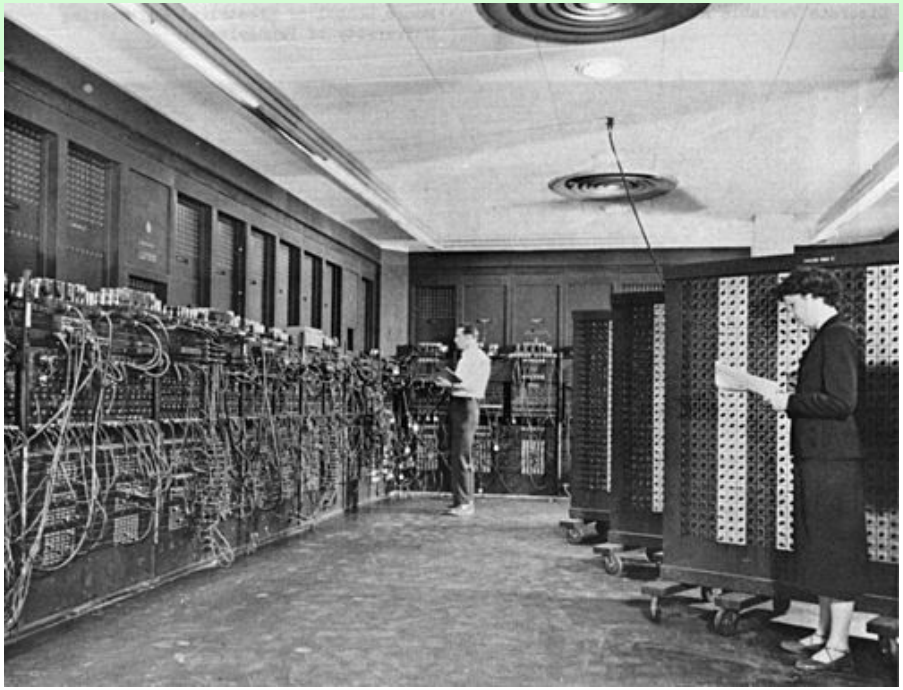
With entanglement we can move an unknown quantum state from one end of the universe to the other end with teleportation.

There are always correlations between the outcomes

"I think there is a world market for about five computers"
-- Remark attributed to Thomas J. Watson (Chairman of the Board of International Business Machines), 1943.

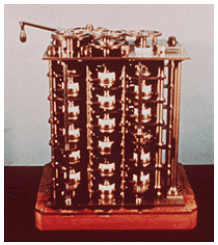


“The Eniac has 18 000 vacuum tubes and weighs 30 tons, we envisage in the future computers with 1000 tubes and of a weight of only 1 1/2 ton”-- Popular Mechanics, 1949.

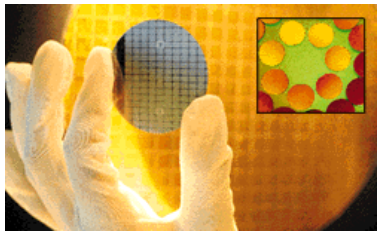


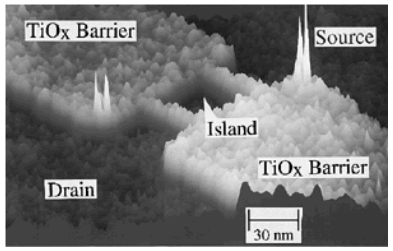
Information Technology

faster → smaller → shrinking computer

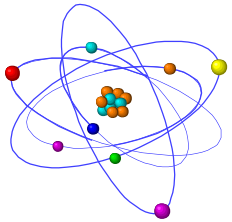


1 m





0.000000001 m



Quantum technology

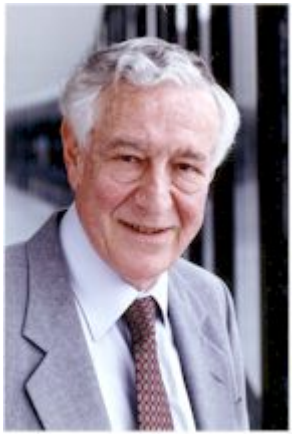
Moore's law:

Every 18 months microprocessors double in speed
IT evolves towards quantum mechanics

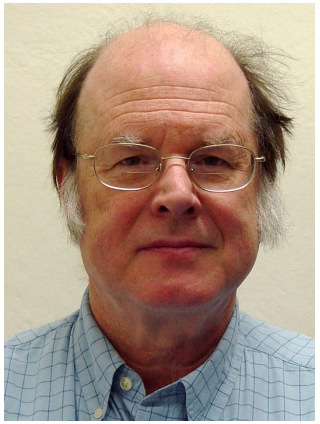
First steps - Reversible computation

Difficulties with small computers - Dissipation of heat!

Rolf Landauer showed 1961 that in irreversible computations, loss of information, makes the entropy increase and energy is dissipated in heat (see AND and XOR, two input and one output)



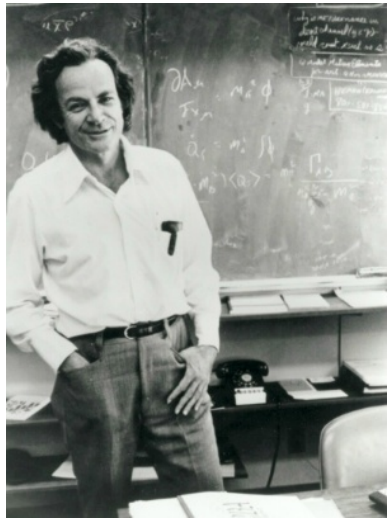
In 1976, Charles Bennett proved that it is possible to build a universal computer from reversible gates, for example the Toffoli gate.



What is a quantum computer:

- Computational device that use quantum mechanics to store and process information.
- It solves *some* problems more efficient than a classical computer, for example factoring large numbers.
- Can also be used to simulate quantum systems which can be used to better understand chemical and biological systems.

Early days of quantum computation



“There is nothing that I can see in the physical laws that says the computer elements cannot be made enormously smaller than they are now. In fact, there may be certain advantages.”

“There's Plenty of Room at the Bottom”
Richard Feynman, 1959

“Let's think of a more general kind of computer... “
He considered simulation of quantum-mechanical objects by other quantum systems

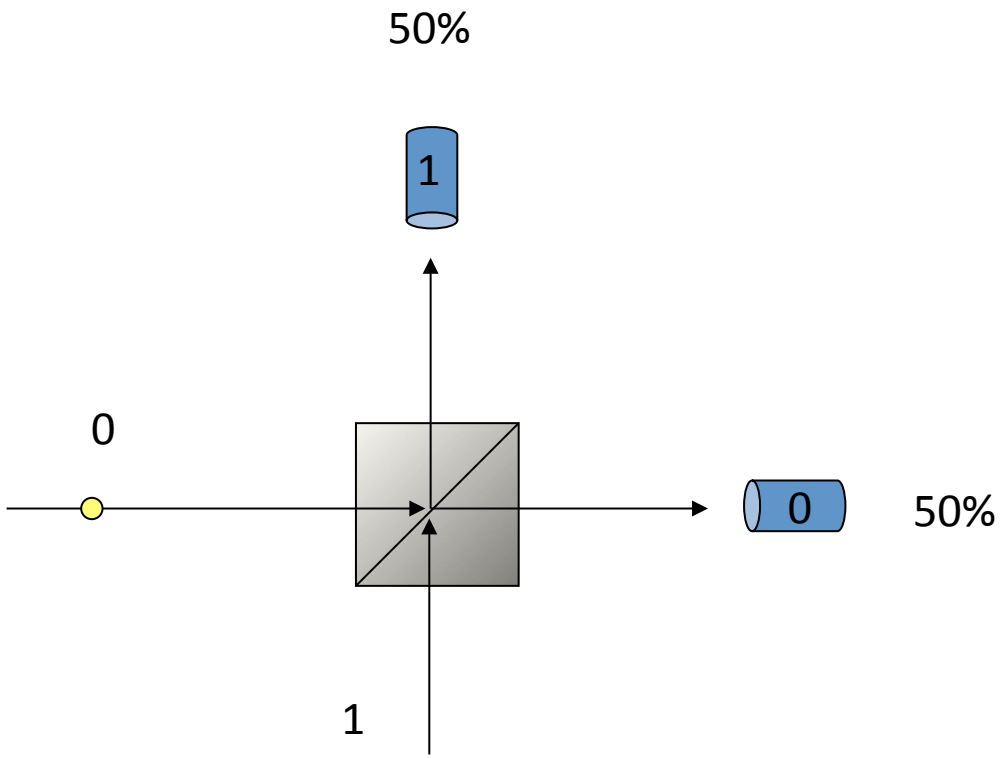
"Simulating physics with computers"
Richard Feynman, 1982

In 1985, David Deutsch, described the first universal quantum computer in his paper “Quantum theory, the Church-Turing principle and the universal quantum computer”.

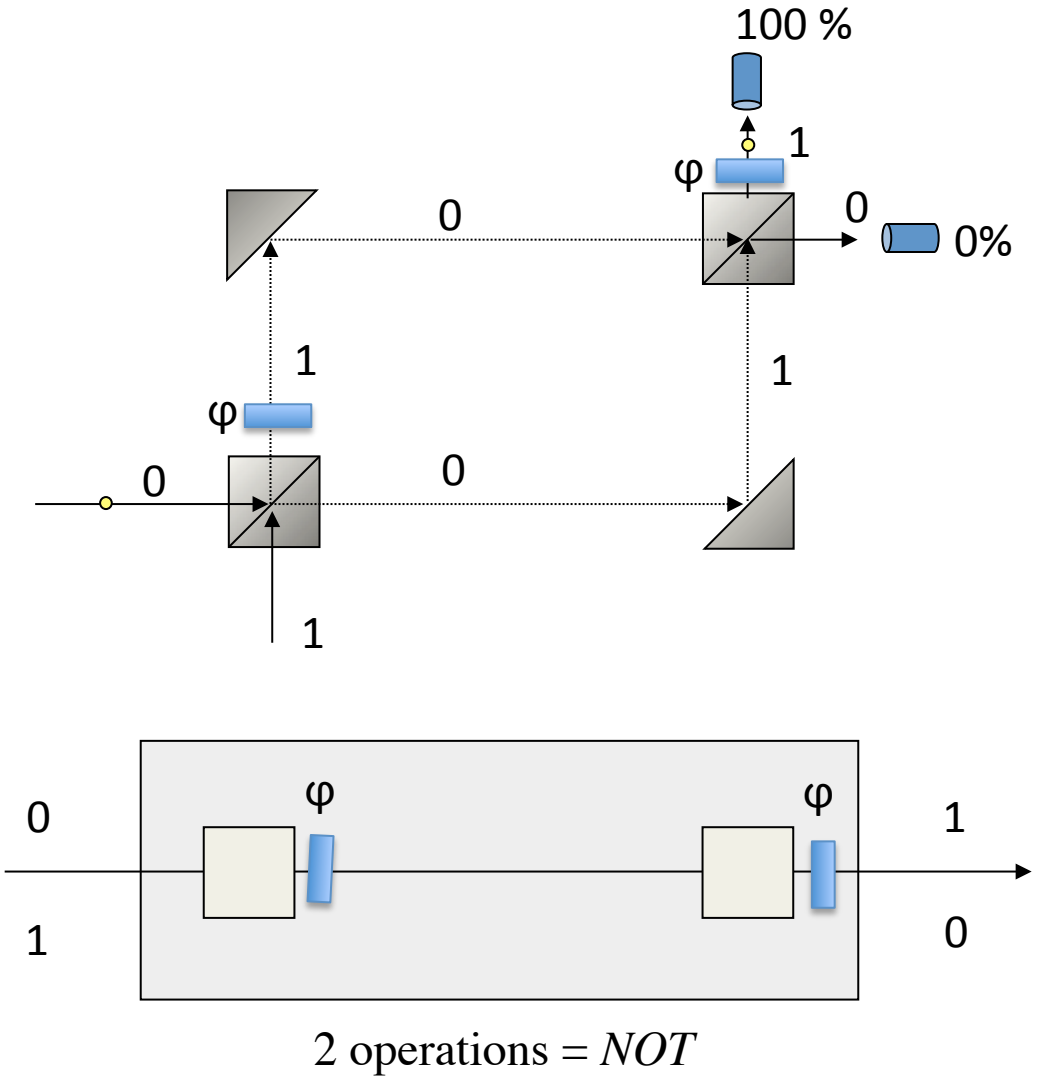
Any physical process could be modelled perfectly by a quantum computer.

This showed that computation is a physical process and not something mathematical.

Logic from physics…

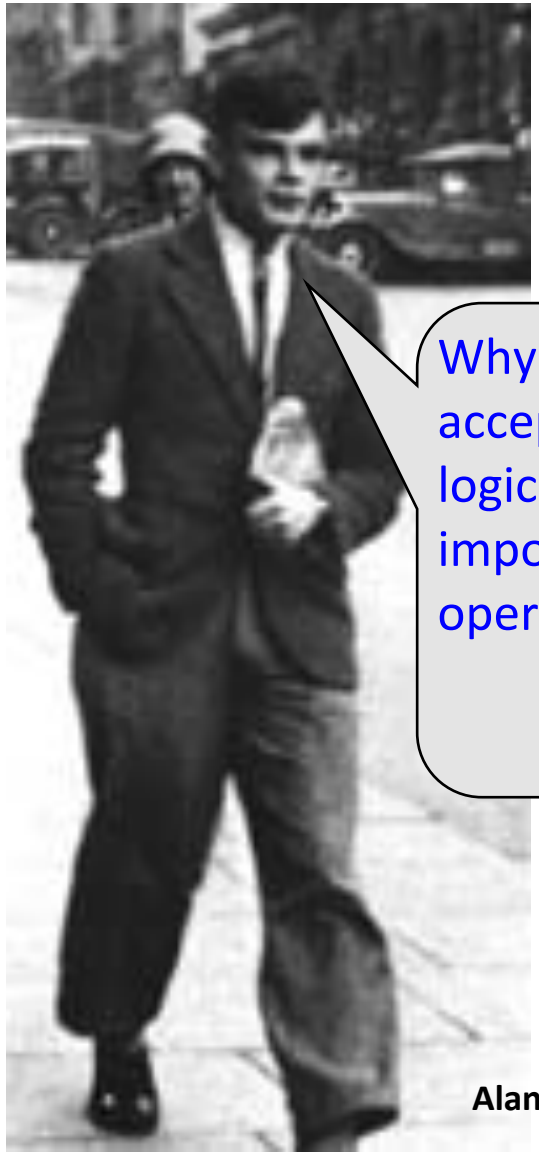


Logic from physics…



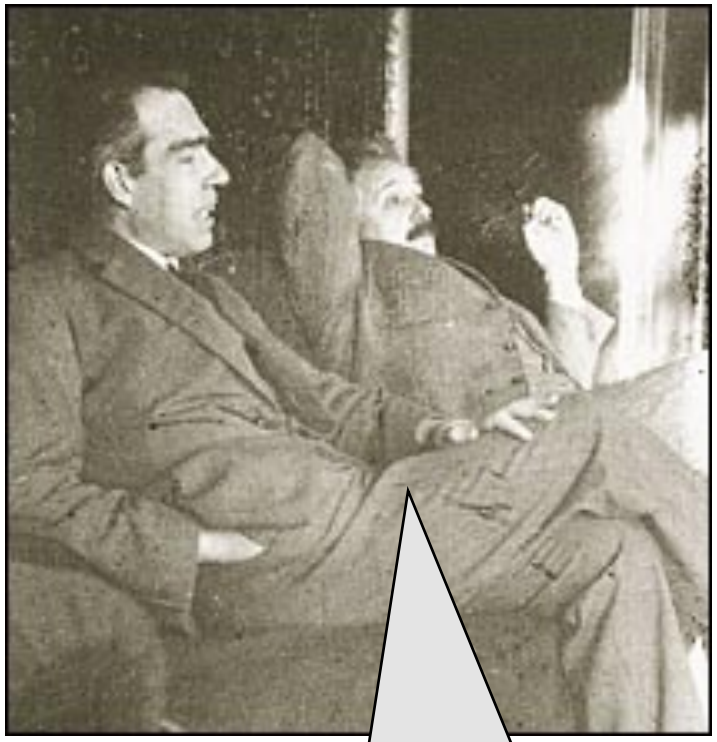
2 operations = *NOT*

Logic or Physics?



Alan Turing

Why shall I accept this logically impossible operation



Niels Bohr & Albert Einstein

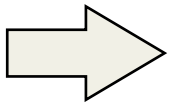
Because its physical representation does exist in nature!
It can be performed!

Qubits & Quantum Registers

Classical Bit

Quantum Bit

0 or 1



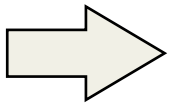
(0+1)

superposition

Classical register

Quantum register

101



000+001+010+100+
011+101+110-111

entanglement

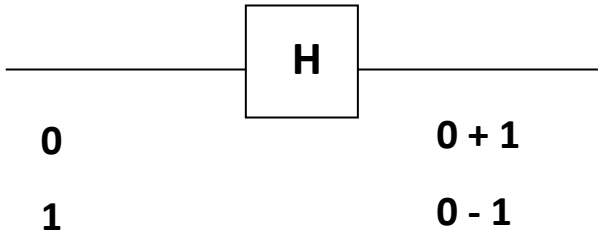
Many qubits

- N bits encode one number, for example 001
- One qubit encode 2 numbers, one for each input, 0+1
- N qubits encode 2^N numbers (2,4,8,16,32,…)
- N=1000, more information than the number of atoms in the universe ($2^{1000} \approx 10^{300}$)
- Quantum parallelism

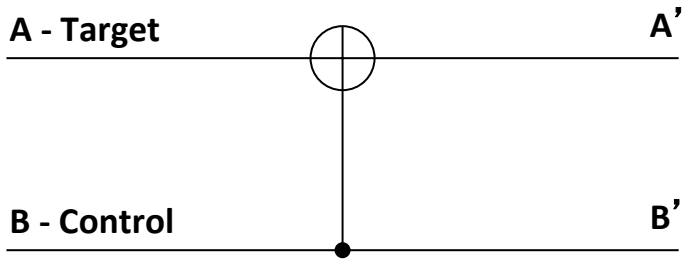
Quantum gates

- The operations on the qubits are called quantum gates.
- A quantum algorithm is build up by these quantum gates.
- Any operation on a set of qubits can be reduced to a finite sequence of gates from a universal set of gates.

- The most common set of universal quantum gates consists of 2 one qubit gates (Hadamard gate and phase gate) and 1 two qubit gate (controlled not gate).



Hadamard gate



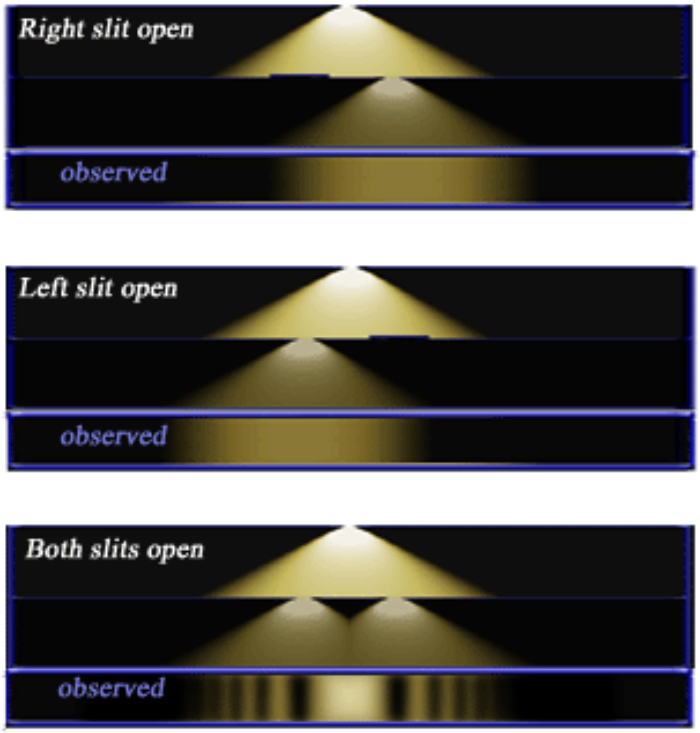
Controlled not gate

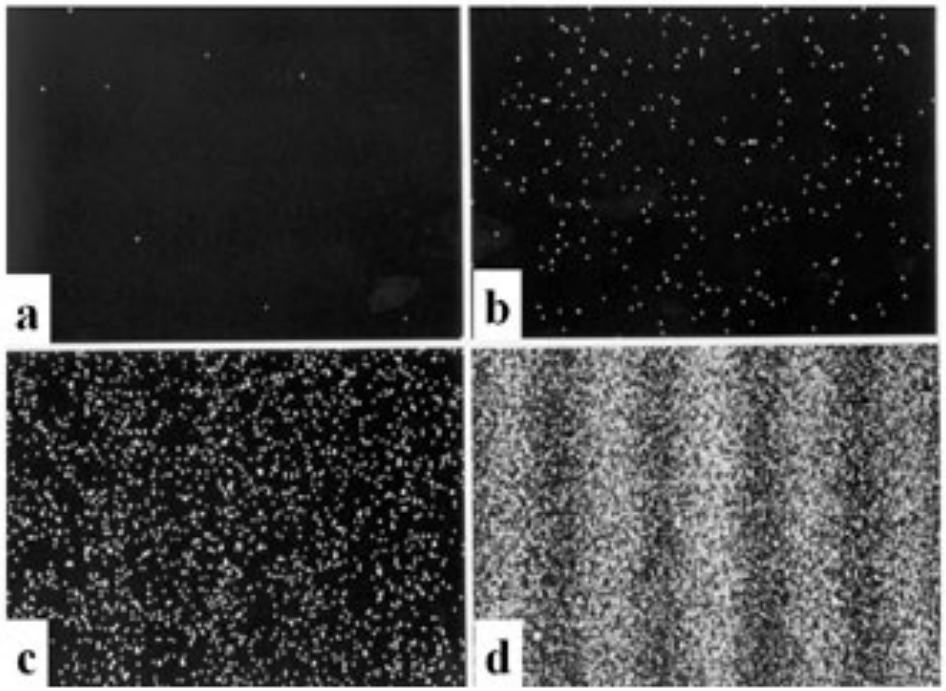
Input		Output	
A	B	A'	B'
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Read out

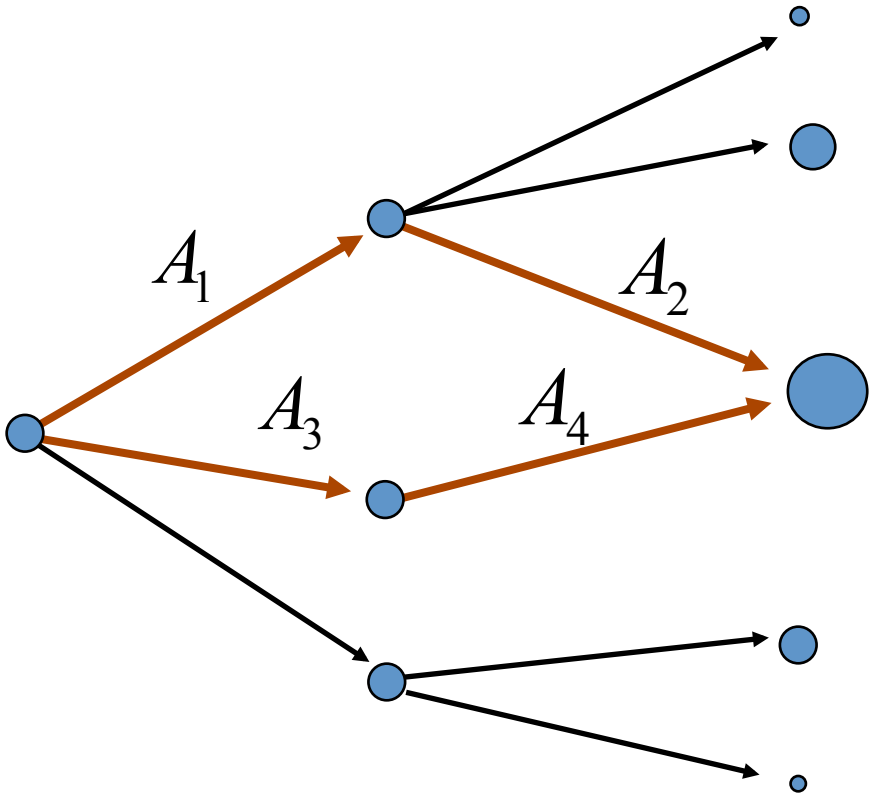
- Read out quantum computation by measure the system.
- Gives a classical output.
- We can increase the probability of getting the right answer using quantum interference.
- The parallel answers can be viewed as waves and will interfere to enhance the right answer.

Light interference vs quantum interference





Electrons showing particle-wave duality



$$A = A_1 A_2 + A_3 A_4$$

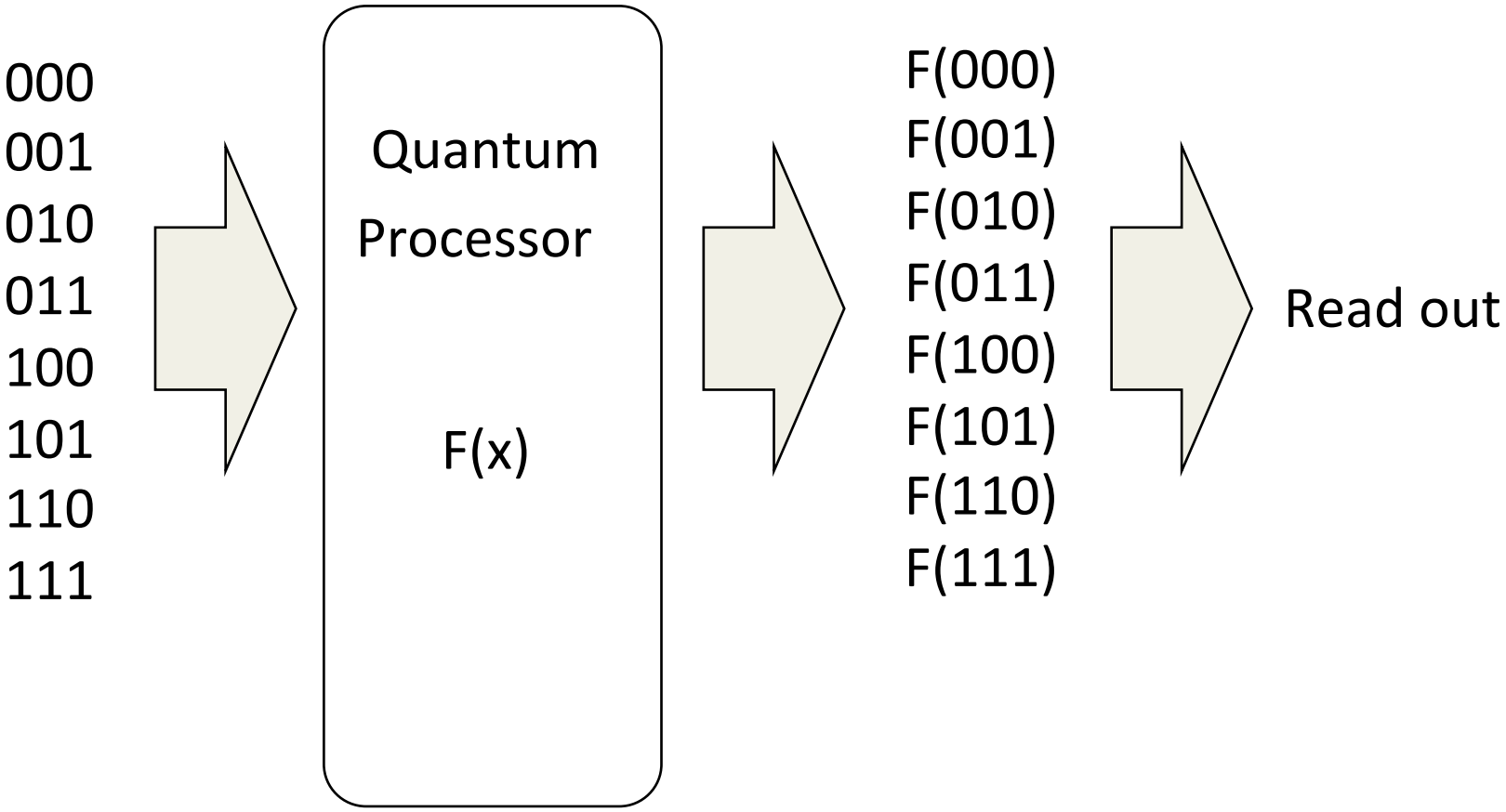
$$P = \left| A_1 A_2 + A_3 A_4 \right|^2$$

$$= \left| A_1 A_2 \right|^2 + \left| A_3 A_4 \right|^2$$

$$+2\,\mathrm{Re}\left(A_1 A_2 A_3^* A_4^* \right)$$

Constructive interference: enhance correct outputs
Destructive interference: suppress wrong outputs

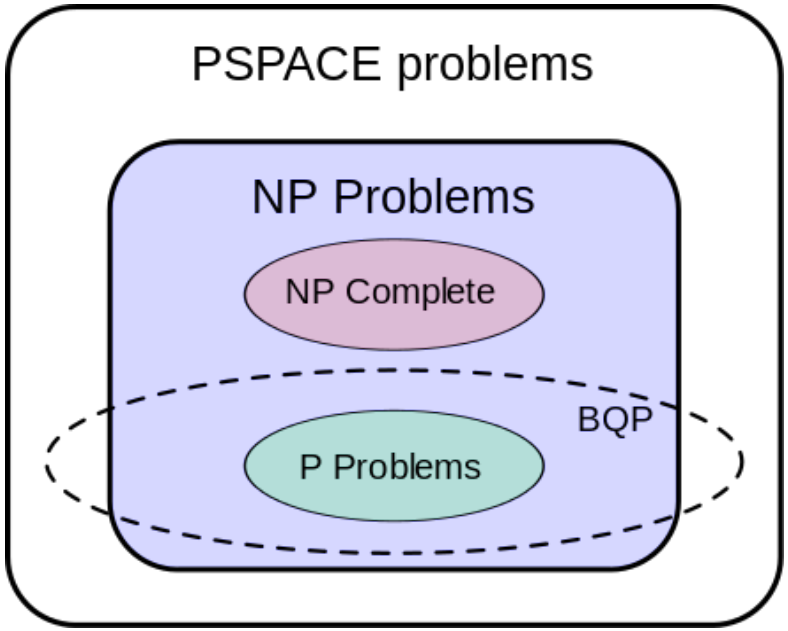
Building blocks for a quantum computer



Computational complexity theory

- How does the number of computational steps scales with the size of the problem?
- Classify problems according to how hard they are.
- If an algorithm grows polynomial, eg $n^{2,}$ it is assumed to be **efficient** algorithm and in the complexity class P.
- Computation grow with n as 1,4,9,16,25,36,49,64 etc.
- If an algorithm grows exponential 2^n then number of steps grow as 2,4,8,16,32,64,128,256

- NP (nondeterministic polynomial time) is a class of problem where the solution can be verified in polynomial time.
- NP-complete problems are the hardest in the NP class and if an algorithm for any such problem is found all NP problems can be solved efficiently, that is, P=NP.
- NP-complete problem: the travelling salesman's problem. Find the shortest path between a set of cities where the path goes through each city once.
- Believed that P≠NP but no proof.
- The problems in NP have only algorithms growing exponential with the problem size.
- All problems solved efficiently on a quantum computer are in a class called BQP (Bounded error, quantum, polynomial).



Quantum algorithms

- An algorithm is a sequance of instructions the computer should perform.
- A quantum algorithm is an algorithm on a quantum computer that uses superposition and entanglement.
- Is usually described by a quantum curcuit acting on input qubits and ends with a measurement.

Grover's algorithm

- Lev Grover, 1996.
- A quantum algorithm for searching an unsorted database with N entries.
- Quadratic speed-up compared to classical computer.
- Grows linear with N on a classical computer and $N^{1/2}$ on a quantum computer, so both in complexity class P.

Shor's factoring algorithm

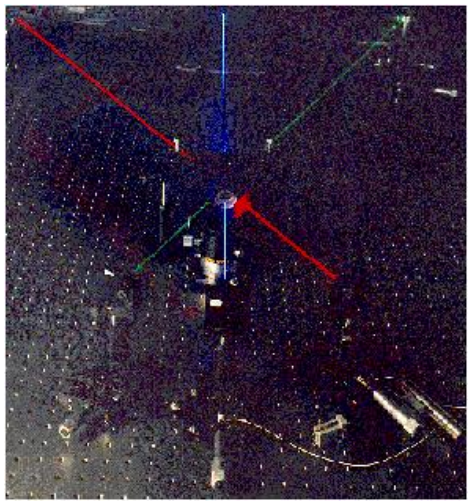
- Peter Shor, 1995.
- Can factor integer numbers in polynomial time on a quantum computer, for example finding that 29083 is 127x229.
- Exponential faster than the best known classical algorithm.
- Grows polynomial with N on a quantum computer, so in complexity class BQP.
- Has been implemented on an 7 qubit NMR quantum computer to find the factors 3 and 5 of 15 (2001).

The quantum take away…

…and the quantum give back!

Classical public key cryptosystems, security based on computational complexity in factoring large numbers

Can be broken by quantum computers!



Quantum cryptography

Simulation of quantum systems

- Feynman, 1982.
- To simulate a quantum system on a classical computer grows exponential with the problem size.
- Seth Lloyd, 1996, showed that QC can simulate local quantum system efficiently.
- Experiments with up to 6 trapped ions have been used to simuate local quantum systems.

Summary

- Computation is a physical process
- A quantum computer will solve some problems faster than a classical computer
- A quantum computer cannot solve NP complete problems like the travelling salesman's problem.