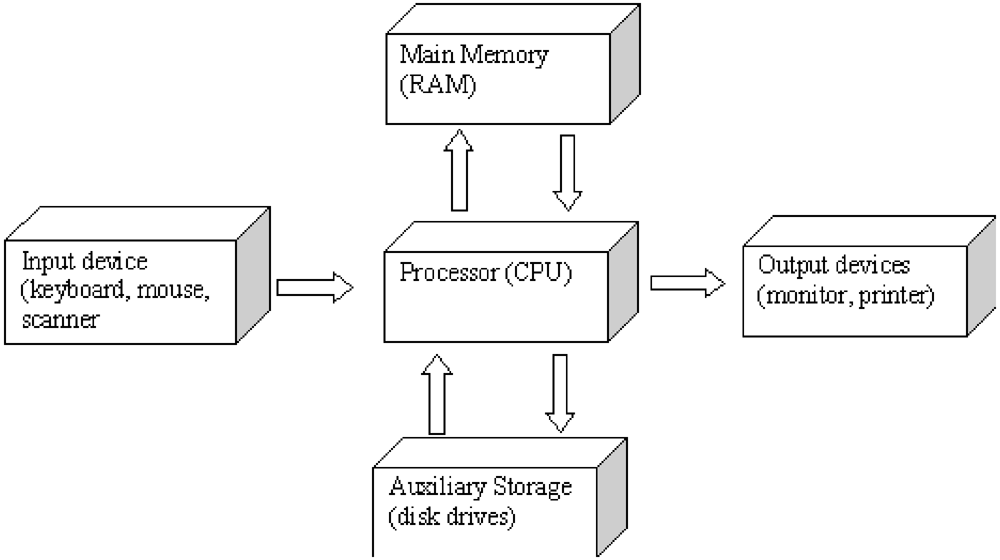
What requirements have to be fulfilled to build a quantum computer?

Task: What are the requirements/elements to realize a quantum computer?

(Hint: Try to translate the individual units of a classical computer to the quantum world.)

Time: 3min

Modus: Work in groups of 2 people. We will discuss your answers then on the black-board.


Main Memory (RAM)
Input device (keyboard, mouse, scanner
Processor (CPU)
Output devices (monitor, printer)
Auxiliary Storage (disk drives)

The DiVincenzo Criteria

for Implementing a quantum computer in the standard (circuit approach) to quantum information processing (QIP):

#1. A **scalable** physical system with well-characterized qubits.
#2. The ability to **initialize** the state of the qubits.
#3. **Long (relative) decoherence** times, much longer than the gate-operation time.
#4. A **universal set** of quantum gates.
#5. A qubit-specific **measurement** capability.

plus two criteria requiring the possibility to transmit information:

#6. The ability to **interconvert** stationary and mobile (or flying) qubits.
#7. The ability to faithfully **transmit** flying qubits between specified locations.

Development of Quantum information science

- 1982 – Feynman suggested that computers based on the principles of quantum mechanics could efficiently simulate quantum systems (quantum simulator)
- *1984 – Bennet and Brassards invented cryptography scheme*
- 1985 – David Deutsch:
  - finds a simple algorithm that is more efficient on a quantum computer
  - searches for computation device that could efficiently simulate any physical system (incl. quantum systems)

  'A computer based on quantum mechanics can simulate every physical process'.
- *1992 – Bennet & Wiesner propose superdense coding*
- *1993 – Bennet invents quantum teleportation*
- 1994 – P. Shor's develops an efficient algorithm to find prime factors of an integer
  - exponential speed-up in comparison to classical algorithm
  - important because encryption schemes (RSA) are based on difficulty of problem
- 1995 – Grover develops algorithm to search in unstructured data bases: quadratic speed up, proof that quantum computer is more powerful than classical
- 1995 – P. Shor's and Steane's error correction codes

State of the art – Quantum communication

- *state of the art:*
  - quantum cryptography is used in commercial applications for distributing keys in optical fiber networks [http://www.idquantique.com/]
  - limited by loss of photons in optical fibers
  - ongoing research into quantum repeaters to extend range

State of the art of Quantum Computation

- difficult to realize and control even a small quantum computer
- BUT the concepts do work and have been demonstrated
  - prime factors of 15 = 3 * 5 have been calculated on a nuclear magnetic resonance (NMR) quantum computer and in linear optics experiments
- ongoing research into realizing scalable hardware for a quantum computer
  - solid state systems (quantum dots, defect centers, superconducting qubits)
  - trapped ions
  - ultra-cold neutral atoms
- ongoing quest for quantum algorithms

  Why is it difficult to find efficient quantum algorithms?

  - adverse to intuition based on classical world
  - quantum algorithms need to be better than classical ones
  - not fully understood what makes a quantum computer more powerful than a classical one (superposition? entanglement?)

How powerful is a quantum computer?

Complexity classes:

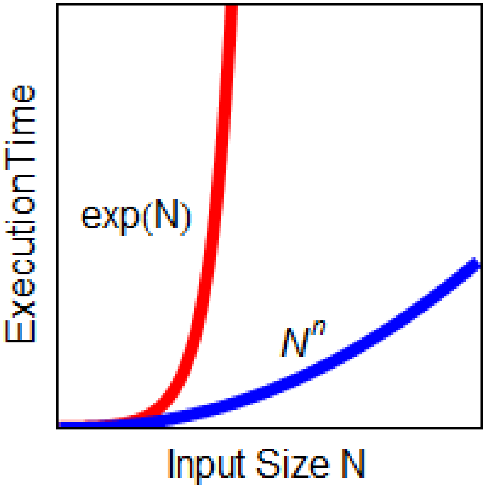
P... problem solvable in polynomial time

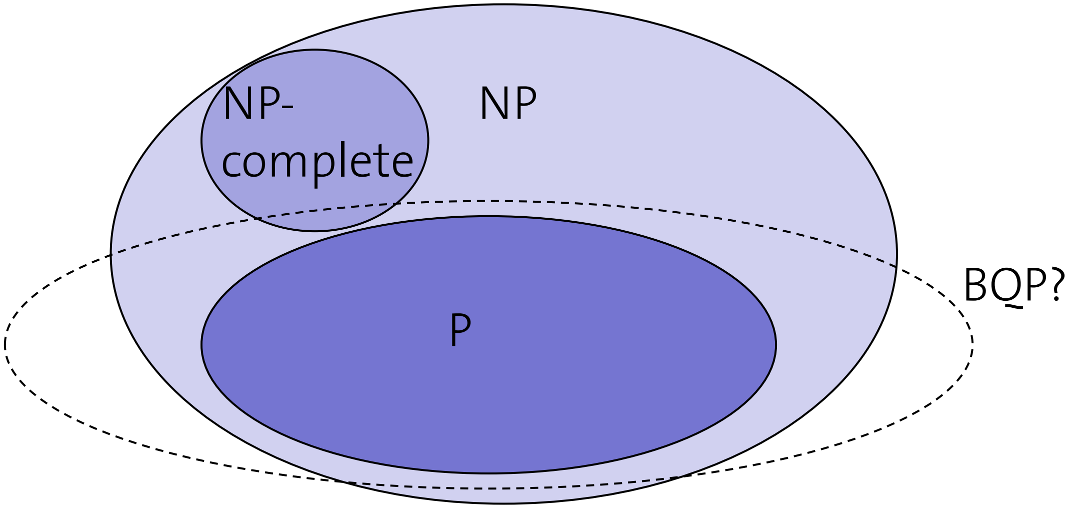
NP... solution can be recognized as correct in polynomial time, but the solution itself is hard to find

NP-complete... If an efficient algorithm is found for any one of them, it could be adapted to solve all other NP problems

BQP.. bounded-error, quantum polynomial time

Note: P=NP? Answer this question and win 1M$!





The fact that quantum computers are more powerful than classical computers has not been proven yet!

see also: THE LIMITS OF Quantum by Scott Aaronson – Scientific American, March 2008