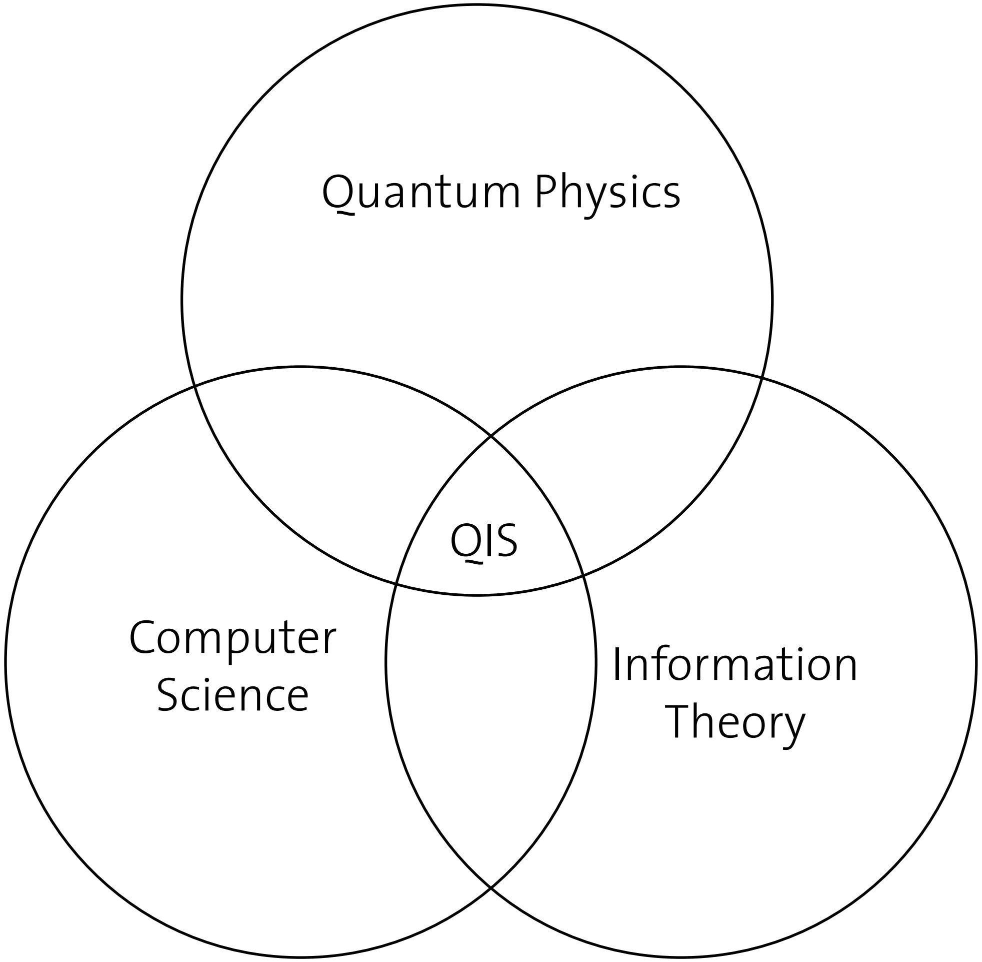
Quantum Information Science (QIS)

combination of three different fields:



Lecture 1 - Outline

1. Quantum Mechanics ✓
2. Computer Science History
3. Aspects of Classical Information processing
4. Architecture of a generic quantum processor
5. Quantum Computation Milestones
6. Quantum bits
7. Single Qubit operations

History of Quantum Physics (rather incomplete)

1900 Planck constant
1905 Einstein photoel. effect
1913Bohr's atom model
1917 Einstein's stimul. emission
1923 de Broglie wavelength
1926 Schödinger equation
1927 Heisenberg uncertainty
1927 Pauli's spin equation
1928 Dirac equation
1946 Purcell effect
1957 BCS theory
1963 Glauber optical coherence
1964 Bell's inequalities
1975 Hänsch & Schawlow / Wineland & Dehmelt laser cooling

(+ many other important discoveries)

1900 — now

1885 Balmer's spectral lines
1911 Kammerling Onnes supercond.
1922 Stern-Gerlach
1927 Davisson-Germer
1937 Rabi oscillations
~1947 Ramsey fringes
1953 Paul's ion trap
1954 Townes & Schawlow's MASER
1960 Mainman's LASER
1977 Freedman&Clauser: Bell inequ.
1977 Mandel's antibunching
1978 ion cooling
1981 Binnings STM
1982 Philipps laser cooling
1985 Meschede's one-atom maser
1986 Hong/Mandel one-photon st.
1995 Ketterle's BEC
1997 Zeilingers Teleportation
1998 Bouchiat SC qubit
1995 Kwiat entangled photons
etc…

History of Quantum Physics (rather incomplete)

theoretical foundations

- 1900 Planck constant
- 1905 Einstein photoel. effect
- 1913Bohr's atom model
- 1917 Einstein's stimul. emission
- 1923 de Broglie wavelength
- 1926 Schrödinger equation
- 1927 Heisenberg uncertainty
- 1927 Pauli's spin equation
- 1928 Dirac equation
- 1946 Purcell effect
- 1957 BCS theory
- 1963 Glauber optical coherence
- 1964 Bell's inequalities
- 1975 Hänsch & Schawlow / Wineland & Dehmelt laser cooling

(+ many other important discoveries)

1900 — now

experiments on collective effects

- 1885 Balmer's spectral lines
- 1911 Kammerlingh Onnes supercond.
- 1922 Stern-Gerlach
- 1927 Davisson-Germer
- 1937 Rabi oscillations
- ~1947 Ramsey fringes
- 1953 Paul's ion trap
- 1954 Townes & Schawlow's MASER
- 1960 Mainman's LASER

coherent experiments on single particles

- 1977 Freedman & Clauser: Bell inequ.
- 1977 Mandel's antibunching
- 1978 ion cooling
- 1981 Binnings STM
- 1982 Phillips laser cooling
- 1985 Meschede's one-atom maser
- 1986 Hong/Mandel one-photon st.
- 1995 Ketterle's BEC
- 1997 Zeilinger's Teleportation
- 1998 Bouchiat SC qubit
- 1995 Kwiat entangled photons

etc...

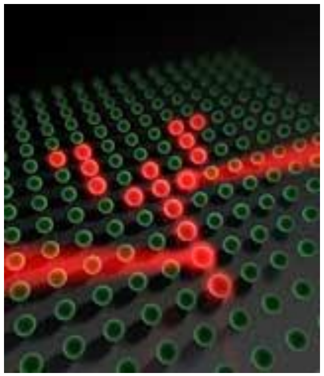
Why the effort to tame quantum mechanics at the level of single particles?

- QIS requires **control over single** quantum systems (degrees of freedom)
- QIS requires possibility to **build complex systems** from basic modular elements (single particles, single operations) in a constructive, bottom up approach

- benefits:
  - quantum computing
  - exploring new regimes of physics by new experimental and theoretical techniques – we are forced to understand quantum mechanics, if we want to build quantum computers
  - quantum effects are likely to become relevant for classical computer
  - testing quantum mechanics
  - …

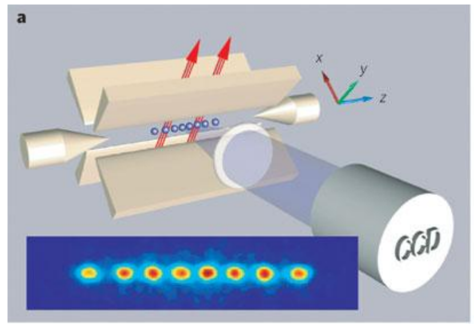
Quantum mechanics at the level of single particles

Ultra-cold atoms
(lattices or on-chip)



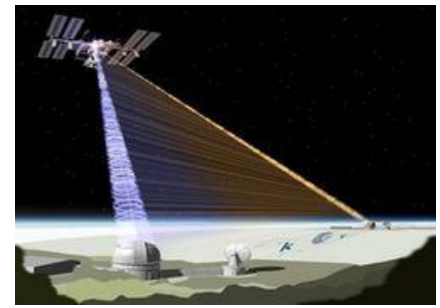
© S. Kuhr

Trapped ions



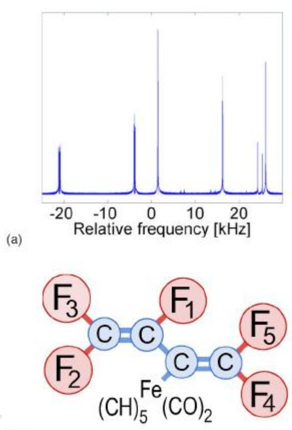
© Blatt & Wineland

Photons



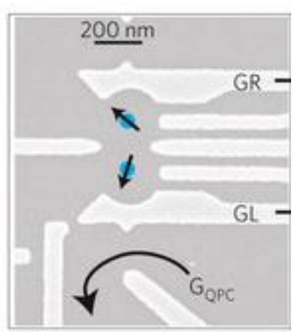
© QUEST, Zeilinger

Nuclear spins (NMR)

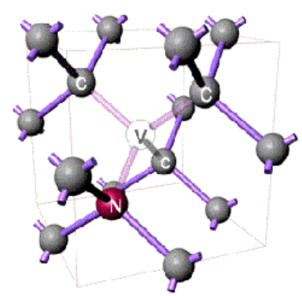


© Vandersypen, Chuang

Quantum dots, NV-centers

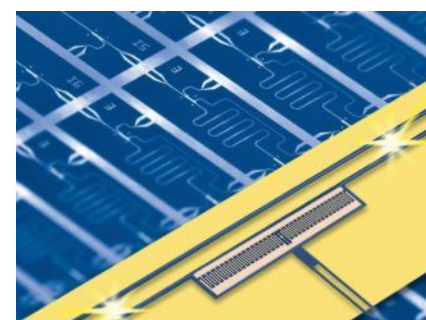


© Bluhm



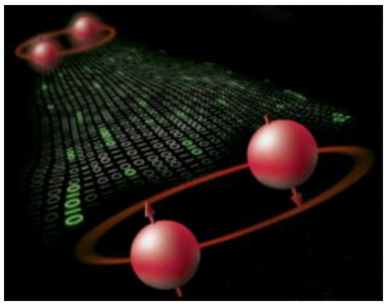
© Wrachtrup

Superconducting qubits



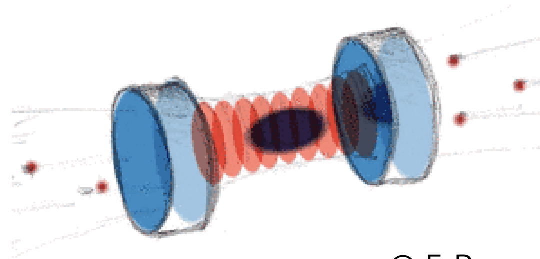
Can be used…

…for quantum information processing



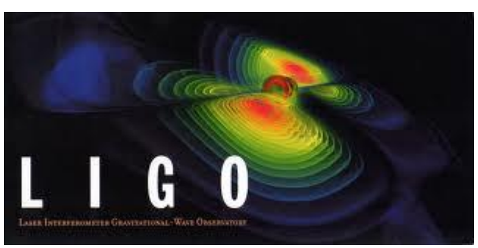
© io9

…for exploring matter-light interactions at the quantum level



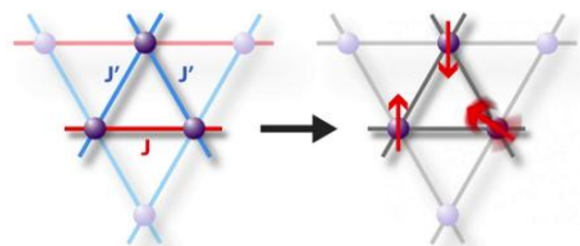
© F. Brennecke

…for quantum detectors



©ligo

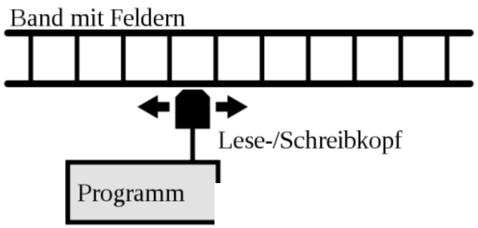
…for quantum simulation



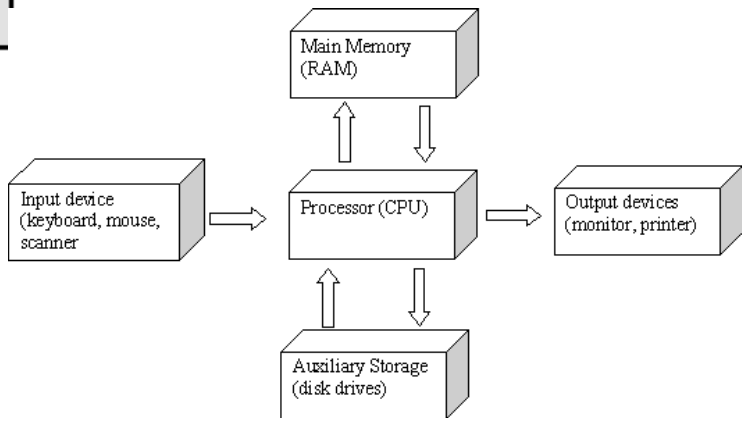
© Struck, Science

Computer Science

- 1936: Turing invented the notion of a (Universal) Turing machine, which is capable of computing any function/computable sequence[1]
  'Any computable function can be computed on a Turing machine.'



- 1945 -- von Neumann:
  theoretical model for programmable computer



- 1947 – Bardeen, Brattain, Shockley
  developed the transistor
- 1948 – Claude Shannon
  established information theory
- 1954/55 – TRADIC, Mailüfterl, CADET:
  first transistorized computers
- 1965 – Moore's law of double computer power every second year
- 1971 – First Intel processor
- ...

[1] e.g. Hofstadter – Goedel, Escher, Bach

The first transistor

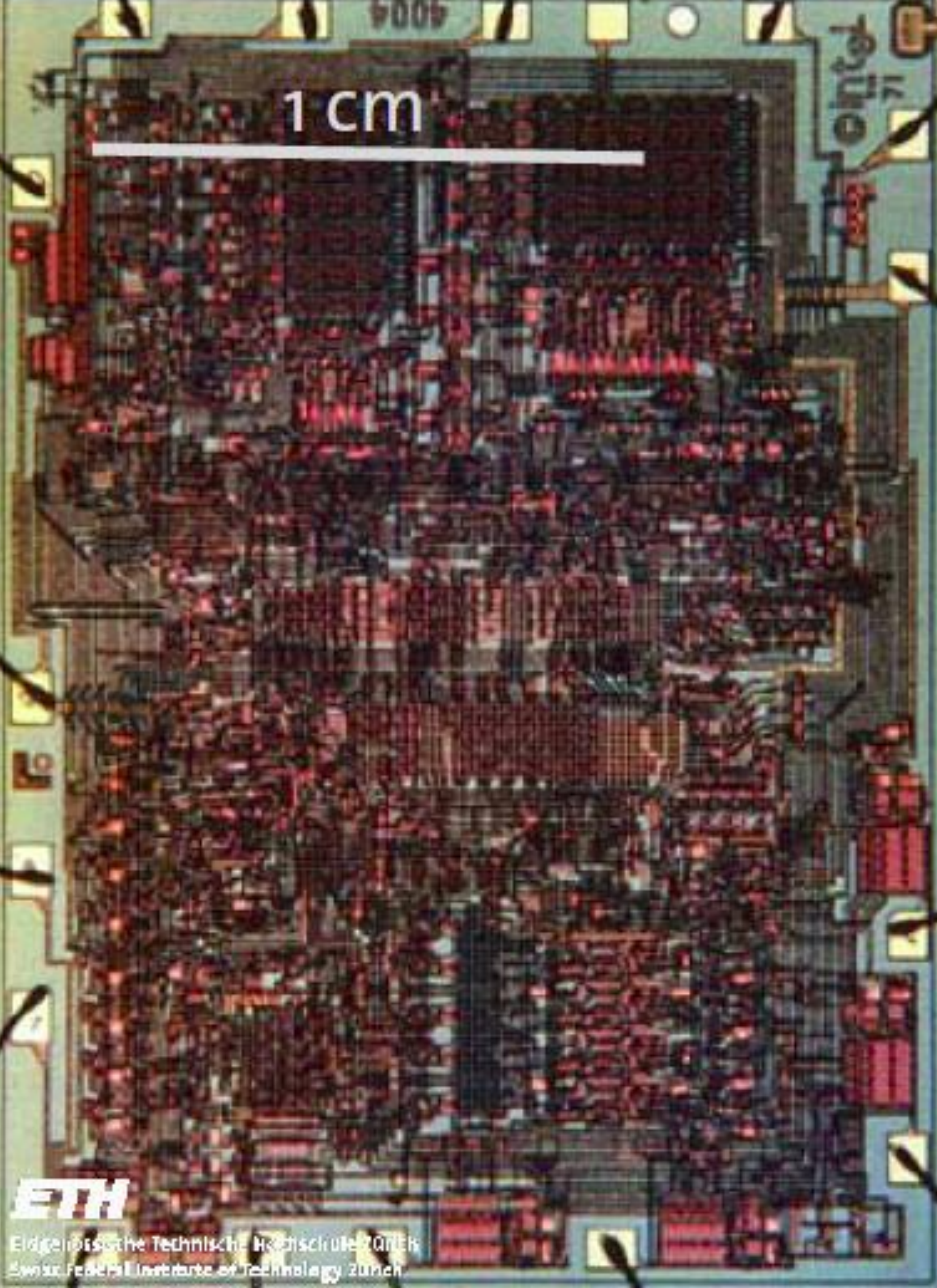
developed at Bell Labs 1947 by John Bardeen, Walter Brattain and William Shockley.

Nobel prize in physics, 1956

material:
- semiconductor

clock rate:
- 1 Hz

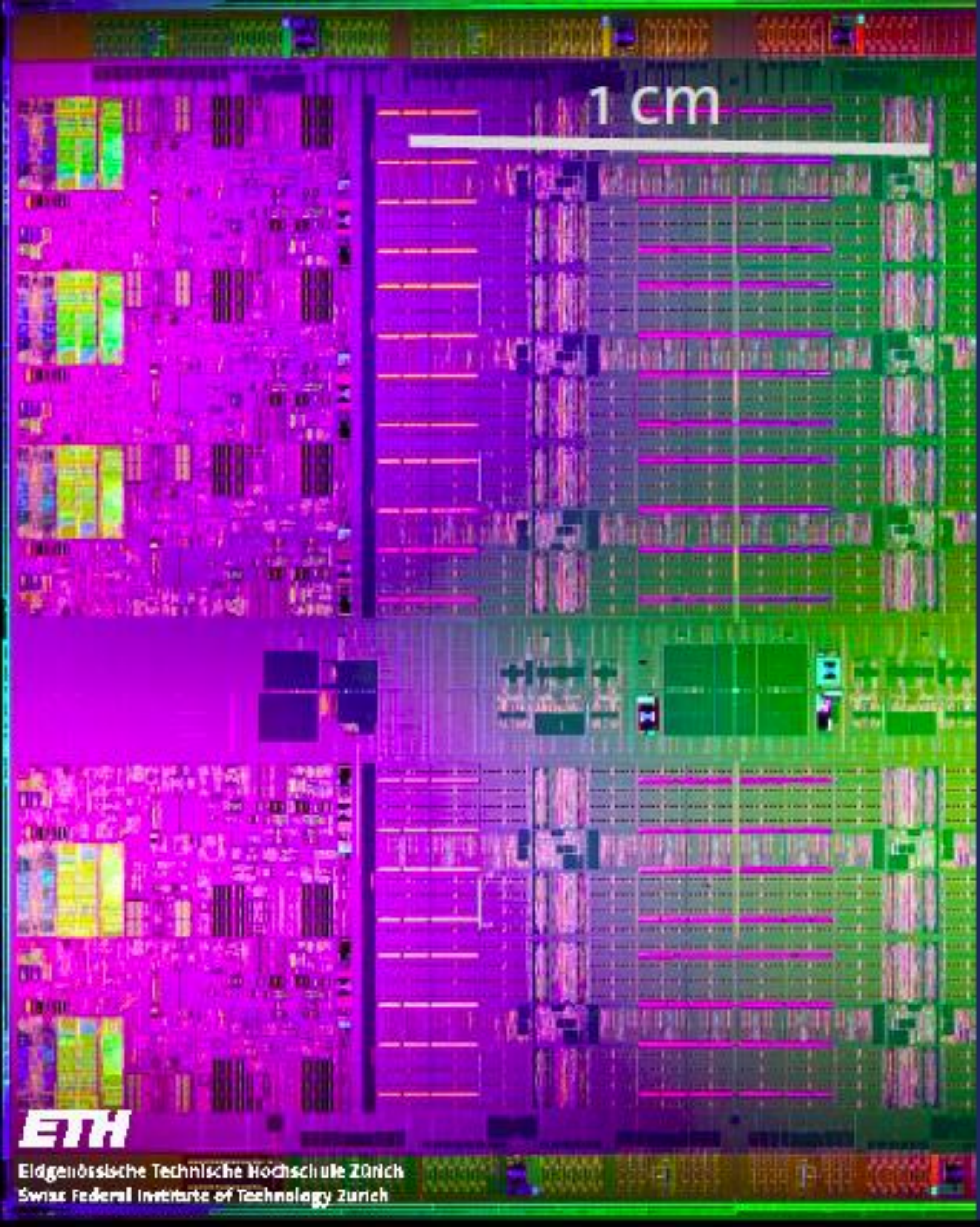
dimensions:
- 1 cm



First Intel Processor

Intel 4004, 1971

- 2000 transistors
- 60 kHz
- 10.000 nm = 0,001 cm

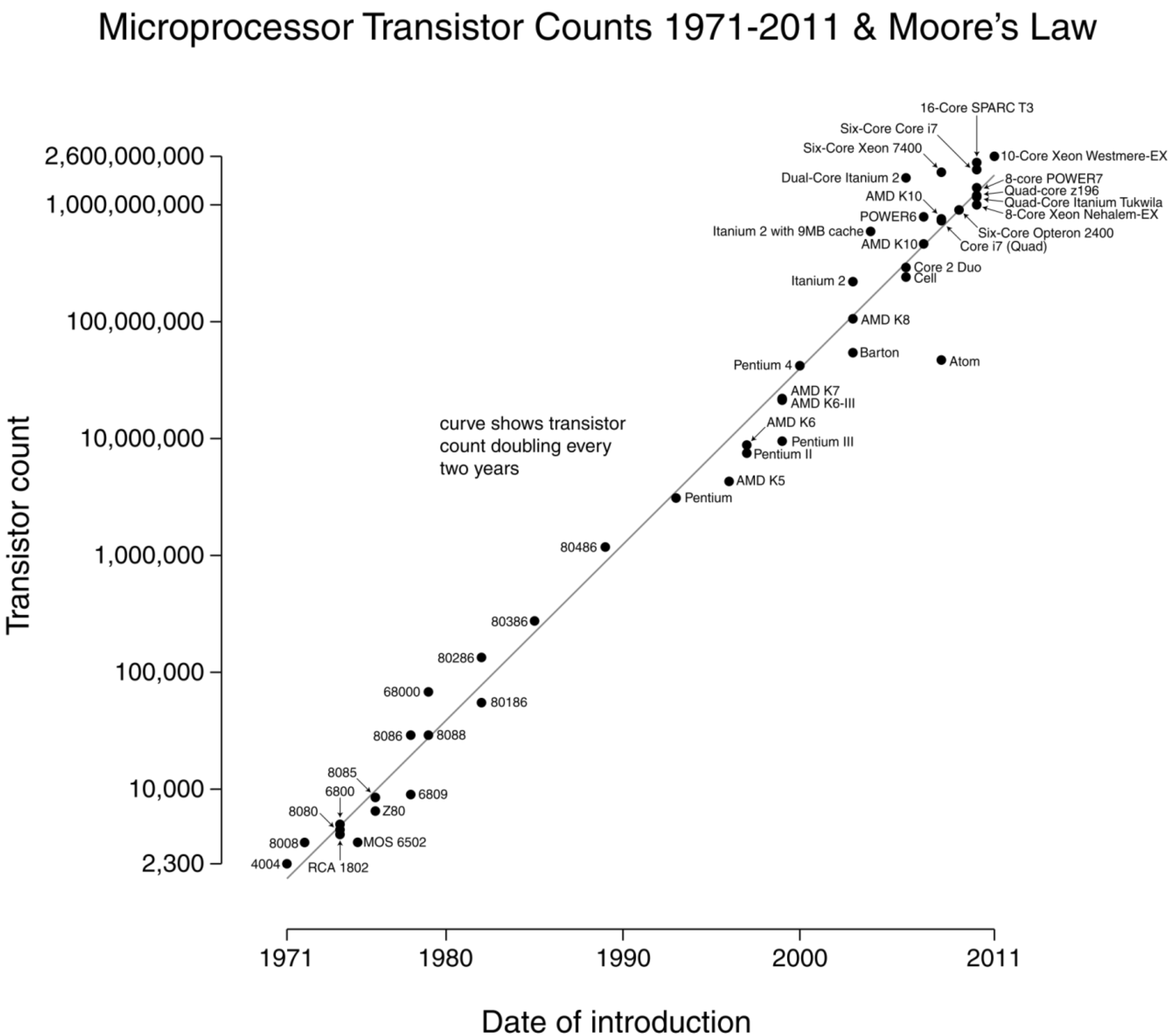


Todays processors

Intel Xeon, 2011

- 3 Billion Transistors
- 3 GHz
- 32 nm = 0.0000032 cm

Moore‘s Law

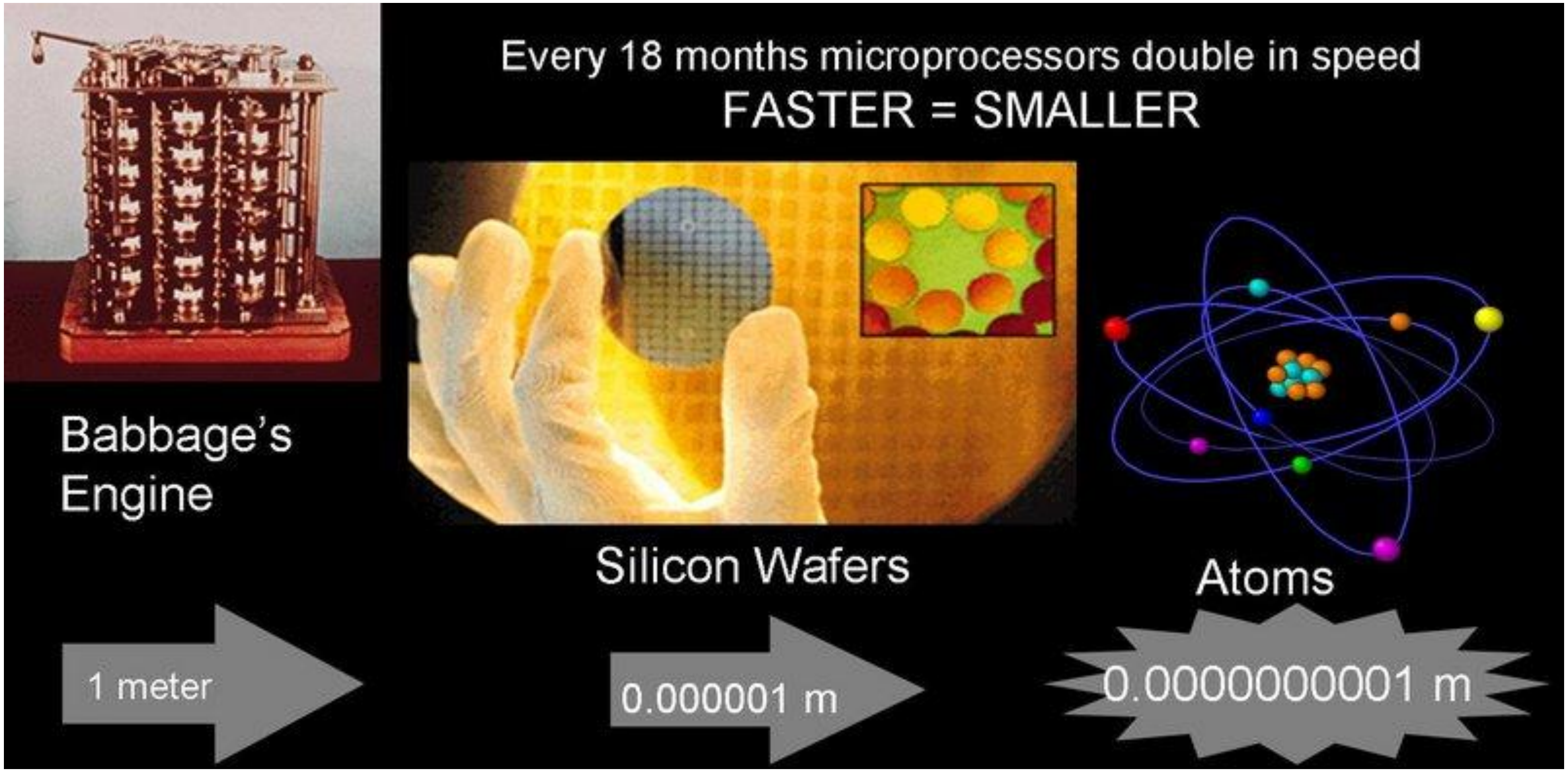


doubling of number of transistors on a processor every 24 months ->exponential growth

basis of modern information and communication based society

first stated in 1965 by Gordon E. Moore, cofounder of Intel

Computation goes nanoscale



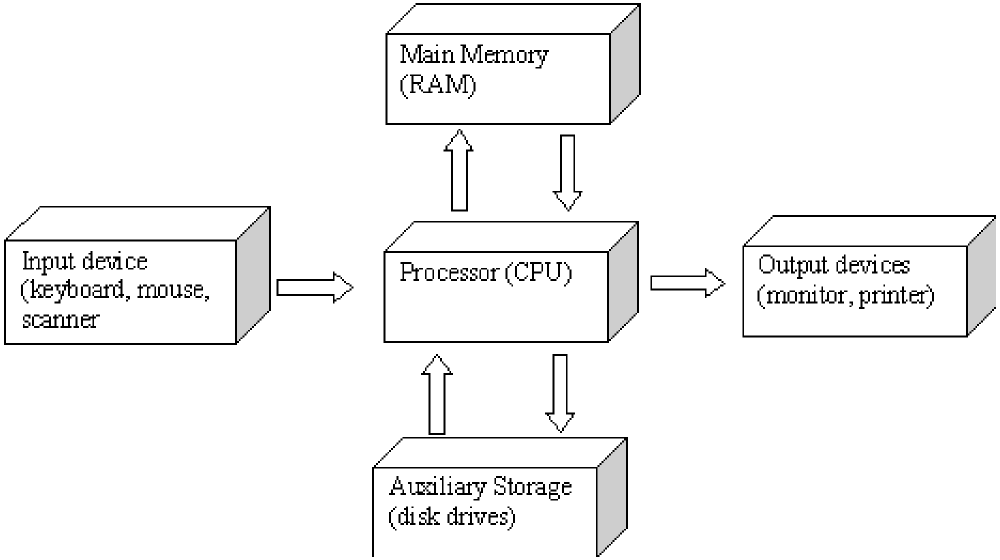
(http://www.quantiki.org/wiki/What_is_Quantum_Computation%3F)

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.



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:

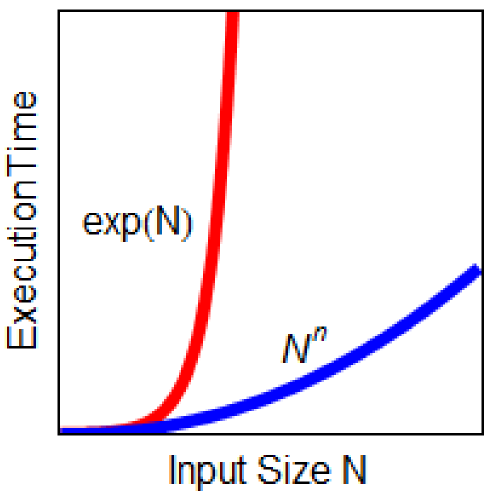
P... problem solvable in polynomial time

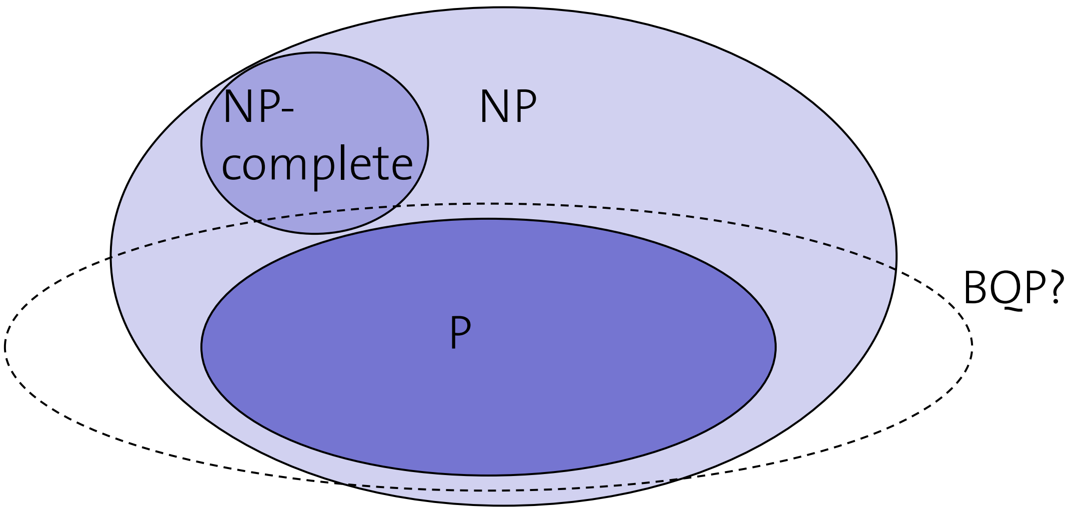
NP... solution can be recognized as correct in polynomial time, but the solution itself is hard to find

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