Motivation to explore quantum systems for information technology

- control and explore the physics of single quantum systems ...
- ... and collections of such systems and their interactions
- explore new physical regimes in Nature
- look for novel approaches to and applications in information processing that are enabled by the quantum nature of the computer
  - efficient quantum algorithms (Deutsch '85, Shor '94, Grover '95)
  - quantum simulation (Feynman '82)
  - ... but it is difficult to develop efficient quantum algorithms
- however, it is still very difficult to realize and control even small numbers of quantum systems for quantum information processing
- quantum systems for communication
  - super dense coding (Bennett '92)
  - quantum cryptography (Bennett, Brassard '84)

I.1 Classical Information Processing

The carrier of information

- binary representation of information as **bits** (Binary digITs).

- classical bits can take values **either** 0 **or** 1

- information is stored in a physical system, for example as a voltage level in a digital circuit (CMOS, TTL)

- 5 V = 1
- 0 V = 0

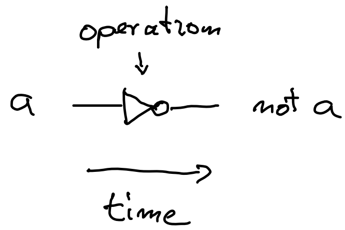
- information is processed by operating on this information using physical processes, e.g. realizing logical gates with transistors

Processing Information with Classical Logic

non-trivial single bit logic gate: NOT

IN	OUT
0	1
1	0

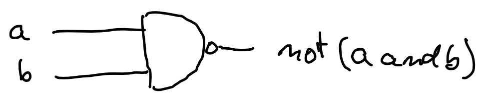
circuit representation



universal two bit logic gate: NAND
AND followed by NOT

IN	OUT
00	1
01	1
10	1
11	0

circuit representation



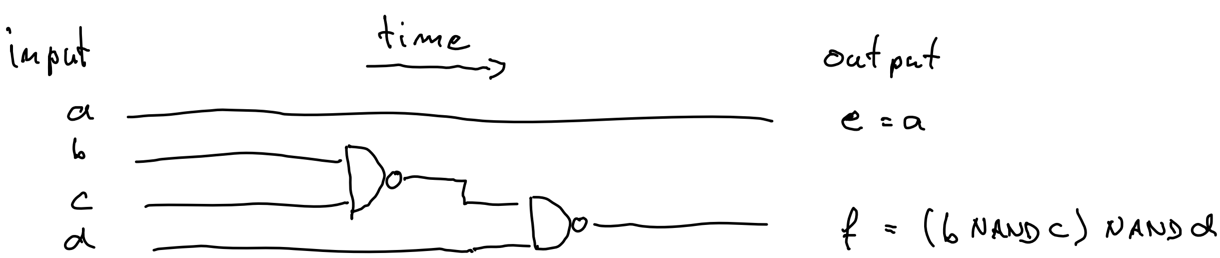
Other gates exist (AND, OR, XOR, NOR) but can all be implemented using NAND gates.

Universality of the NAND gate

- Any function operating on bits can be computed using NAND gates. Therefore NAND is called **a universal logic gate**.

Circuit representation

- Any computable function can be represented as a circuit composed of universal gates acting on a set of input bits generating a set of output bits.



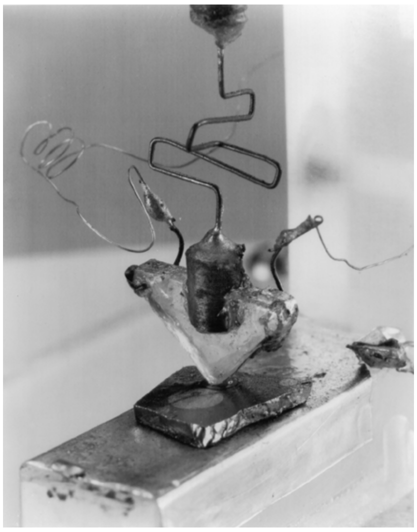
logical circuit computing a function

not reversible

One realization of classical information processing ...

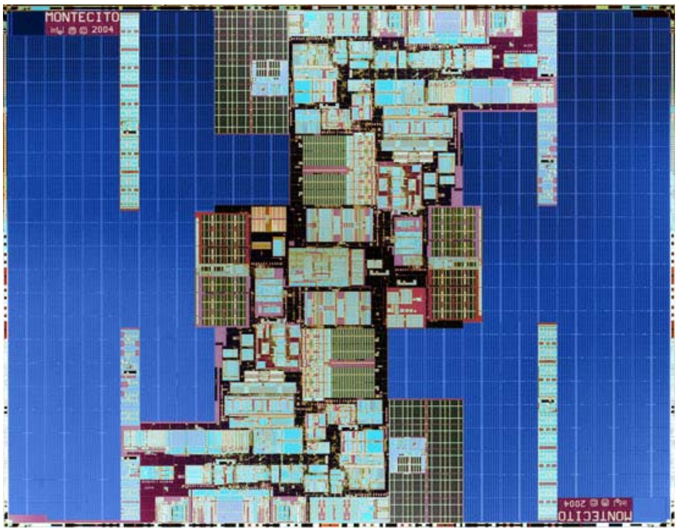
... with electronic circuits

first transistor at Bell Labs (1947)

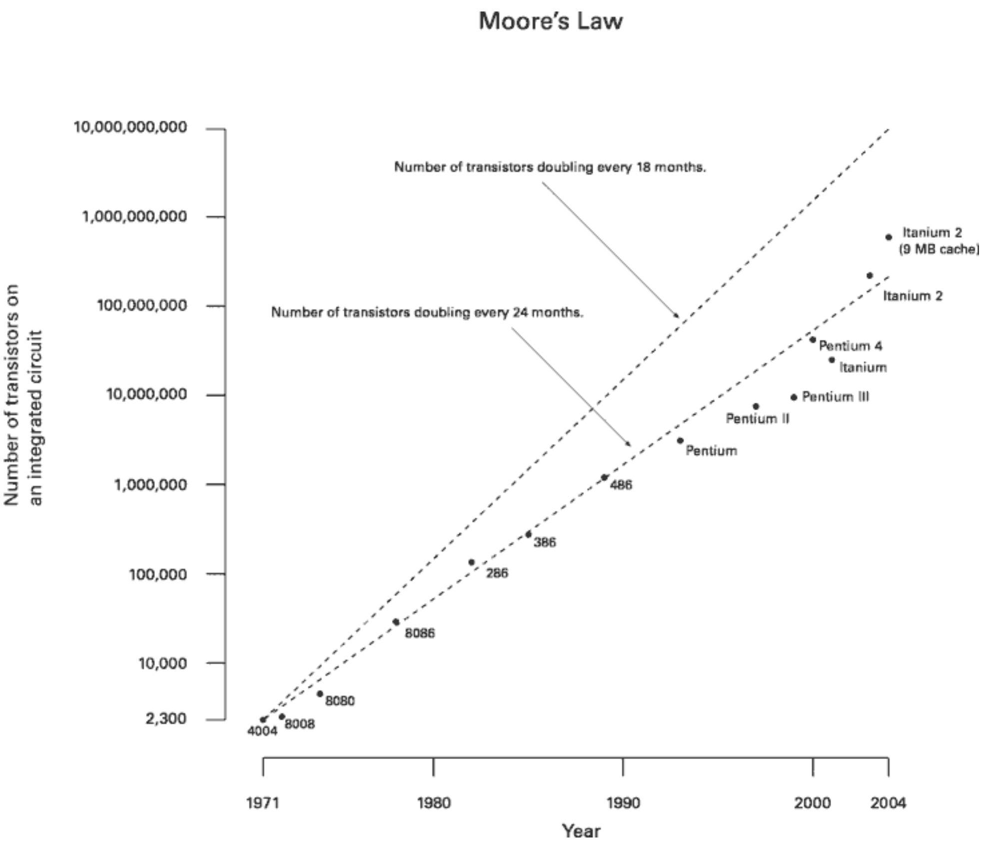


- 1 transistor
- size a few cm

intel dual core processor (2006)



- 2.000.000.000 transistors
- smallest feature size 65 nm
- clock speed ~ 2 GHz
- power consumption 10 W
- 5 nW per transistor
- 2.5 10^{-18}J per transistor per cycle



Moore's Law

- doubling of number of transistors on a processor every 24 months (at constant cost)
- exponential growth
- basis of modern information and communication based society

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

Conventional electronic circuits for information processing:

- work according to the laws of **classical physics**
- quantum mechanics does usually not play an important role
- What happens when circuits are miniaturized to near atomic scales?
- Do they continue working the same way?
- Does quantum mechanics get in the way?
- Or can it be used?

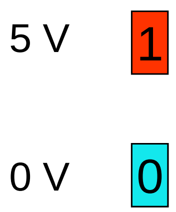
Make use of **quantum mechanics** for information processing!

- Is there something to be gained?
- Can it be realized?

Classical Bits and Quantum Bits

classical bit (binary digit)

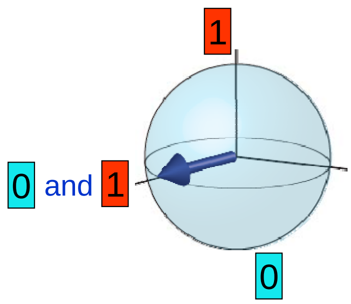
- can take values 0 or 1



- realized e.g. as a voltage level 0 V or 5 V in a circuit

qubit (quantum bit) [Schumacher '95]

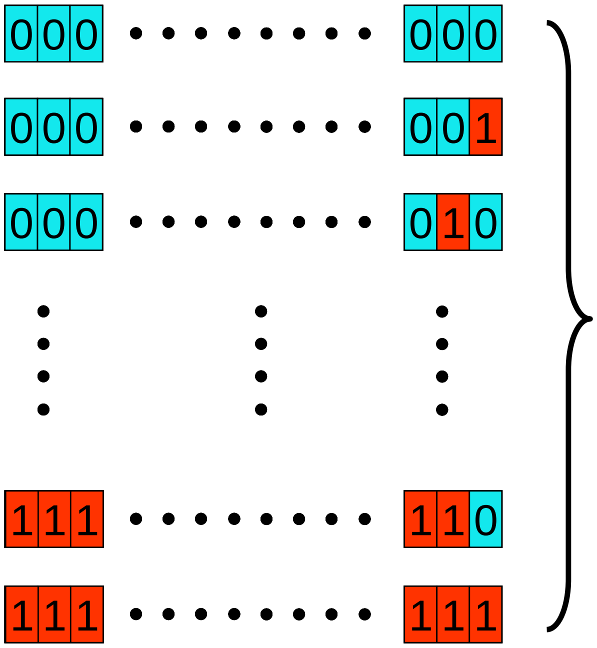
- can take values 0 and 1 'simultaneously'



- realized as the states of a physical quantum system

The Power of Quantum Computers

register with n bits:



classically:
can store 1 number only

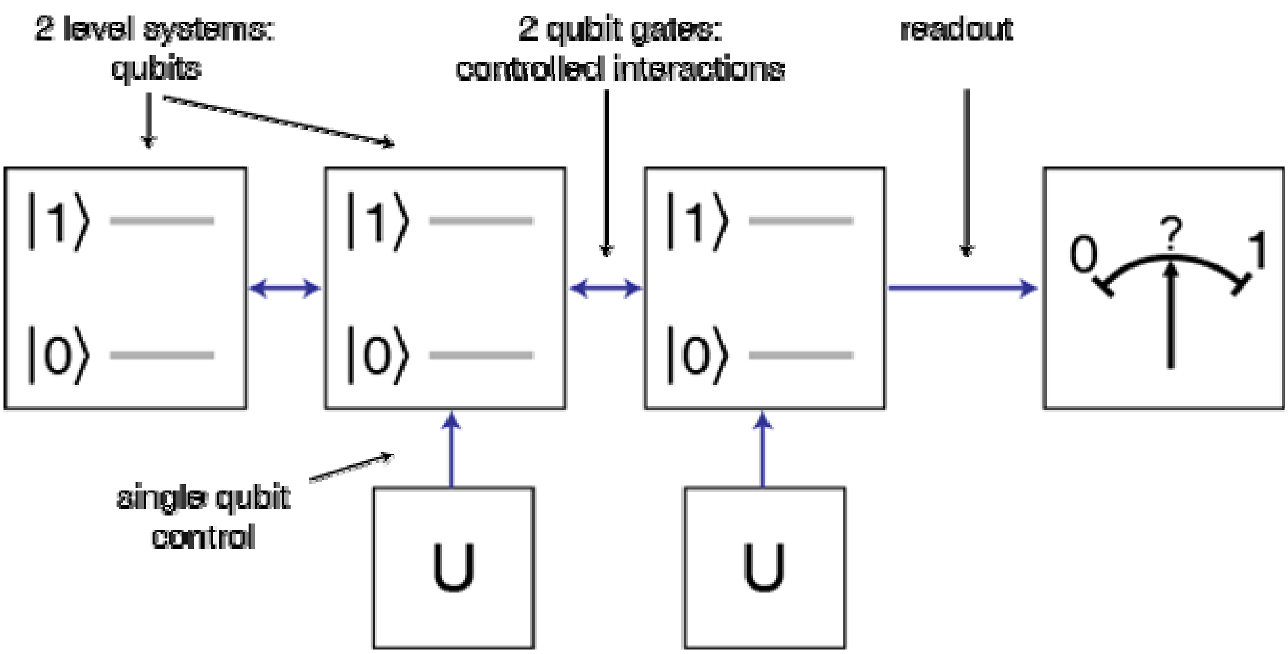
2^N possible configurations

**quantum mechanically:
can store all numbers simultaneously**

**Process all numbers simultaneously
in a quantum computer!**

But what is needed to construct a quantum computer and how would it be operated?

Schematic of a Generic Quantum Processor



The 5 (+2) DiVincenzo Criteria for Implementation of 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 to a simple fiducial state.

#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.

#6. The ability to interconvert stationary and mobile (or flying) qubits.

#7. The ability to faithfully transmit flying qubits between specified locations.

Quantum Bits

Quantum **bit**s (qubits) are quantum mechanical systems with two distinct quantum mechanical states. Qubits can be realized in a wide variety of physical systems displaying quantum mechanical properties. These include atoms, ions, electronic and nuclear magnetic moments, charges in quantum dots, charges and fluxes in superconducting circuits and many more. A suitable qubit should fulfill the **DiVincenzo criteria**.

Quantum Mechanics Reminder:

QM postulate I: The quantum state of an isolated physical system is completely described by its state vector in a complex vector space with a inner product (a **Hilbert Space** that is). The state vector is a unit vector in that space.

The qubit states are represented as vectors in a 2-dimensional Hilbert space. A set of possible qubit (computational) basis states is:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} ; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$ (Dirac notation)

A quantum **bit** can take values (quantum mechanical states) $|\psi\rangle$

$$|0\rangle, \quad |1\rangle$$

or both of them at the same time.

I.e. a qubit can be in a **superposition of states:**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \quad \text{where} \quad \alpha, \beta \in \mathbb{C}$$

when the state of a qubit is measured one will find

$$|0\rangle \text{ with probability } |\alpha|^2 = \alpha\alpha^*$$
$$|1\rangle \quad \text{"} \qquad |\beta|^2 = \beta\beta^*$$

where the normalization condition is $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$

$$\text{with} \quad \langle\psi| = |\psi\rangle^+ = \alpha^*\langle 0| + \beta^*\langle 1| = (\alpha^*, \beta^*)$$

This just means that the sum over the probabilities of finding the qubit in any state must be unity.

Example: $$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Bloch Sphere Representation of Qubit State Space

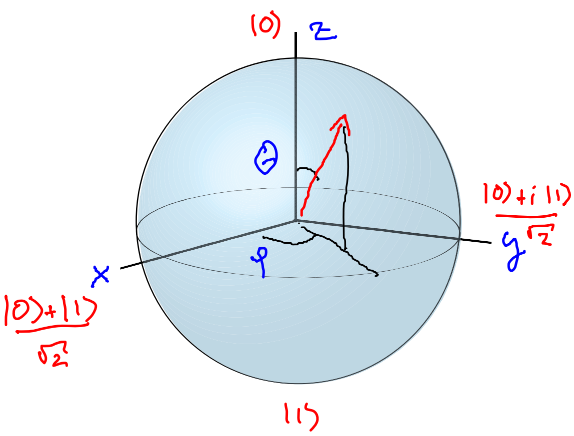
alternative representation of qubit state vector

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$= e^{i\gamma}\left[\cos\frac{\Theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\Theta}{2}|1\rangle\right]$$

γ global phase factor
Θ polar angle
φ azimuth angle

unit vector pointing at the surface of a sphere:

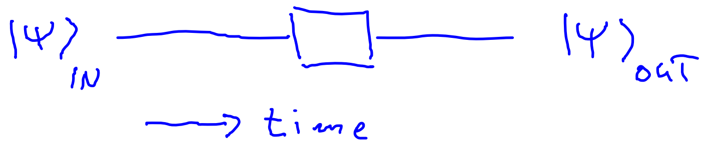
$$\vec{v} = (\cos\varphi \sin\Theta, \sin\varphi\sin\Theta, \cos\Theta)$$



- ground state $|0\rangle$ corresponds to a vector pointing to the north pole
- excited state $|1\rangle$ corresponds to a vector pointing to the south pole
- equal superposition state $(|0\rangle + e^{i\phi}|1\rangle)/2^{1/2}$ is a vector pointing to the equator

Single Qubit Logic Gates

quantum circuit for a single qubit gate operation:



operations on single qubits:

X	bit flip	$\|0\rangle \rightarrow \|1\rangle$; $\|1\rangle \rightarrow \|0\rangle$
Y	bit flip*	$\|0\rangle \rightarrow -i\|1\rangle$; $\|1\rangle \rightarrow i\|0\rangle$
Z	phase flip	$\|0\rangle \rightarrow \|0\rangle$; $\|1\rangle \rightarrow -\|1\rangle$
I	identity	$\|0\rangle \rightarrow \|0\rangle$; $\|1\rangle \rightarrow \|1\rangle$

any operation on a single qubit can be represented as a rotation on a Bloch sphere

Pauli Matrices

The action of the single qubit gates discussed before can be represented by Pauli matrices acting on the computational basis states:

bit flip (NOT gate) $\quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $X|0\rangle = |1\rangle$; $X|1\rangle = |0\rangle$

bit flip* (with extra phase) $\quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$; $Y|0\rangle = i|1\rangle$; $Y|1\rangle = -i|0\rangle$

phase flip $\quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; $Z|0\rangle = |0\rangle$; $Z|1\rangle = -|1\rangle$

identity $\quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $I|0\rangle = |0\rangle$; $I|1\rangle = |1\rangle$

all are unitary: $\quad U = X, Y, Z, I$: $\quad U^{\dagger}U = I$

exercise: calculate eigenvalues and eigenvectors of all Pauli matrices and represent them on the Bloch sphere

Hadamard gate:

a single qubit operation generating superposition states from the qubit computational basis states

$$|0\rangle \;—\boxed{H}—\; \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|1\rangle \;—\boxed{H}—\; \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

matrix representation of Hadamard gate:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\; X + Z \qquad ; \quad H^{\dagger}H = I$$

exercise: write down the action of the Hadamard gate on the computational basis states of a qubit.