Quantum Information: Theory and Experiments

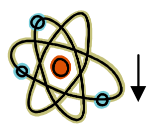
J IGNACIO CIRAC
MAX-PLANCK INSTITUT FÜR QUANTENOPTIK

Universidad Autónoma de Madrid
January 13, 2010

BASIC CONCEPTS
SUPERPOSITIONS

- The properties of objects are not well defined.
- They become defined when we measure them.

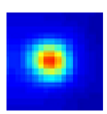
ELECTRONIC SPIN

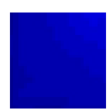


$|0\rangle$

$|1\rangle$

- It can be manipulated: Magnetic field
- and measured: Fluorescence



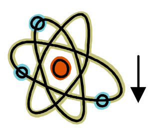


One could store a bit of information in the spin

BASIC CONCEPTS
SUPERPOSITIONS

- The properties of objects are not well defined.
- They become defined when we measure them.

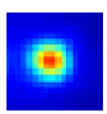
ELECTRONIC SPIN

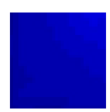


$|0\rangle$

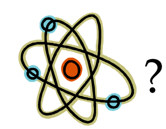
$|1\rangle$

- It can be manipulated: Magnetic field
- and measured: Fluorescence

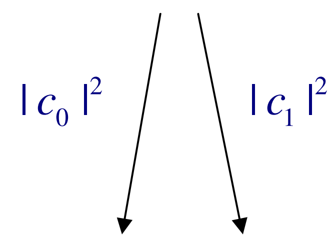


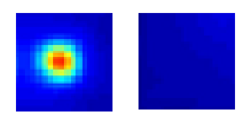


superposition



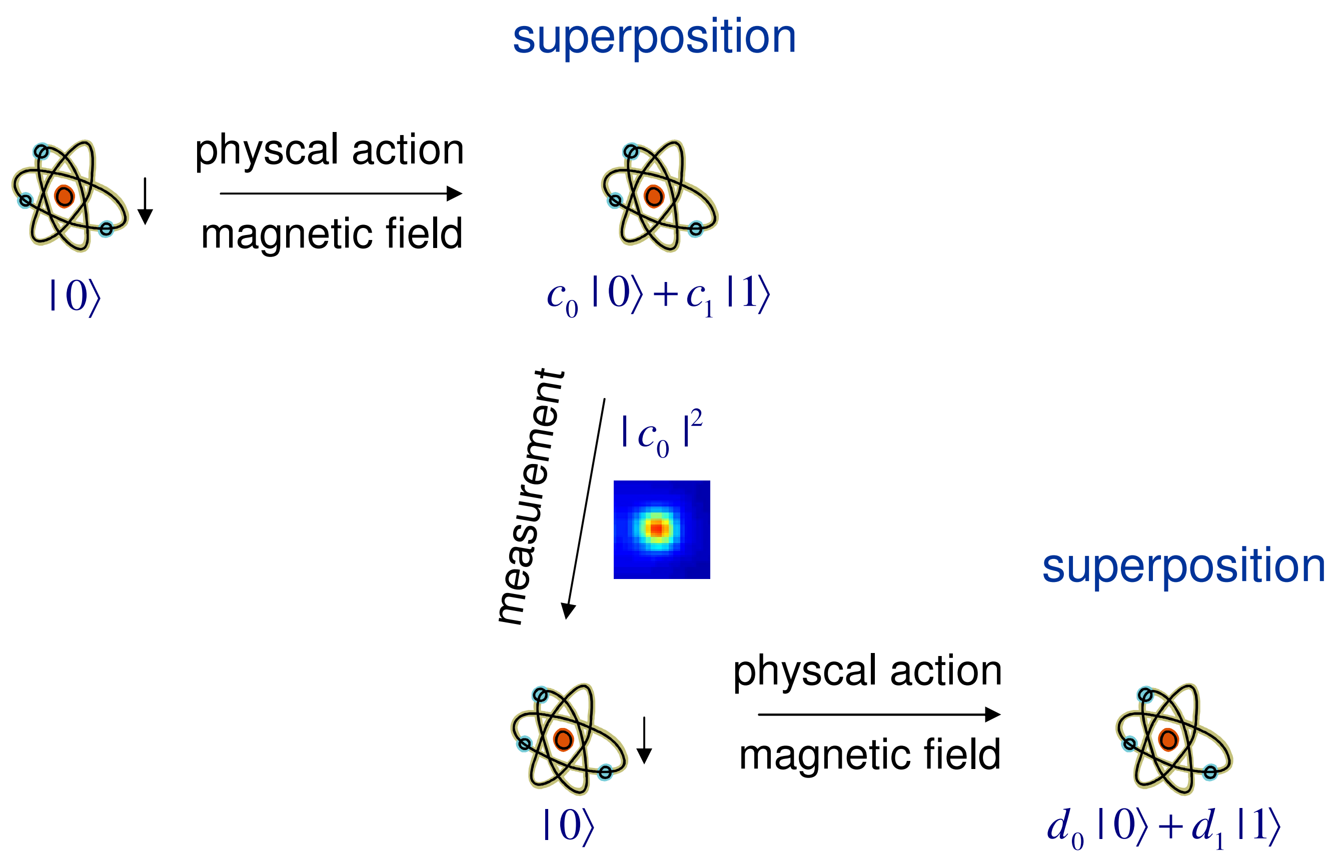
$c_0|0\rangle + c_1|1\rangle$





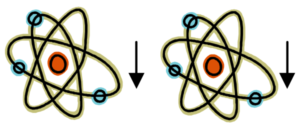
One could store a bit of information in the spin

BASIC CONCEPTS
SUPERPOSITIONS



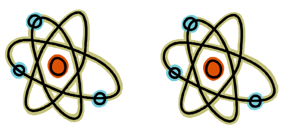
BASIC CONCEPTS
ENTANGLEMENT

- If we have two objects:



$|0\rangle \quad |0\rangle$

or we can have an „entangled state“:

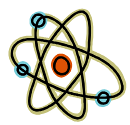


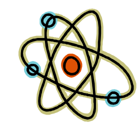
$|0,0\rangle + |1,1\rangle \quad \neq |\alpha;\beta\rangle_2$

Those states can be created by letting the atoms interact with each other.

BASIC CONCEPTS
SUPERPOSITIONS

- If we have two objects: $|0,0\rangle + |1,1\rangle$



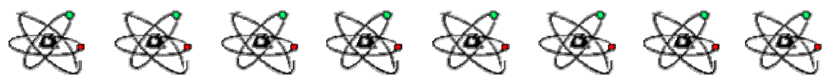


If we measure one and obtain 0, then the other one is also projected

„spooky action at a distance“

BASIC CONCEPTS
SUPERPOSITIONS

- If we have MANY objects:



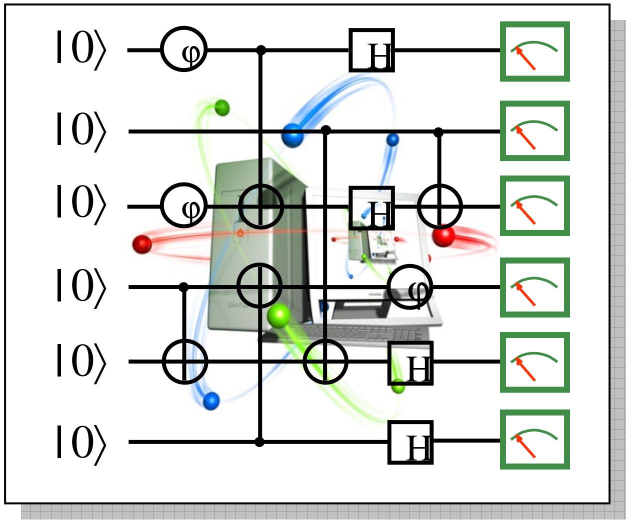
$$c_1 \,|000\ldots0\rangle + c_2 \,|000\ldots1\rangle + \ldots + c_{2^N} \,|111\ldots1\rangle$$

- We have a superpostions of 2^N states.
- We can manipulate the superpositions, make them interfere, measure, etc

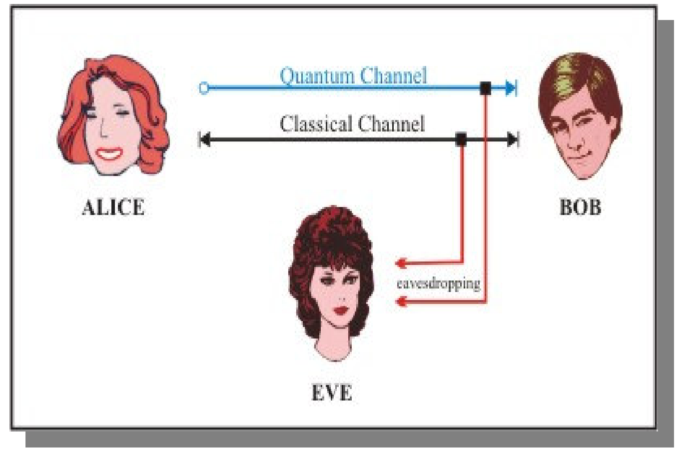
We have new laws at hand, thus we can do new things

QUANTUM INFORMATION SCIENCE

Quantum computation



Quantum communication



- Simulations
- Precission measurements
- Sensing

OUTLINE

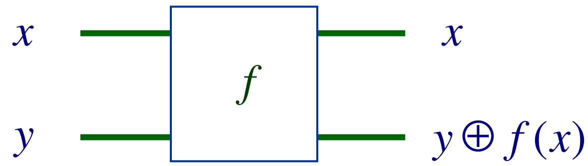
- Algorithms
- Circuit model
- Decoherence and error correction
- Experimental situation
- Other approaches to Quantum Computing:
    - Measurement-based QC
    - Dissipation-driven QC
    - Topological QC

QUANTUM COMPUTING:
ALGORITHMS

EXAMPLE

- Black Box:

input:



: output

$x, y \in \{0,1\}$

$f : \{0,1\} \rightarrow \{0,1\}$

- Four kinds of boxes:

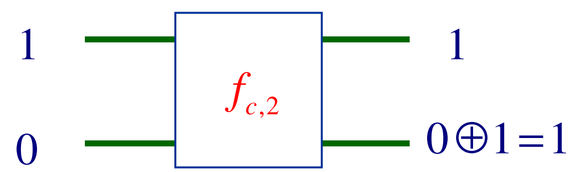
one-to -one

$$f_{b,1} : \begin{cases} 0 \rightarrow 0 \\ 1 \rightarrow 1 \end{cases} \qquad f_{b,2} : \begin{cases} 0 \rightarrow 1 \\ 1 \rightarrow 0 \end{cases}$$

constant

$$f_{c,1} : \begin{cases} 0 \rightarrow 0 \\ 1 \rightarrow 0 \end{cases} \qquad f_{c,2} : \begin{cases} 0 \rightarrow 1 \\ 1 \rightarrow 1 \end{cases}$$

- Example:

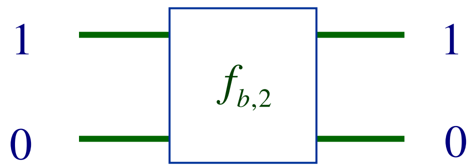


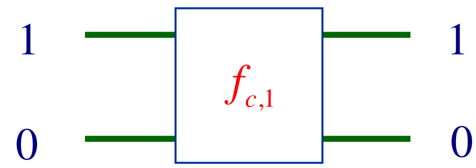
- We can use the box once.
- We have to find out if it is constant or one-to-one

QUANTUM ALGORITHMS
EXAMPLE

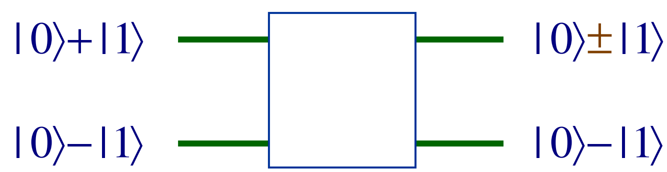
(Deutsch, 89)

Imposible: Every outcome is compatible with the two kinds of boxes





By using quantum superpositions, it is possible



(for const or 1-to1, resp.)

The existence of quantum superpositions gives us new possibilities and allows us to solve certain tasks in a more efficient way

QUANTUM COMPUTATION

new laws

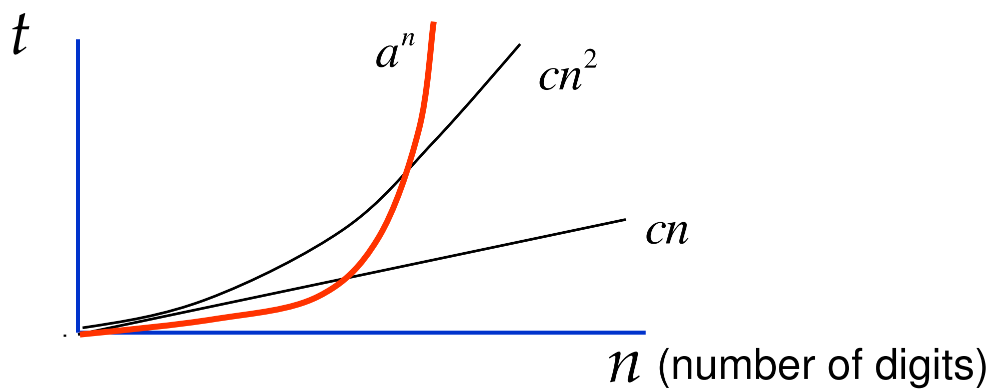
new algorithms

more efficient

COMPUTATIONAL COMPLEXITY

Quantum computers are more efficient than classical computers:

Mathematical problems can be classified according to their difficulty:
i.e. scaling of the computation time with the size of the input.



COMPUTATIONAL COMPLEXITY

(Shor, 94)

Example: multiplication and factoring:

3980750864240649373971 2550055038649119906436 2342526708406385189575 946388957261768583317

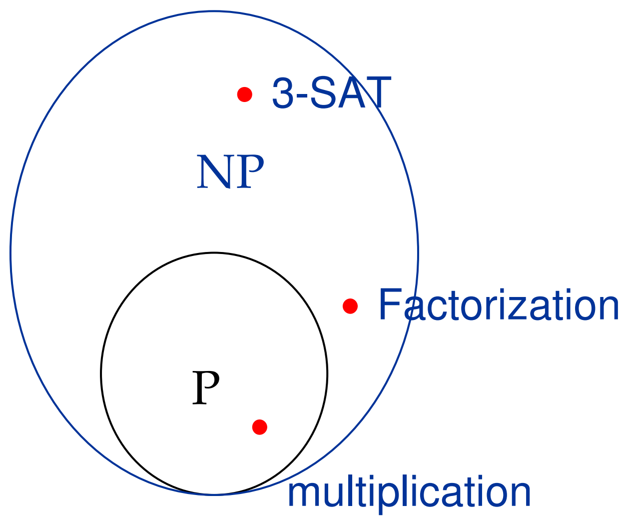
×

4727721461074353025362 2307197304822463291469 5302097116459852171130 520711256363590397527

=

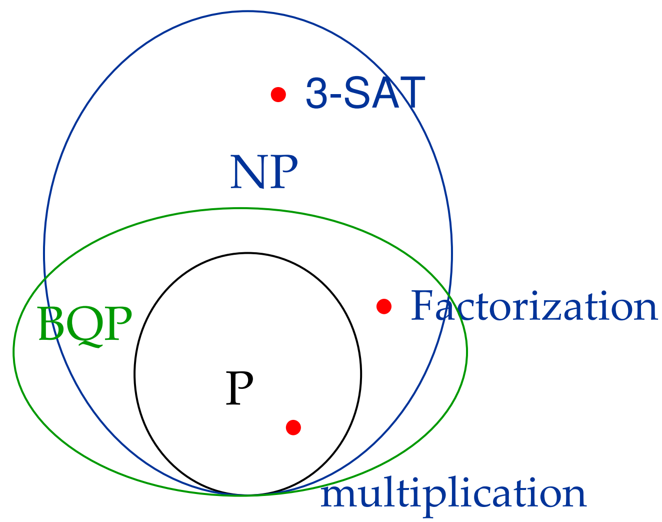
188198812920607963838697239461650439 807163563379417382700763356422988859 715234665485319060606504743045317388 011303396716199692321205734031879550 656996221305168759307650257059

Classical computational complexity:



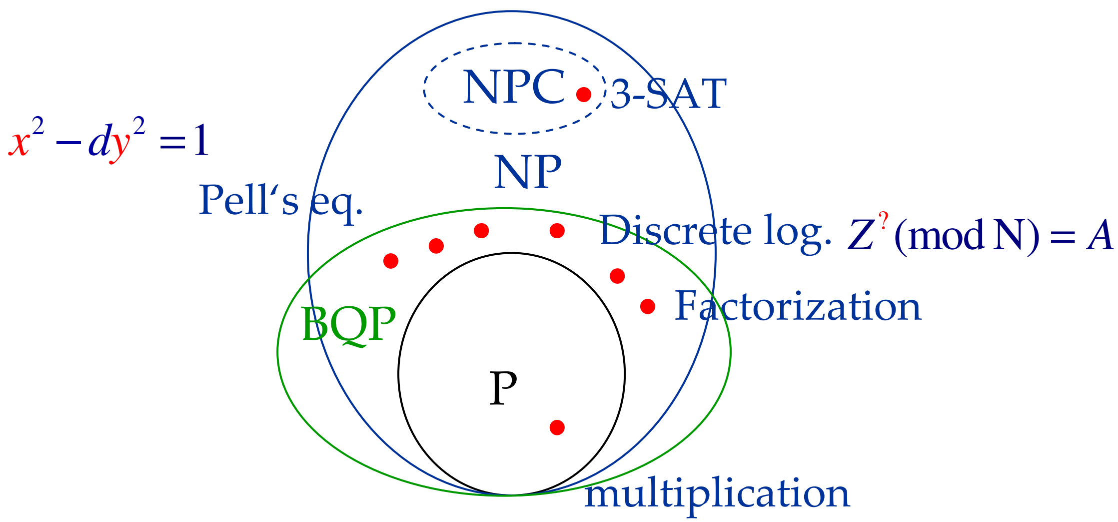
P=NP?

Quantum computational complexity:

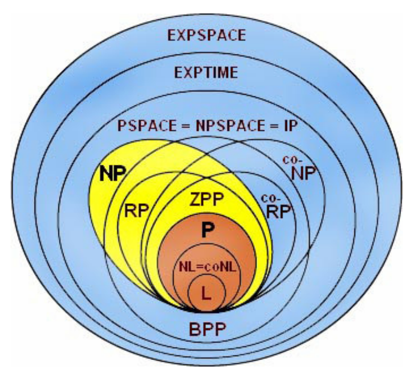


P=BQP? BQP=NP?

Quantum computational complexity:



There are other problems for which the gain is polynomical



QUANTUM ALGORITHMS

Algorithms:

- Factoring (94)
- Discrete Log (94)
- Database search (96)
- Pell's equation (02)
- Transversal graph (03)
- Special search (03)
- Element distinction (03)
- Other graph problems (04)
- Tests matrix products (04)
- Jones' polynomials (05)
- Matrix powers (06)
- NAND trees (07)
- Differential equations (08)

- Hidden subgroups:
  - Abelian (95)
  - $\mathbb{Z}_2^n \times \mathbb{Z}_2$ (98)
  - Normal (00)
  - Quasi-Abelian (01)
  - $\mathbb{Z}_{p^k}^n \times \mathbb{Z}_2$ (02)
  - Quasi-Hamiltonian (04)
  - q-hedrics (04)
  - $\mathbb{Z}_p^n \times \mathbb{Z}_p$ (04)
  - Heisenberg type (05)

QUANTUM COMPUTING:
CIRCUIT MODEL

CIRCUIT MODEL

(Deutsch, 85)

Classical computer:

1. Bits

$$0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0$$

2. Logical gates

$$0 \rightarrow 1$$

3Initialization and measurement

$$0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0$$

Quantum computer:

1. Qubits

$$|0\rangle|1\rangle|1\rangle|1\rangle|0\rangle|1\rangle$$

o superposiciones

2. Logical gates

$$|00\rangle \rightarrow |00\rangle + |11\rangle$$

3. Initialization and measurement

$$0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0$$

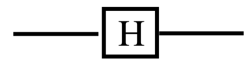
Manipulation: Universal quantum gates

- 1-qubit gates:

1. Phase:

$$|0\rangle \leftrightarrow |0\rangle$$
$$|1\rangle \leftrightarrow e^{i\varphi}|1\rangle$$

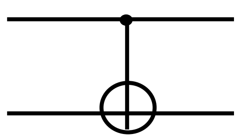
2. Hadamard:



$$|0\rangle \leftrightarrow |0\rangle + |1\rangle$$
$$|1\rangle \leftrightarrow |0\rangle - |1\rangle$$

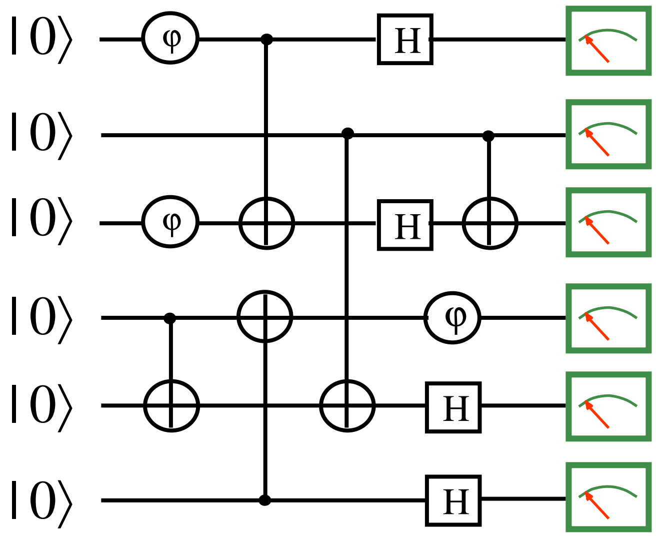
- 2-qubit gates:

1. Control-NOT



$$|00\rangle \leftrightarrow |00\rangle$$
$$|01\rangle \leftrightarrow |01\rangle$$
$$|10\rangle \leftrightarrow |11\rangle$$
$$|11\rangle \leftrightarrow |10\rangle$$

QUANTUM COMPUTING
CIRCUIT MODEL



Requirements:

- Identify qubits.
- Initialization.
- Controlled manipulation:
  Logic gates:
  + single-qubit
  + 2-qubit
- Read-out.

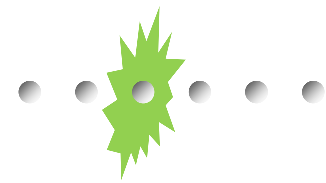
+ Scalable

QUANTUM COMPUTING:
DECOHERENCE AND ERROR CORRECTION

DECOHERENCE

- Interaction with the environment destroys the computation.

1 error messes up the outcome.



- Probability:

qubit: $\begin{cases} \text{Prob. } p & \text{: nothing happens} \\ \text{Prob. } 1-p & \text{: error } |0\rangle \leftrightarrow |1\rangle \end{cases}$

Success probability: p^N

Número of repetitions: $\frac{1}{p^N}$

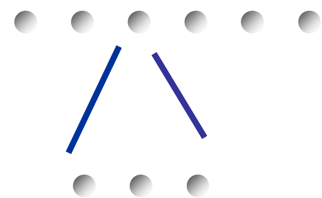
We have lost the exponential speed-up!

QUANTUM COMPUTING
ERROR CORRECTION

(Shor, Steane, 95)

- Redundant codes:

$$|0\rangle \rightarrow |000\rangle$$
$$|1\rangle \rightarrow |111\rangle$$



- We detect if all the qubits are in the same state
- If not, we use majority vote to correct the one which is different.

It fails if there are two or more errors

Error probability: $(1-p)^2 << (1-p)$ for small p

- Continuous measurement: Repeating the detection-correction procedure very often the errors can be kept arbitrarily small.

- Fault-tolerant error correction:

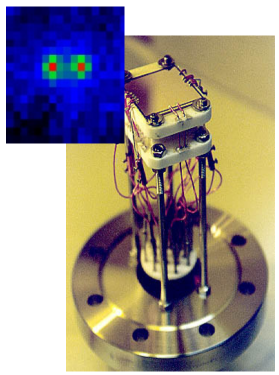
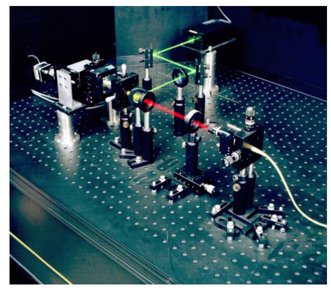
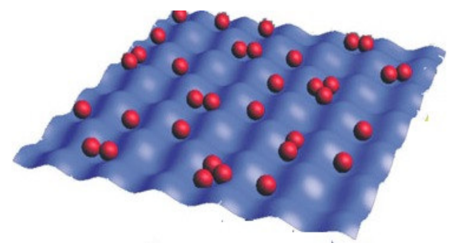
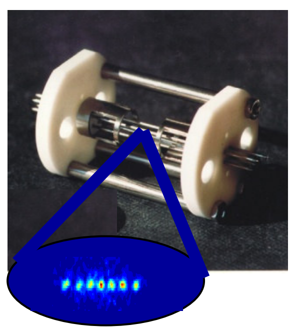
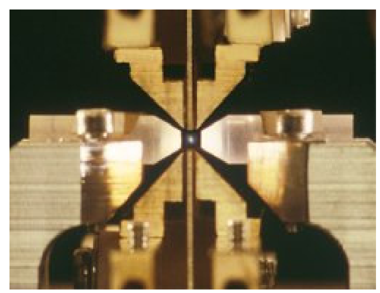
  - There are errors during the logical gates.
  - There are errors while correcting errors...

- Error threshold:

  Probability: $10^{-3} - 10^{-4}$ for each elementary step.

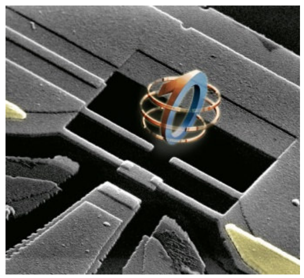
QUANTUM COMPUTING:
EXPERIMENTAL SITUATION

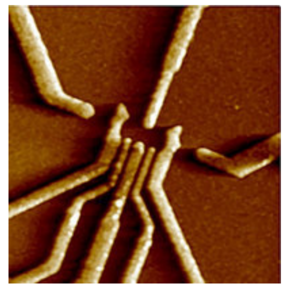
- Atomic, molecular, and optical systems

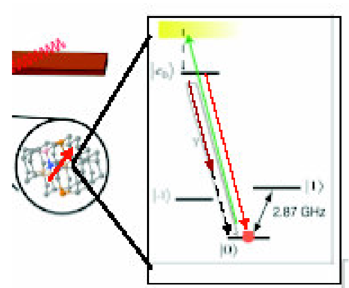






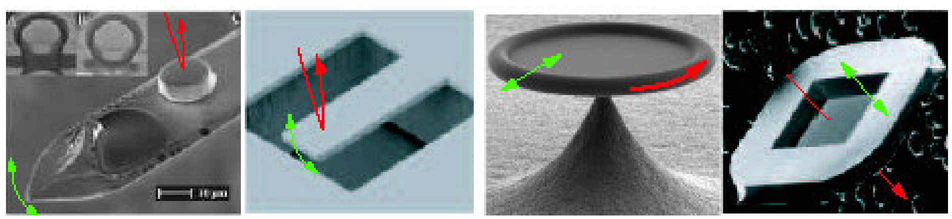

QUANTUM SYSTEMS
EXPERIMENTAL PROGRESS

- Solid-state systems

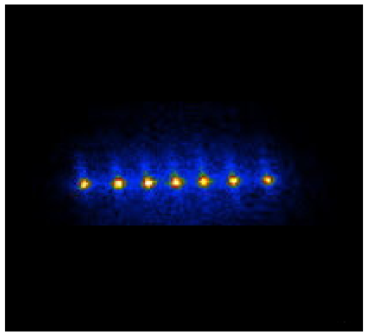


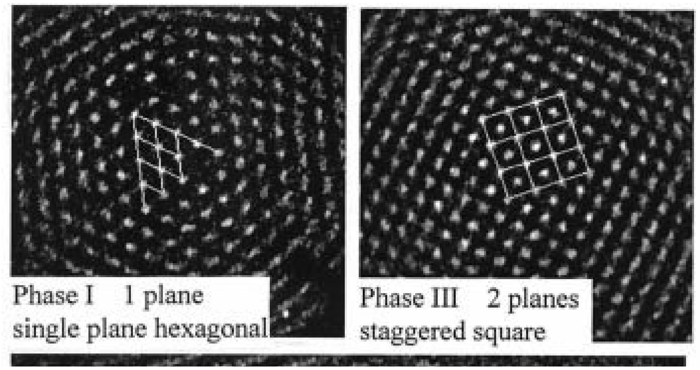






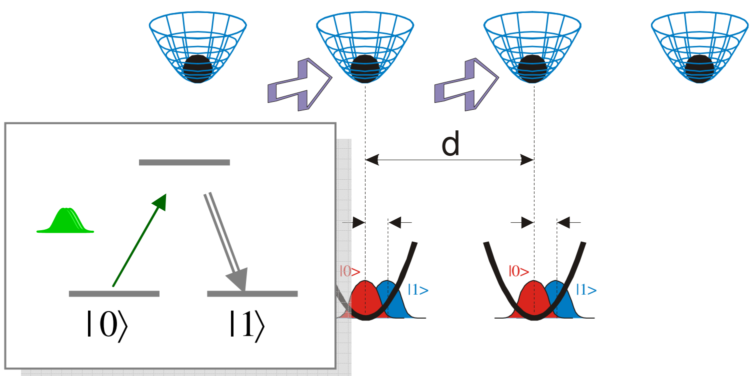
EXPERIMENTAL SITUATION
IONS





(Innsbruck, Boulder, Munich,
Oxford, Barcelona, Maryland, …)

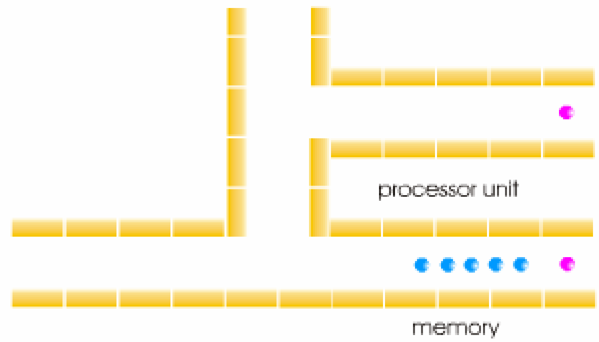
- Mechanism:



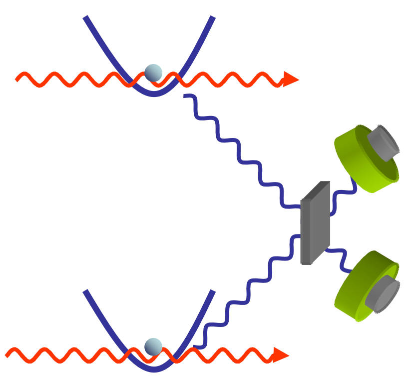
- Achievements:
  - Crystals: 1-1.000-100.000 ions
  - Single and two-qubit gates: > 99% fidelities
  - Detection: 99.99
  - Entanglement of up to 8 ions.

EXPERIMENTAL SITUATION
IONS

- Scalable versions:



- Mechanism:

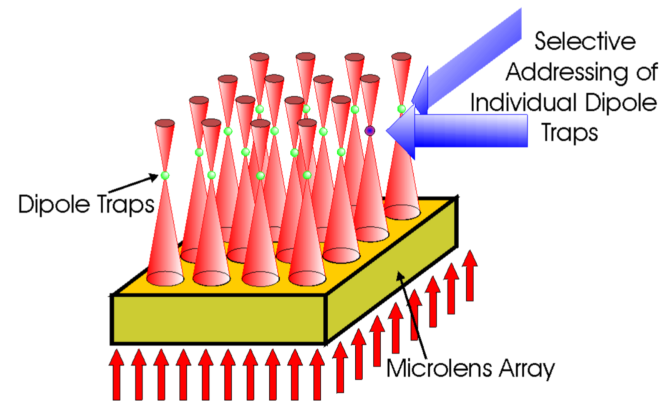


- Achievements:
  - Motion, simpathetic cooling, etc
  - Violation Bell's inequalities
  - Teleportation
  - Distant entanglement
  - Precission measurements
  - Simulation

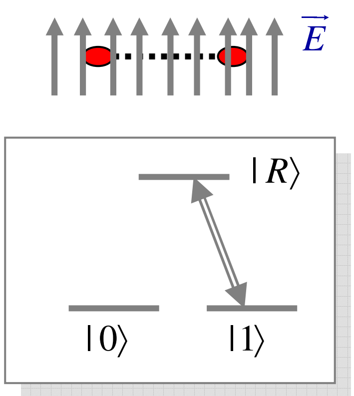
EXPERIMENTAL SITUATION
NEUTRAL ATOMS IN TRAPS

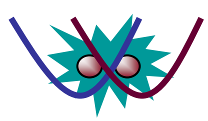
- Achievements:
  - From single atoms to condensates
  - BEC … optical lattices …
  - Single qubit gates: > 90% fidelities
  - Two atoms: Rydberg blockade/collisions
  - Detection: 99.99%
  - Moving atoms
  - Quantum simulations

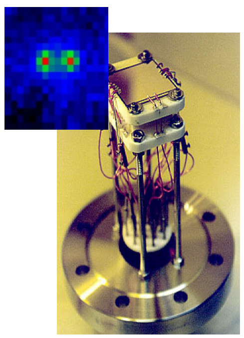
(Paris, Vienna, Hannover, London, Winsconsy, Boulder, Munich, …)

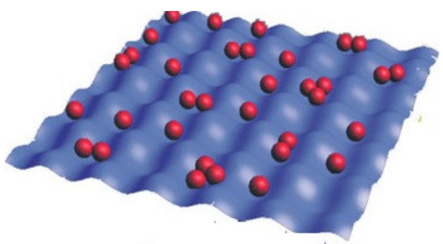


- Mechanisms:







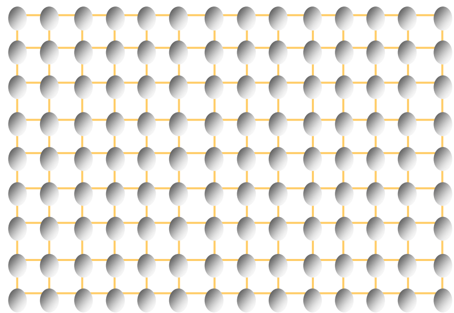


OTHER APPROACHES:
MEASUREMENT-BASED QUANTUM COMPUTING

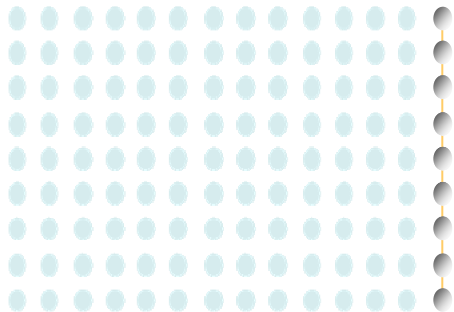
OTHER APPROACHES
MEASUREMENT BASED QC

(Raussendorf and Briegel, 01)

- Create an entangled-state (cluster):



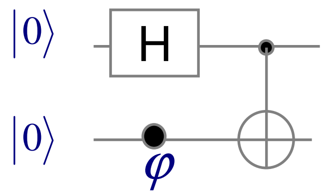
- Perform local measurements:



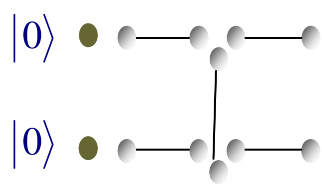
OTHER APPROACHES
MEASUREMENT BASED QC

(explanation: Verstraete and IC, 03)

- Teleportation-based gates:



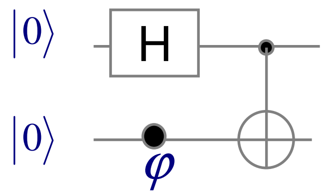
can be carried out as follows:



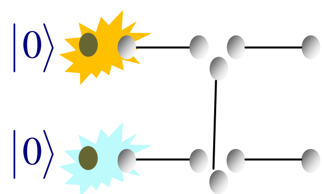
OTHER APPROACHES
MEASUREMENT BASED QC

(explanation: Verstraete and IC, 03)

- Teleportation-based gates:



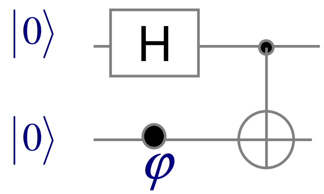
can be carried out as follows:



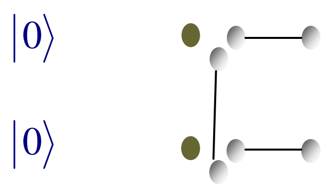
OTHER APPROACHES
MEASUREMENT BASED QC

(explanation: Verstraete and IC, 03)

- Teleportation-based gates:



can be carried out as follows:

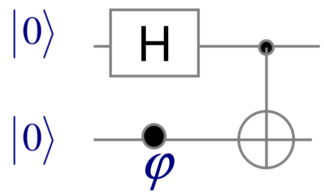


phase and Hadamard gates

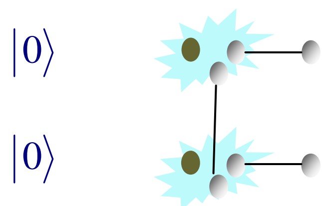
OTHER APPROACHES
MEASUREMENT BASED QC

(explanation: Verstraete and IC, 03)

- Teleportation-based gates:



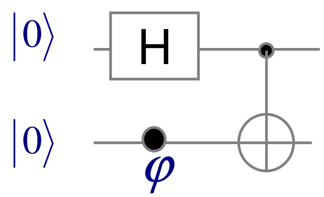
can be carried out as follows:



OTHER APPROACHES
MEASUREMENT BASED QC

(explanation: Verstraete and IC, 03)

- Teleportation-based gates:

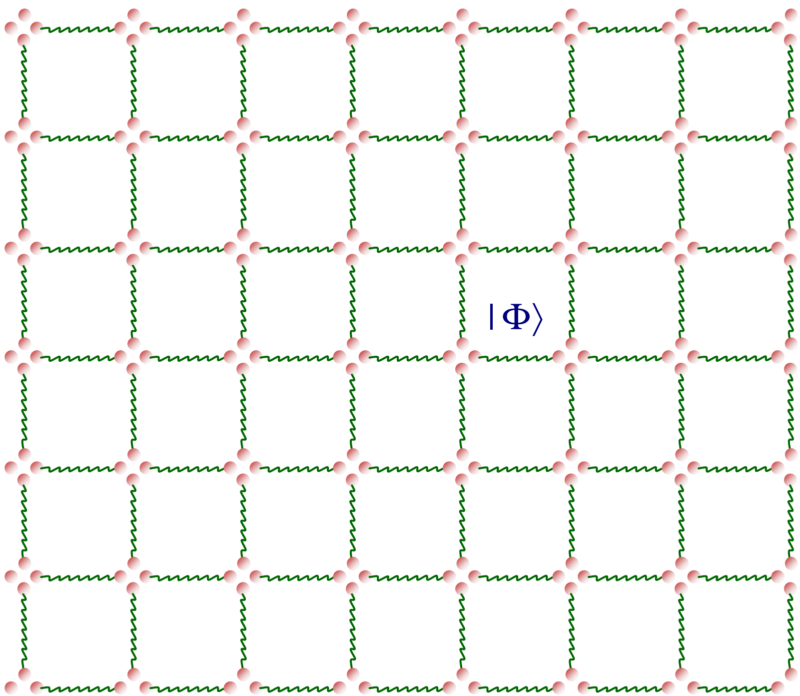


can be carried out as follows:

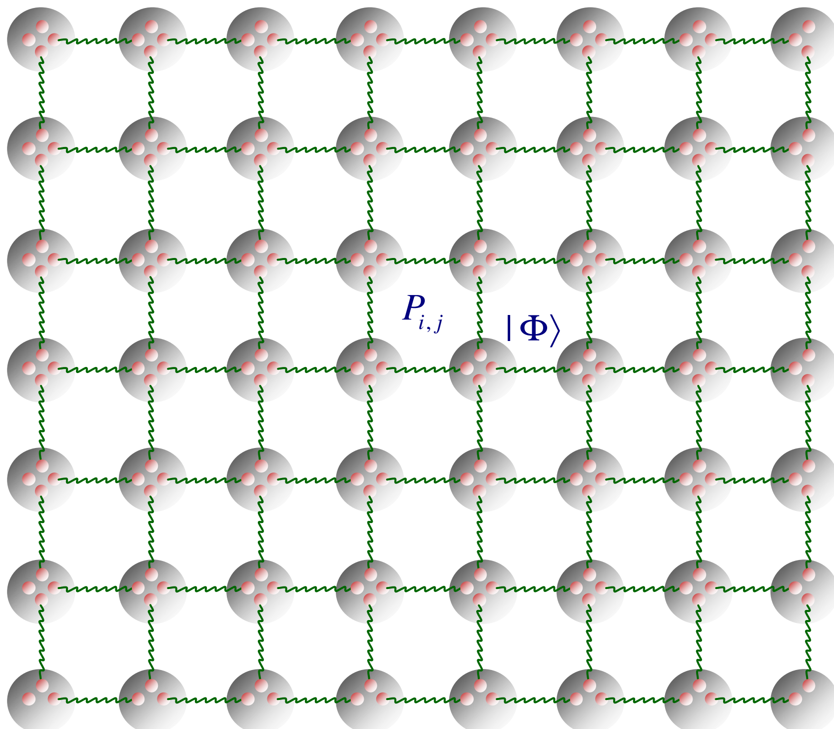
Controlled-not gate

OTHER APPROACHES
MEASUREMENT BASED QC

- In a 2D lattice



In a 2D lattice



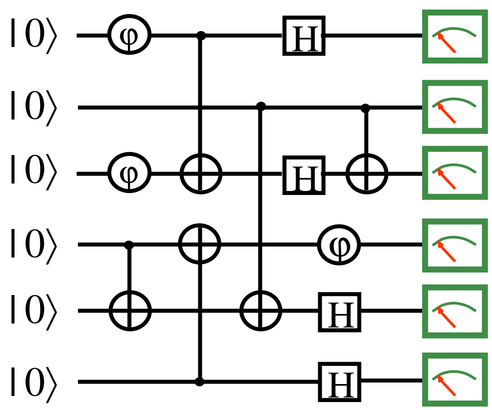
$$P_n : C^D \otimes C^D \otimes C^D \otimes C^D \to C^2$$

OTHER APPROACHES:
DISSIPATION-DRIVEN QUANTUM COMPUTING

OTHER APPROACHES
DISSIPATIVE QC

(Verstraete; Wolf and IC, 09)

Quantum computing:



i) ~~Initialization: $|00...0\rangle$~~

ii) ~~Controlled manipulation: $|\Psi_M\rangle = U_M...U_2U_1|00...0\rangle$~~

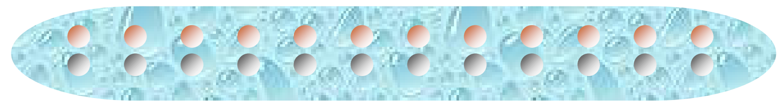
iii) Detection.

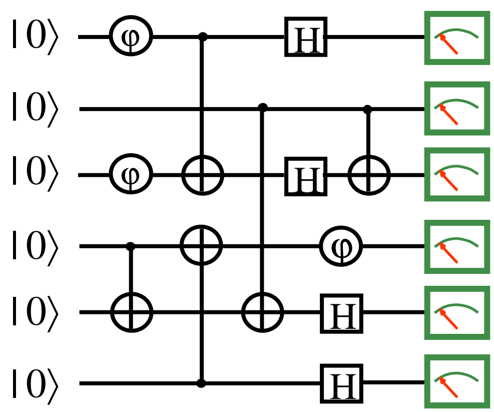
- ~~Avoid~~ use decoherence/dissipation: $|\Psi\rangle \to \rho$

OTHER APPROACHES
DISSIPATIVE QC

(Verstraete; Wolf and IC, 09)

N qubits:





$$|\Psi_M\rangle = U_M \ldots U_2 U_1 |00\ldots0\rangle$$

M gates

$$\dot{\rho} = -i[H,\rho] + \sum_k L_k \rho L_k^\dagger - \frac{1}{2}\left[\sum_k L_k^\dagger L_k, \rho\right]_+$$

no coherent interaction

local traceless

- Unique steady state: ρ_{ss}
- The steady state is reached after a time $O(M^{-2})$

$$\kappa = \pi^2 (3 + 2M)^{-2}$$

- Ψ_M can be obtained from ρ_{ss} with prob. $1/M$
- The Liouvillian can be engineered by coupling pairs of qubits to a local environment

OTHER APPROACHES
DISSIPATIVE QC

Main Idea:

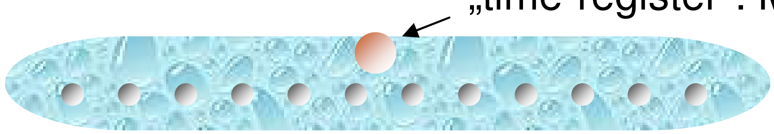
(Verstraete; Wolf and IC, 09)

- Standard QC:

$$|\Psi_M\rangle = U_M \ldots U_2 U_1 |00\ldots0\rangle$$

- With dissipation: Use Feynman construction:

„time-register“: M-level system



$$\dot{\rho} = \sum_k L_k \rho L_k^\dagger - \frac{1}{2}\left[\sum_k L_k^\dagger L_k, \rho\right]_+$$

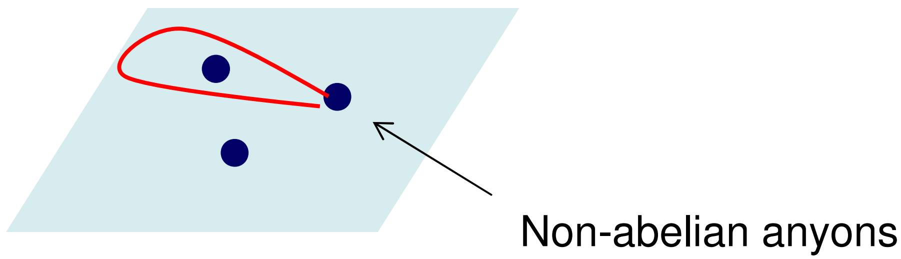
  - Define: $|\Psi_t\rangle = U_t \ldots U_2 U_1 |00\ldots0\rangle$
  - Assume we start out with: $|00\ldots0\rangle \otimes |0\rangle$
  - We take $L_t = U_t \otimes |t+1\rangle\langle t| + U_t^\dagger \otimes |t\rangle\langle t+1|$ as Lindblad operators
  - The evolution takes place in the subspace spanned by $|\Psi_t\rangle \otimes |t\rangle$
  - For $t \to \infty$ one ends up in $\rho_0 = \frac{1}{(1+M)} \sum_{t=0}^{M} |\Psi_t\rangle\langle\Psi_t| \otimes |t\rangle\langle t|$
  - By measuring the second register we obtain the right state with prob. 1/(1+M)

OTHER APPROACHES:
TOPOLOGICAL QUANTUM COMPUTING

OTHER APPROACHES
TOPOLOGICAL QC

(Kitaev 97)

Main Idea:

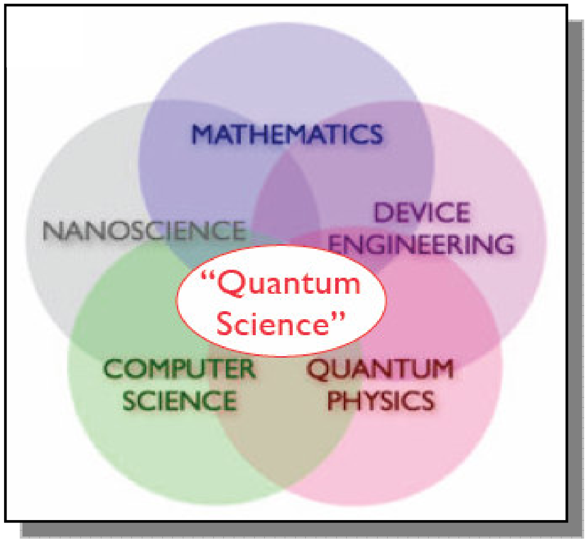


- Gates are performed by „braiding“
- Gates are robust against imprecisions
- The state is „topologically proctected“ against decoherence

Search for systems with (universal) non-abelian excitations!

OUTLOOK

- Multi-disciplinary area:



- Applications:
  - Communication
  - Computation
  - Precission measurement
  - Sensors
  - Materials science
  - …

- Main distinctive feature: coherent quantum phenomena.
- Common objectives.
- Next step after nano-science.
- Preparation of the „second quantum revolution“
- Goal: control of quantum systems
- A theory to be developed …