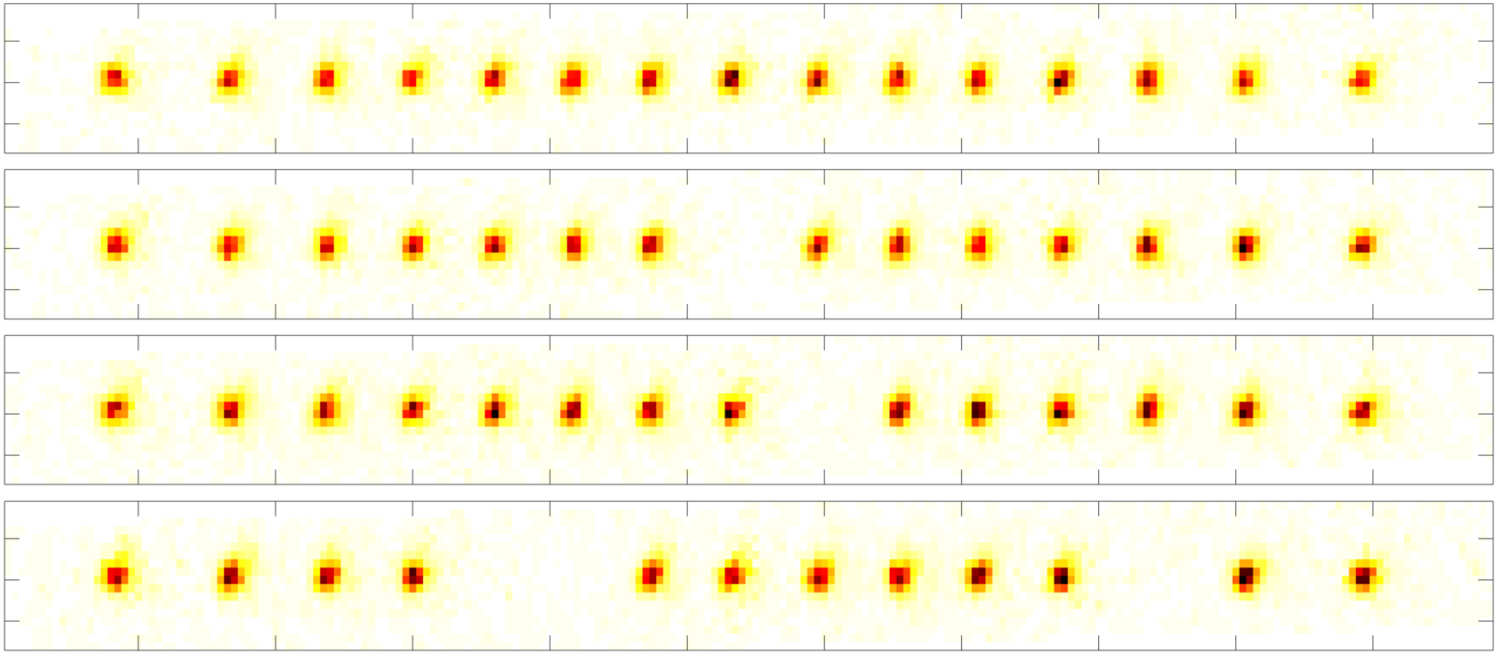
# Quantum information processing with trapped ions



Christian Roos
Institute for Quantum Optics and Quantum Information
Innsbruck, Austria

Les Houches Winter School on "Physics with Trapped Particles", 19-30.1.2015

# Quantum information processing with trapped ions

Content:

1. Quantum information processing
2. Basics of quantum information with trapped ions
3. Quantum information and simulation with trapped ions
4. Entanglement (in trapped ion experiments)

# Quantum information processing

## Physics

- study of Nature
- based on observation
- mathematical models explaining and predicting phenomena

deals with material world

## Information

… can be communicated

… can be stored

… can be processed

… can be quantified

abstract and immaterial ?

Rolf Landauer (1991): Information is physical !

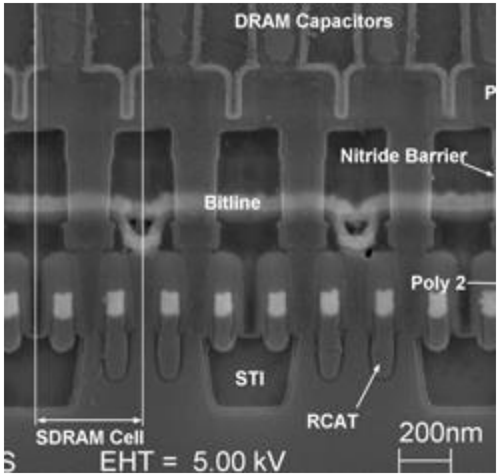
Phys. Today **43**(?), 26 (1991)

# Information is physical

**Storage and processing of information requires a physical representation of information:**

Encoding a bit as

- charge state of a capacitor
- magnetic orientation of a ferromagnet
- bistable electronic circuit




**Do physical laws set limits as to how information can be processed?**

**Landauer's principle** (1961): erasing information requires dissipation

$\longrightarrow$ minimun energy cost $\Delta Q = T\Delta S = k_B T \log 2$

# Information is physical

**Reversible computation**

Logic gates are typically irreversible and create entropy:

Example: NAND $(a,b) \to \neg(a \wedge b)$

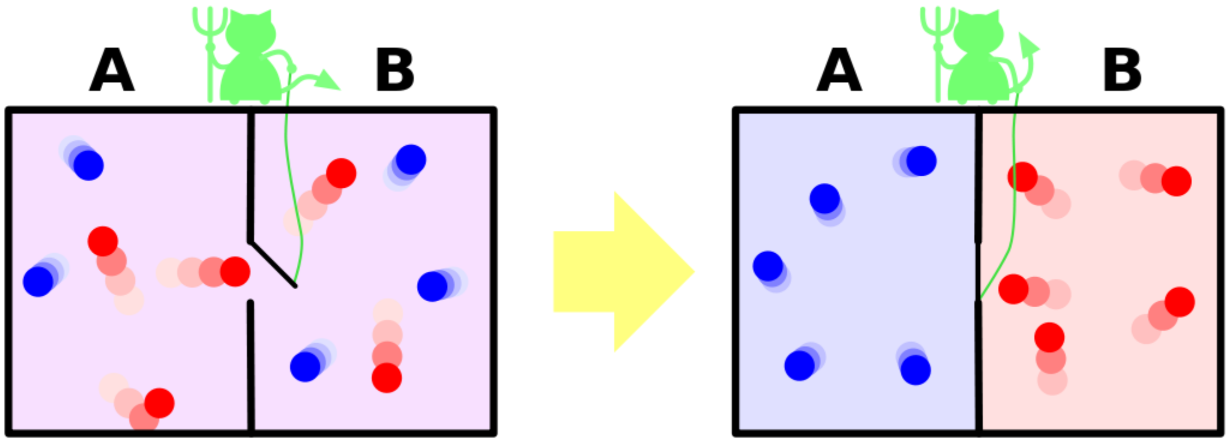
$$\begin{aligned}(0,0) &\to 1\\(0,1) &\to 0\\(1,0) &\to 0\\(1,1) &\to 0\end{aligned}$$

$\longrightarrow$ minimum energy cost of computation can be overcome by reversible computation based on Toffoli gates:

$$(a,b,c) \to (a,b,c \oplus a \wedge b)$$

# Information and thermodynamics

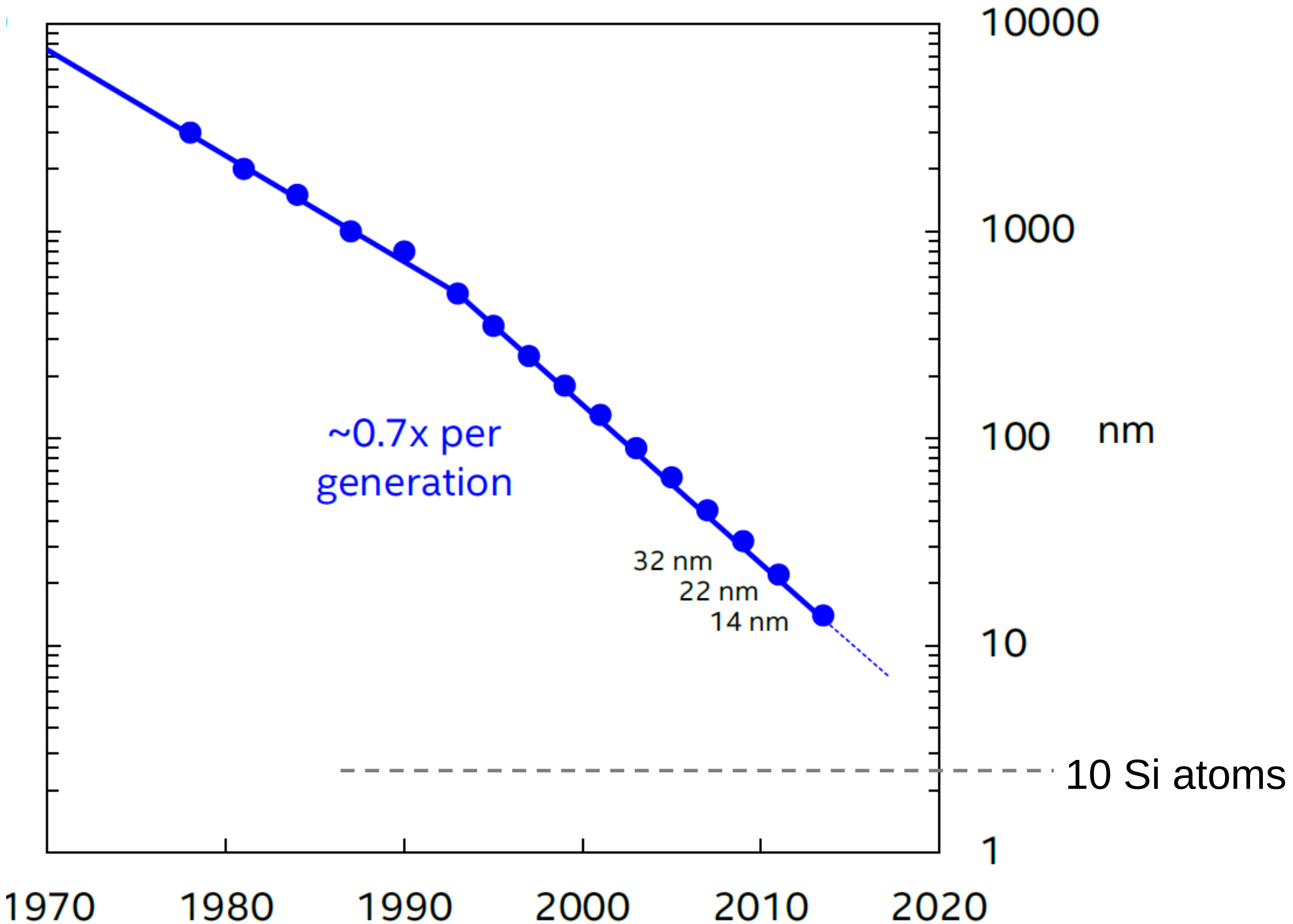
**Maxwell's demon:** Violation of second law of thermodynamics?




source: https://commons.wikimedia.org/wiki/File:Maxwell%27s_demon.svg

C. Bennett (1982): Even if the demon operated without energy expense,
the information about the demon's measurements of molecules would have to stored.
finite storage capacity prevents cooling of the gas.

# Development of logic gate size

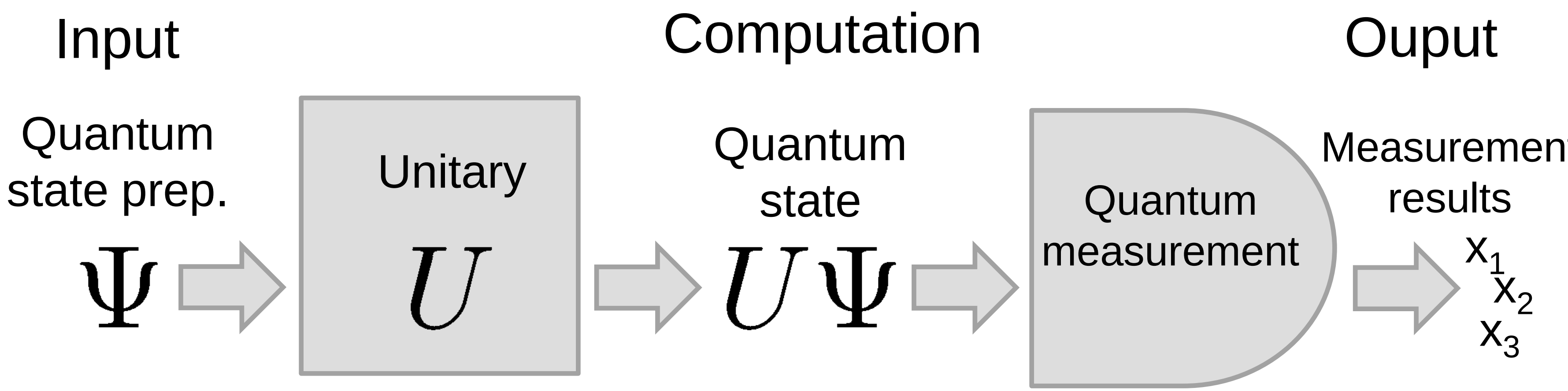



Quantum physics

source: www.intel.com

# Information processing and quantum physics

How can information be encoded in and processed by quantum systems?




Remarks:

- The outcome of a computation is probabilistic because of the quantum measurement process.
- In general, quantum measurements will act only on parts of the quantum state and followed by further unitary operations and measurements

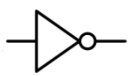
# Classical vs. quantum information processing

**Bit:**

Physical system with two distinct states 0 or 1

**Logic gates**

Boolean logic operation



$$0 \rightarrow 1$$
$$1 \rightarrow 0$$

$$(\epsilon_1, \epsilon_2) \rightarrow \epsilon_1 \oplus \epsilon_2$$

XOR truth table

$$(0,0) \longrightarrow 0$$
$$(0,1) \longrightarrow 1$$
$$(1,0) \longrightarrow 1$$
$$(1,1) \longrightarrow 0$$

**Quantum bit:**

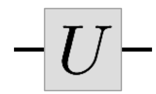
Two-level quantum system with state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

**Quantum logic gate**

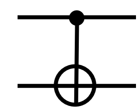
Unitary transformation

single qubit gate




$$|\psi\rangle \rightarrow U|\psi\rangle$$

two-qubit gate



$$|\epsilon_1\rangle|\epsilon_2\rangle \rightarrow |\epsilon_1\rangle|\epsilon_1 \oplus \epsilon_2\rangle$$

CNOT truth table

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

# Classical vs. quantum information processing

**Bit:**

Physical system with two distinct states 0 or 1

**Quantum bit:**

Two-level quantum system with state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

**Logic gates**

Boolean logic operation

$0 \rightarrow 1$

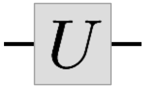
$1 \rightarrow 0$

$(\epsilon_1, \epsilon_2) \rightarrow \epsilon_1 \oplus \epsilon_2$

**Quantum logic gate**

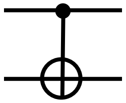
Unitary transformation

single qubit gate



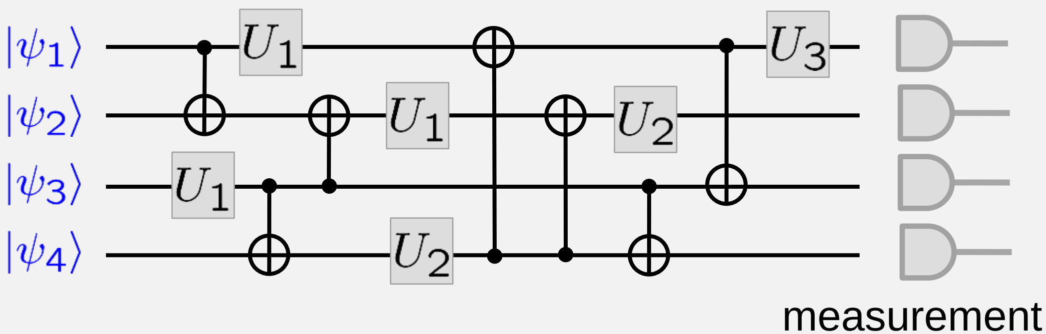

$|\psi\rangle \rightarrow U|\psi\rangle$

two-qubit gate



$|\epsilon_1\rangle|\epsilon_2\rangle \rightarrow |\epsilon_1\rangle|\epsilon_1 \oplus \epsilon_2\rangle$

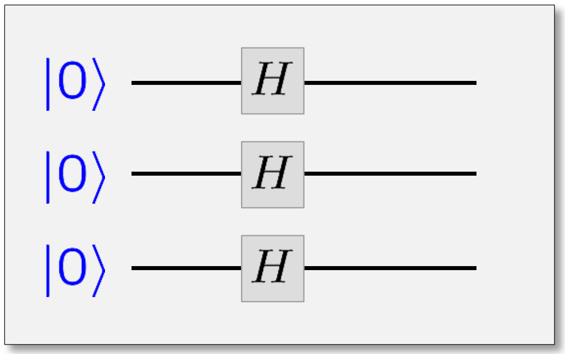
Quantum logic circuit



# Superpositions and entanglement

## Putting a quantum register in a superposition

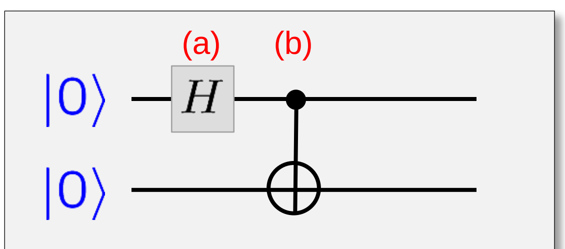
$$|\psi\rangle = |0\rangle|0\rangle|0\rangle \longrightarrow (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$




$$= |000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle$$

If applied at the start of a quantum algorithm, this operation enables parallel processing on all possible input states.

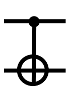
## Entangling quantum bits in a quantum register




$$|\psi\rangle = |0\rangle|0\rangle \xrightarrow{(a)} (|0\rangle + |1\rangle)|0\rangle \xrightarrow{(b)} |00\rangle + |11\rangle$$

The computation creates quantum correlations between the qubits.

controlled-NOT gate



$$= |\epsilon_1\rangle|\epsilon_2\rangle \longrightarrow |\epsilon_1\rangle|\epsilon_1 \oplus \epsilon_2\rangle$$

# How hard is a computational problem?

**How does the computation time T scale with the  size of the input size n ?**

| Examples: | algorithm | computation time |
|---|---|---|
| | addition of two numbers | $\mathcal{O}(n)$ |
| | (naive) multiplication of two numbers | $\mathcal{O}(n^2)$ |
| | (naive) matrix multiplication | $\mathcal{O}(n^3)$ |

**Complexity classes**

**P:** The set of problems that can be solved in polynomial time $T = \mathcal{O}(n^k)$

**NP:** The set of problems whose solutions can be checked in polynomial time

**… and many more**

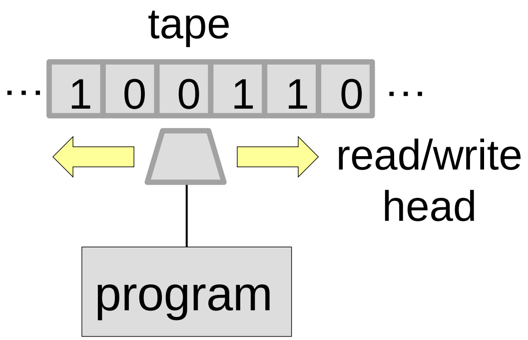
Example: factorization of numbers is in NP but probably not in P

Open question: **P ≠ NP ?**

# How hard is a computational problem?

**P:** The set of problems that can be solved in polynomial time $T = \mathcal{O}(n^k)$ on a Turing machine

Turing machine: a model for a universal computer




Classical computers can efficiently simulate Turing machines.

→ complexity of a problem does not depend on computer hardware

Does the hardness of a problem change when run on a quantum computer?

# Factoring numbers

**Finding prime factors on a classical computer:**

$N = p \cdot q$ → factoring

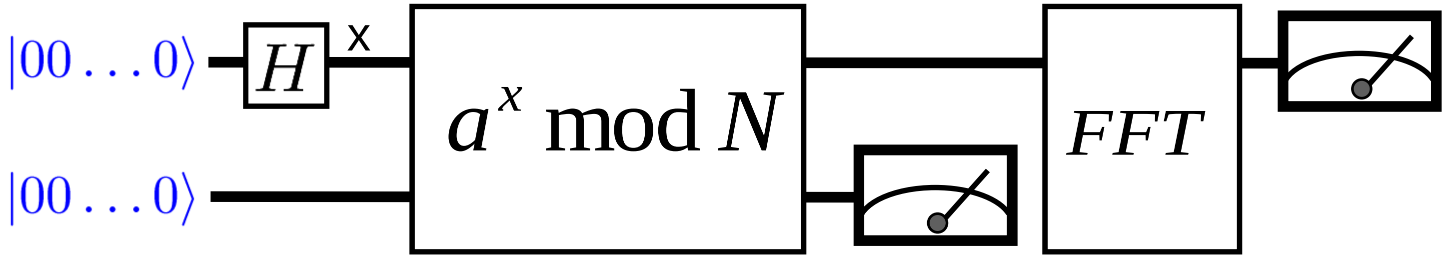
hard:
known classical algorithms
have exponential run time

$p \cdot q = N$ → multiplication

easy:
Solution to problem
easily checked
-> problem is in NP

**Finding prime factors on a classical computer:**

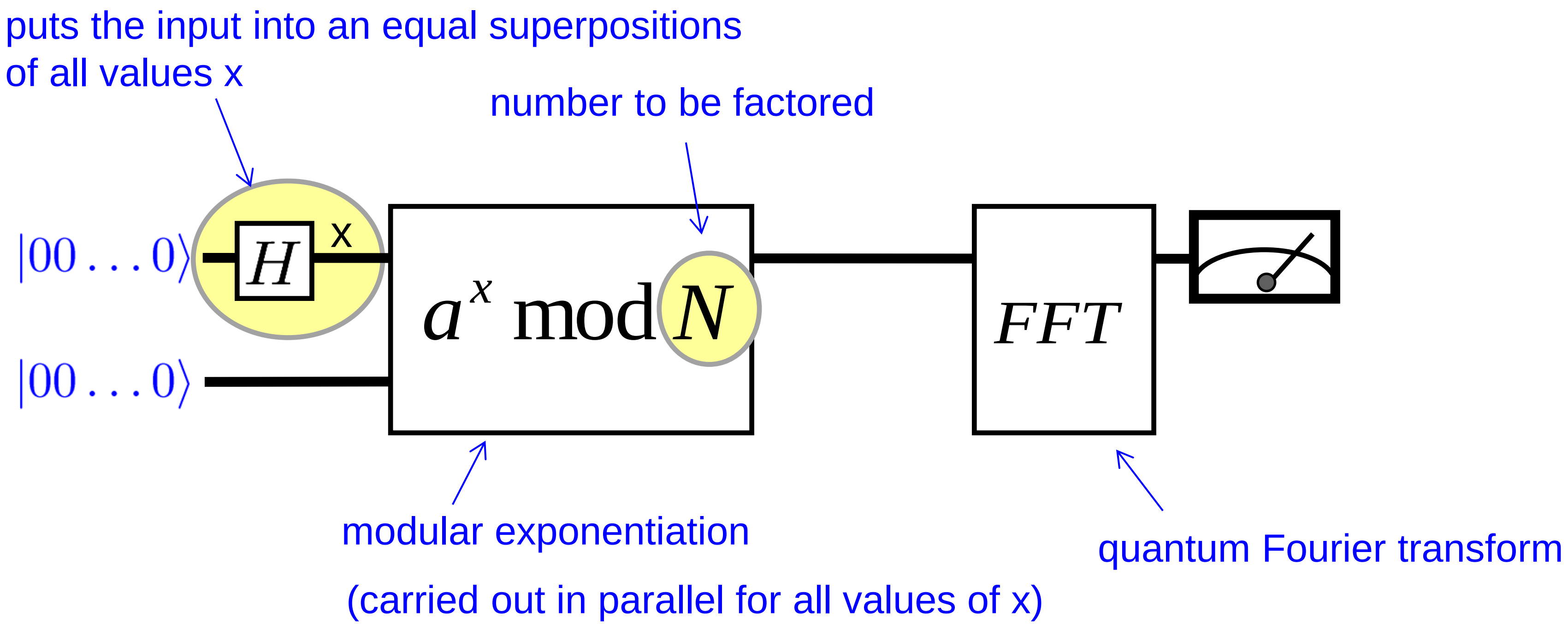
Peter Shor (1994): A quantum computer can factor large numbers in subexponential time



# Factoring numbers

**Finding prime factors on a classical computer:**

Peter Shor (1994): A quantum computer can factor large numbers in subexponential time.




N: n-bit number -> 2n qubits required, ~$n^3$ gate operations

The Shor algorithm is an indication of quantum computing's superior power over classical computing for certain classes of problems.

# Where does the power of quantum computing stem from?

**Superposition principle** *parallel computing?*

> *[…].Because a quantum computer essentially operates as a massive parallel processing machine, it can work on millions of calculations simultaneously (whereas a traditional computer works on one calculation at a time, in sequence).*
> *. . .* http://www.techradar.com/news/computing/the-mind-blowing-possibilities-of-quantum-computing-663261

**Wrong!**

Easy to put a quantum register into a superposition of all input states:

$$|0\rangle \longrightarrow |0\rangle + |1\rangle \qquad |00\ldots0\rangle \longrightarrow |\Psi\rangle = \sum_{i=0}^{2^N-1} |x_i\rangle$$

$$|x_0\rangle = |00\ldots00\rangle$$
$$|x_1\rangle = |00\ldots01\rangle$$
$$|x_2\rangle = |00\ldots11\rangle$$
$$\vdots$$

Quantum parallelism during coherent evolution:

$$|\Psi\rangle \longrightarrow U|\Psi\rangle = \sum_{i=0}^{2^N-1} U|x_i\rangle$$

But: A quantum measurement yields only one bit of information per qubit.
we cannot read out the result of the "parallel computation"!

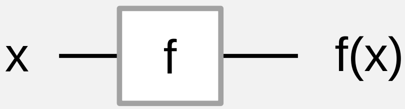
Quantum algorithms need to make clever use of the superposition principle to map all the relevant information in a way that can be read out by single measurement.

# Interlude:

# Deutsch algorithm: quantum parallelism at work

# Deutsch algorithm: quantum parallelism at work

**The problem (classical version):** Find out whether the function *f* operating on bit x is balanced or even.




$$f_1 : \begin{cases} 0 \longrightarrow 0 \\ 1 \longrightarrow 1 \end{cases} \qquad f_3 : \begin{cases} 0 \longrightarrow 0 \\ 1 \longrightarrow 0 \end{cases}$$

$$f_2 : \begin{cases} 0 \longrightarrow 1 \\ 1 \longrightarrow 0 \end{cases} \qquad f_4 : \begin{cases} 0 \longrightarrow 1 \\ 1 \longrightarrow 1 \end{cases}$$

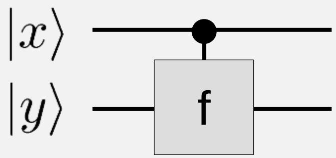
balanced constant

The function needs to be evaluated twice to find the solution.

Can a quantum processor do better?

# Deutsch algorithm: quantum parallelism at work

**The problem (quantum version):** Find out whether the function *f* operating on bit x is balanced or even.




$$|x\rangle|y\rangle \longrightarrow |x\rangle|y \otimes f(x)\rangle$$

addition modulo 2

qubits (two qubits needed to ensure that the operation is unitary)

We have $|x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$

$$|x\rangle|1\rangle \longrightarrow |x\rangle|\neg f(x)\rangle \qquad (\neg\text{: logical not})$$

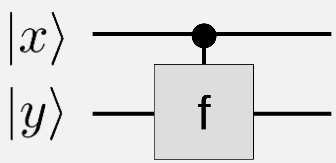
Naive approach to quantum parallelism: doing the calculation simultaneously for both input values: $|x\rangle = |0\rangle + |1\rangle$

$$|0\rangle + |1\rangle|0\rangle \longrightarrow |0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$$

Not very helpful for this problem; we cannot read out the results simultaneously. The two parts of the superposition need to interfere.

# Deutsch algorithm: quantum parallelism at work

**The problem (quantum version):** Find out whether the function *f* operating on bit x is balanced or even.




$$|x\rangle|y\rangle \longrightarrow |x\rangle|y \otimes f(x)\rangle$$

A better input state:

$$|x\rangle(|0\rangle - |1\rangle) \longrightarrow |x\rangle(|f(x)\rangle - |\neg f(x)\rangle)$$

$$= \left\{ \begin{array}{ll} |x\rangle(|0\rangle - |1\rangle) & \text{if } \ f(x) = 0 \\ |x\rangle(|1\rangle - |0\rangle) & \text{if } \ f(x) = 1 \end{array} \right\} = (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Specifically:

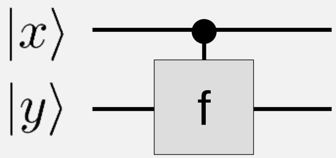
$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \longrightarrow ((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)(|0\rangle - |1\rangle)$$

$$= (\underbrace{|0\rangle + (-1)^{f(0)+f(1)}|1\rangle}_{})(|0\rangle - |1\rangle)$$

$$= \left\{ \begin{array}{ll} |0\rangle + |1\rangle & \text{if } \ f(x) \text{ constant} \\ |0\rangle - |1\rangle & \text{if } \ f(x) \text{ balanced} \end{array} \right.$$

# Deutsch algorithm: quantum parallelism at work

**The problem (quantum version):** Find out whether the function *f* operating on bit x is balanced or even.



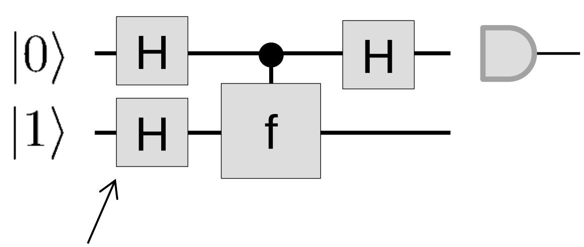

$$|x\rangle|y\rangle \longrightarrow |x\rangle|y \otimes f(x)\rangle$$

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \longrightarrow \underbrace{(|0\rangle + (-1)^{f(0)+f(1)}|1\rangle)}(|0\rangle - |1\rangle)$$

$$= \begin{cases} |0\rangle + |1\rangle & \text{if } f(x) \text{ constant} \\ |0\rangle - |1\rangle & \text{if } f(x) \text{ balanced} \end{cases}$$

All we need to do is to measure whether the first qubit is in state |0+1⟩ or |0-1⟩

Final quantum circuit:




measure qubit in state |0⟩ or |1⟩

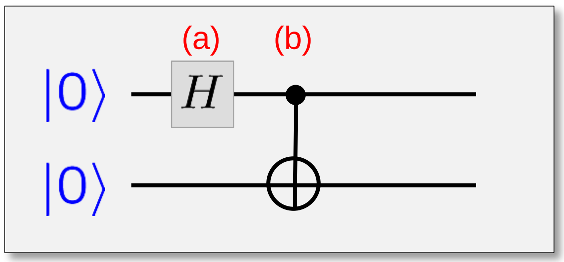
Hadamard gate $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

A single run of the circuit suffices to find the answer

# Where does the power of quantum computing stem from?

## Entanglement

In nearly every quantum computation, qubits become highly entangled.

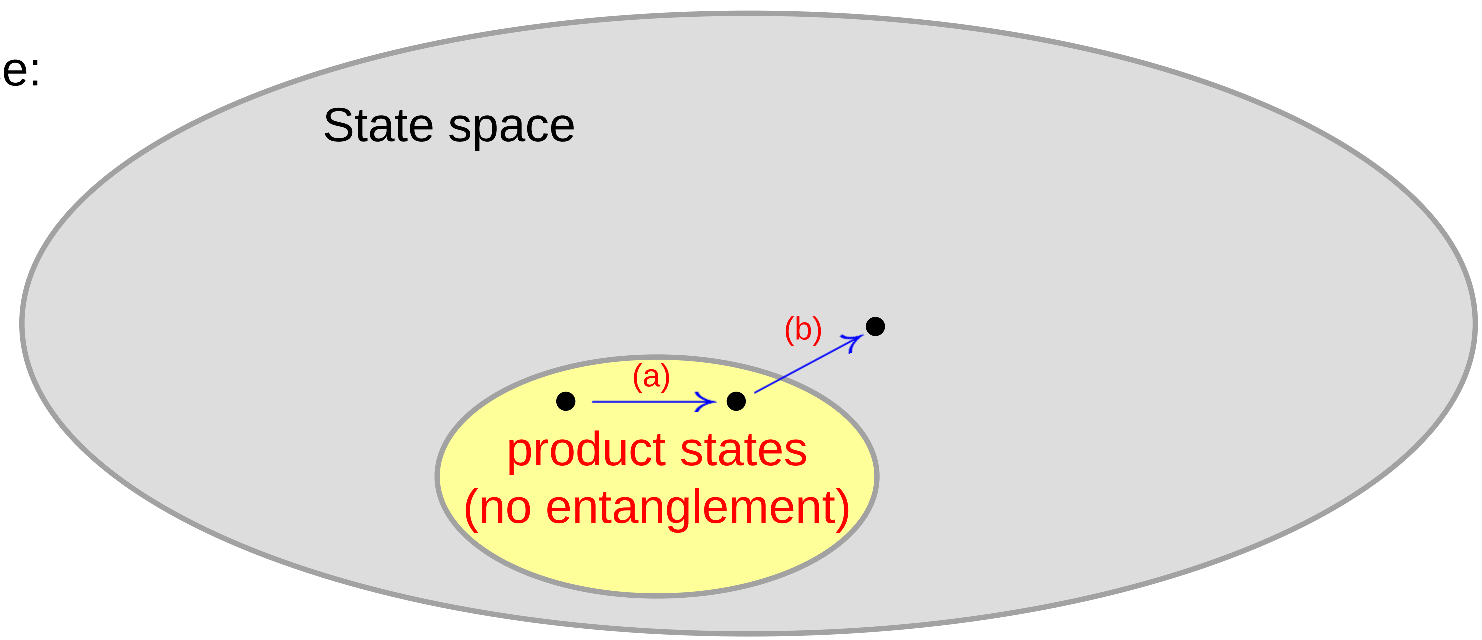



$$|\psi\rangle = |0\rangle|0\rangle \xrightarrow{(a)} (|0\rangle + |1\rangle)|0\rangle$$

$$\xrightarrow{(b)} |00\rangle + |11\rangle$$

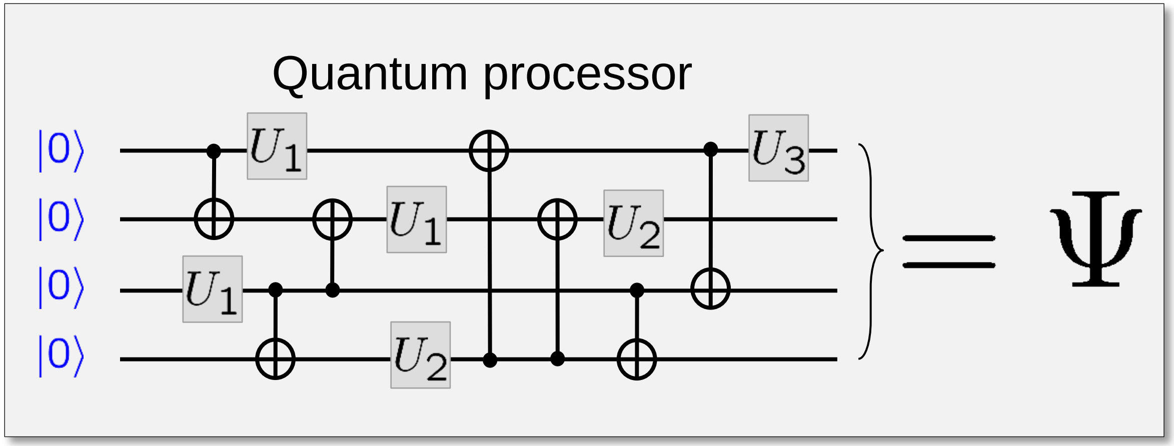
Interactions between quantum systems generate almost always entanglement!

Hilbert space:



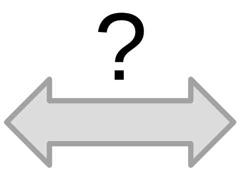
# … and back to the main topic

# Quantum processor: coupling to the environment?




Typical states:

highly entangled states
of many qubits




Schrödinger cat states: highly sensitive to decoherence


Are the states produced by a quantum processor as fragile to decoherence
as Schrödinger cat states ?

Does decoherence kill the concept of a real-world quantum processor?

# Quantum computing in the presence of errors

Can quantum computing cope with imperfections causing errors?

(imperfect gate operations, coupling to the environment)

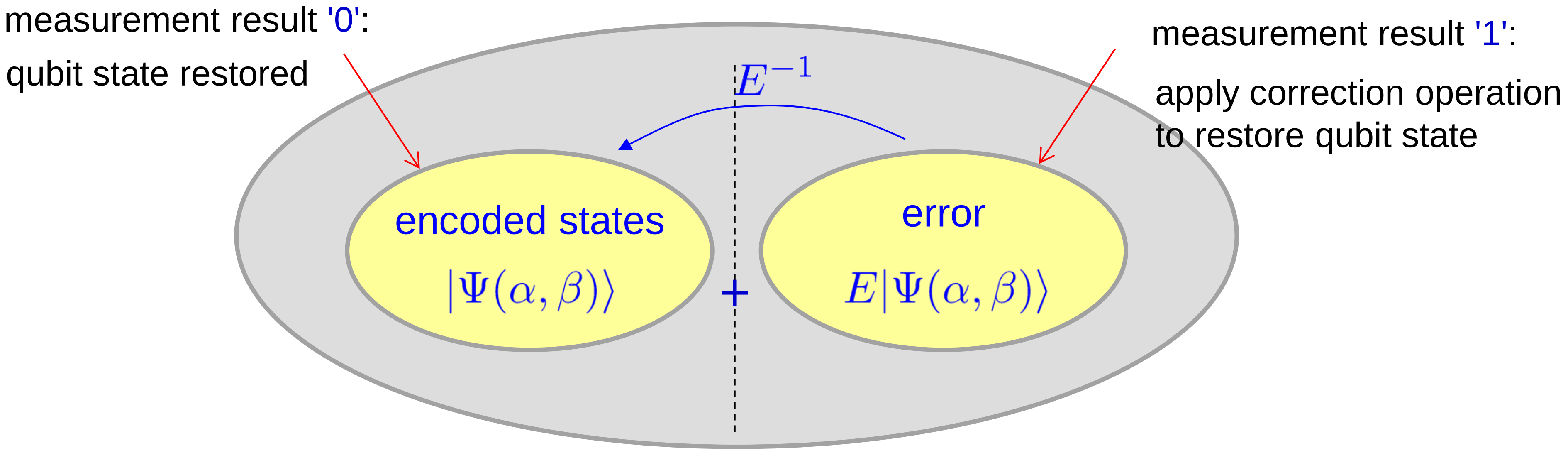
**Challenges:** 1. Errors are not discrete. (a coherent operation can be slightly wrong)

2. A measurement detecting an error will disturb the quantum state.

3. Quantum states cannot be cloned. (no redundant encoding possible)

**Strategy**: encode qubit in several qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\Psi(\alpha,\beta)\rangle$

Project onto qubit state space: preserves qubit + discretizes error



# Fault-tolerant quantum computing

**Is quantum computation in the presence of noise possible ?**

Yes, error correction techniques can be applied provided
that the errors per operation are below a certain treshold.

⟶ Arbitrarily good computations are theoretically achievable

**Strategy:**

- carry out quantum gates operations on encoded data
- use quantum error correction to reduce errors

  (concatenated error correction schemes)

**The prize to pay:**

- many more qubits and operations required as compared to error-free quantum computation
- error thresholds are a big challenge to experiments

  (~ $10^{-5}$ …$10^{-2}$ per quantum gate)

# Quantum information processing

## Quantum information

Investigating resources for information processing tasks, entanglement characterization,…

## Quantum computing

Quantum algorithms for efficient computing

## Quantum communication

Secure communication certified by quantum physics

## Quantum simulation

Investigating many-body Hamiltonians using well-controlled quantum systems

## Quantum metrology

Entanglement-enhanced measurements

→ Piet Schmidt's lecture