# What is Quantum Computing?

Vladimir P. Gerdt

Laboratory of Information Technologies

Joint Institute for Nuclear Research

Dubna, Russia

## Introduction

1. Current computers still have problems with certain mathematical problems:

   These problems are used in today's current encryption methods.

   Accurately modeling quantum mechanical processes.

2. Computers are becoming more powerful everyday.

3. These computers will eventually find a limit to there capabilities.

## Simulating Physics with Computers

Can a universal classical computer simulate physics *exactly*?

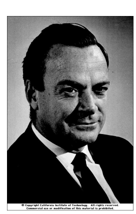
Can a classical computer *efficiently* simulate quantum mechanics?

"I'm not happy with all the analyses that go with just classical theory, because Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem!"

Richard Feynman 1981

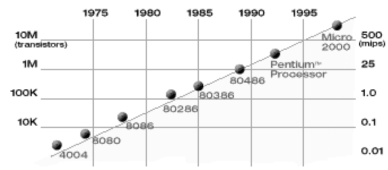
"How can we simulate the quantum mechanics?....Can you do it with a new kind of computer - a quantum computer? It is not a Turing machine, but a machine of a different kind."

R P Feynman 1981

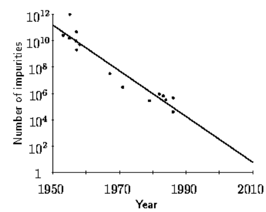


## Limitations of Classical Computer Technology

- Moore's Law.
  - Gordon E. Moore
  - Developed in 1965.
  - Predicted that the number of transistors on a chip will double every 18-24 months.




- The Wall!
  - Transistors are to become of size $10^8$ cm.
  - Most companies believe this will happen in the next 20 years.




## Postulates of Quantum Mechanics

Postulate 1: A closed quantum system is described by a unit vector in a complex inner product space known as state space.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation.

$$|y(t)\rangle = U\,|y(0)\rangle = \exp(-iHt)\,|y(0)\rangle$$

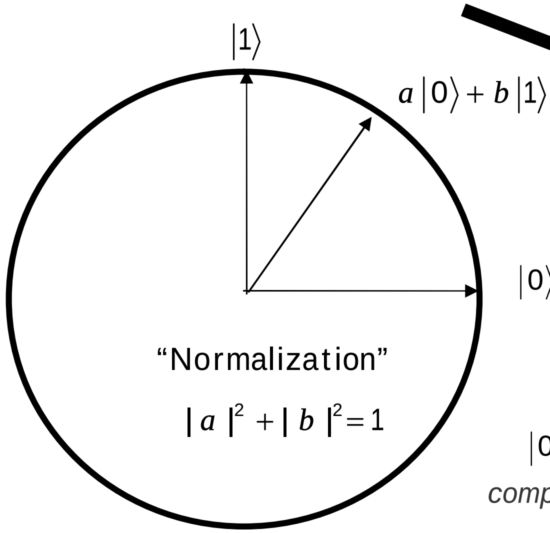
Postulate 3: If we measure $|y\rangle$ in an orthonormal basis $|e_1\rangle, \ldots, |e_d\rangle$, then we obtain the result $j$ with probability

$$P(j) = \left|\langle e_j | y\rangle\right|^2.$$

The measurement disturbs the system, leaving it in a state $|e_j\rangle$ determined by the outcome.

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component systems.

## Example: qubits (two-level quantum systems)




photons
electron spin
nuclear spin
etcetera

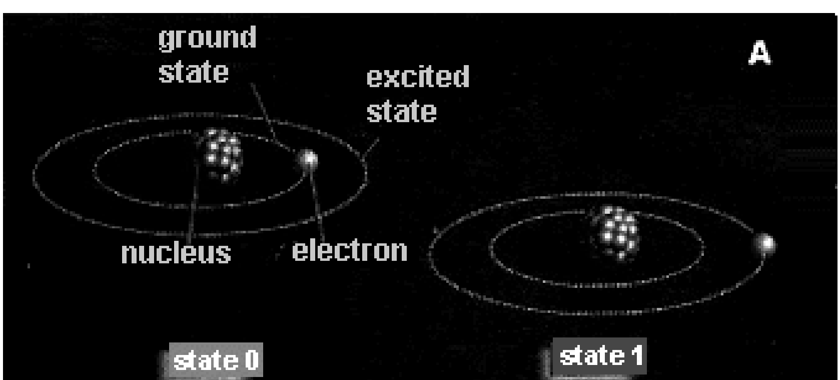
"Normalization"

$$|a|^2 + |b|^2 = 1$$

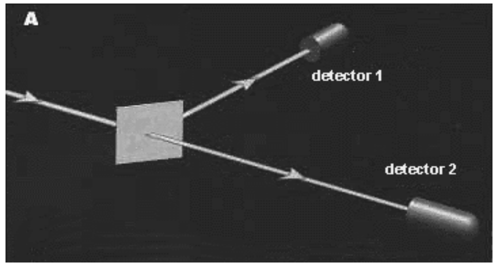
$|0\rangle$ and $|1\rangle$ are the *computational basis states*

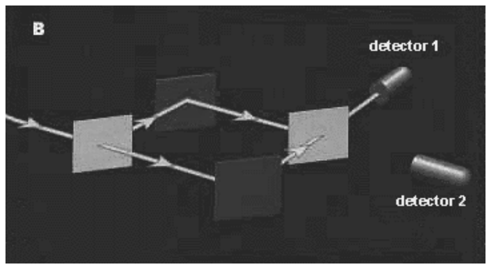
"All we do is draw little arrows on a piece of paper - that's all."
- Richard Feynman

## Qubits: a quantum not-gate

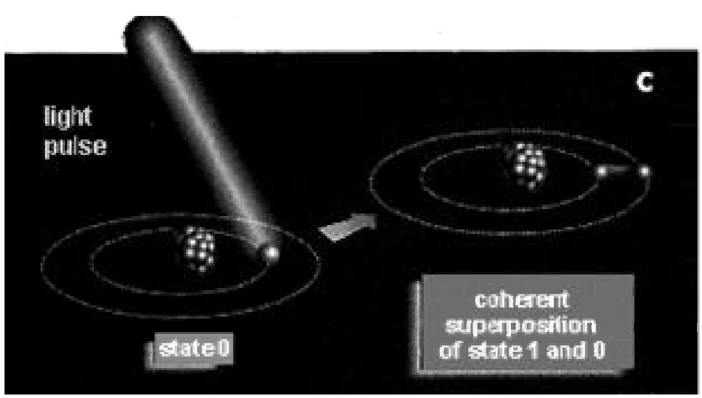


## Quantum superposition




## Coherent superposition



## Circuit model of computation

### Classical

Unit: bit

1. Preparation of *n*-bit input
2. 1- and 2-bit gates
3. Readout of output bits.

### Quantum

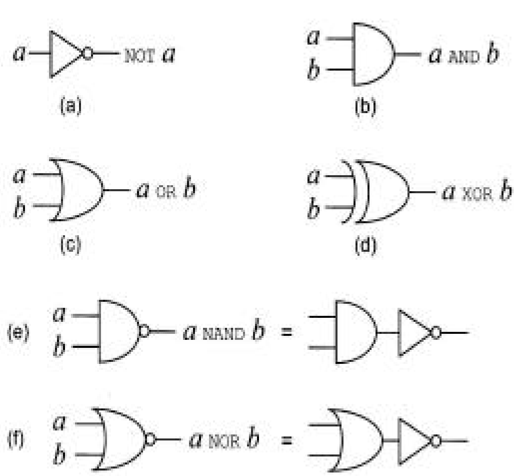
$|x_1, x_2, \ldots, x_n\rangle$

Unit: qubit

1. Preparation of *n*-qubit input in the given basis.
2. Unitary 1- ? 2-qubit gates
3. Detection of partial information on qubit state by their measurement.

???? ??? ?????????? ???????????? ?????? ?????

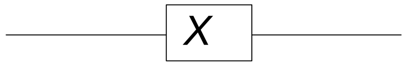
## Classical logical gates




| A | B | AND | OR | XOR | NOT B |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 0 |

## Dynamics: quantum logic gates

Quantum not gate:

Input qubit  Output qubit


$$X\,|0\rangle = |1\rangle; \quad X\,|1\rangle = |0\rangle.$$

$$a\,|0\rangle + b\,|1\rangle \rightarrow ?$$

$$a\,|0\rangle + b\,|1\rangle \rightarrow a\,|1\rangle + b\,|0\rangle$$

Matrix representation: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

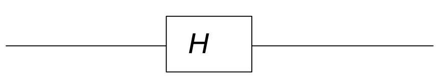
General dynamics of a closed quantum system (including logic gates) can be represented as a unitary matrix.

## Single-qubit quantum logic gates

Pauli gates

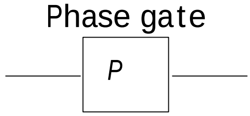
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

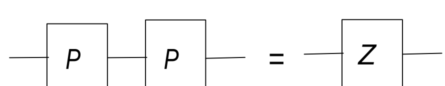
Hadamard gate




$$H\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; \quad H\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}; \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Phase gate

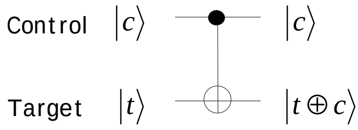


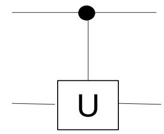

$$P\,|0\rangle = |0\rangle; \quad P\,|1\rangle = i\,|1\rangle \quad P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$P^2 = Z$$

## Controlled-not gate

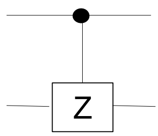



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



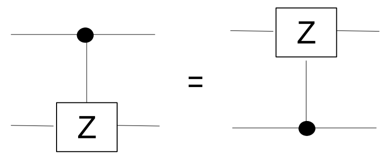

CNOT is the case when U=X

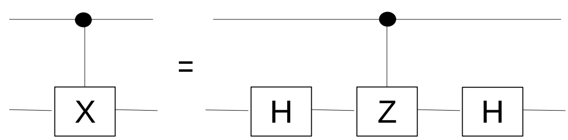
## Controlled-phase gate



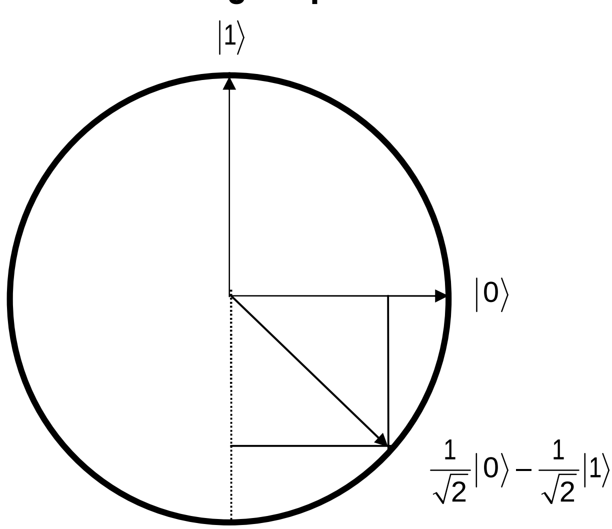

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$|c,t\rangle \rightarrow (-1)^{ct}\,|c,t\rangle$$




## **Measuring a qubit**




$$P(0) = P(1) = \frac{1}{2}$$

## Postulate 4

The state space of a composite physical system is the tensor product of the state spaces of the component systems.

**Example:** Two-qubit state space is $C^2 \otimes C^2 = C^4$

Computational basis states: $|0\rangle \otimes |0\rangle$; $|0\rangle \otimes |1\rangle$; $|1\rangle \otimes |0\rangle$; $|1\rangle \otimes |1\rangle$

Alternative notations: $|0\rangle|0\rangle$; $|0,0\rangle$; $|00\rangle$.

## Multiple-qubit systems

$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$

Measurement in the computational basis: $P(x,y) = |a_{xy}|^2$

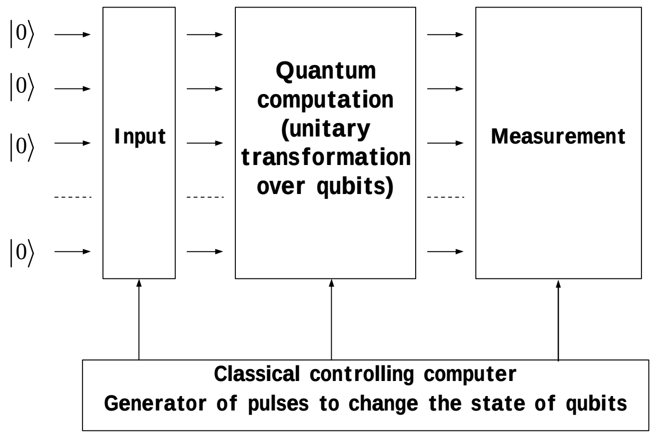
General state of $n$ qubits: $\sum_{x \in \{0,1\}^n} a_x |x\rangle$

Classically, requires $O(2^n)$ bits to describe the state.

**"Hilbert space is a big place" - Carlton Caves**

"Perhaps [...] we need a mathematical theory of quantum automata. [...] the quantum state space has far greater capacity than the classical one: [...] in the quantum case we get the exponential growth [...] the quantum behavior of the system might be much more complex than its classical simulation." – Yu Manin (1980)

# Structure of a quantum computer




# Advantage of quantum computers: cryptography

- Current encryption methods work by factoring numbers.
  - Ex. 12=2*2*3.
  - Very easy to do for small numbers.
- Current encryption numbers use over 400 digits in size.
  - Today's computers would take about a billion years to factor these numbers.
  - A quantum computer with a similar performance as modern computers would need seconds (Shor's algorithm).

## Example: RSA-129 problem

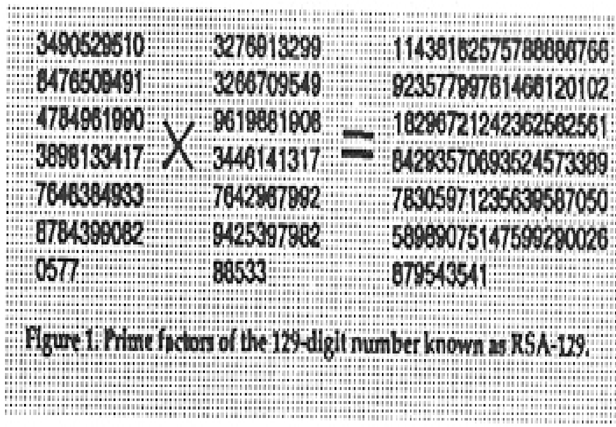
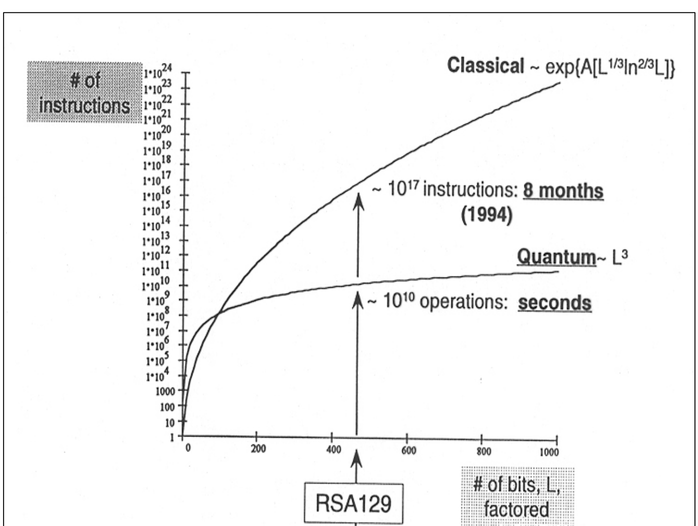



Figure 1. Prime factors of the 129-digit number known as RSA-129.

## Comparison of classical and quantum computers for RSA-129



## **Advantage of quantum computers:** search

Quantum computer would be able to locate a desired item in a very short amount of time in an unsorted data base.

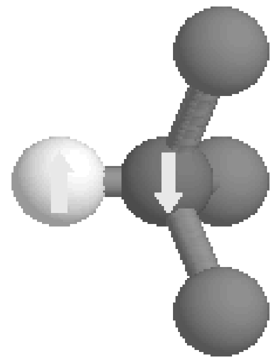
- Normal computers search algorithms have to search an N size database N/2 tries on average before they find a specific piece of data.
- Quantum computer search algorithms have to search an N size database N^(1/2) tries on average to find specific data (Grover's algorithm).

## Quantum Computer Designs

- NMR (Nuclear Magnetic Resonance)
- Ion Trap
- Quantum Dots

## NMR

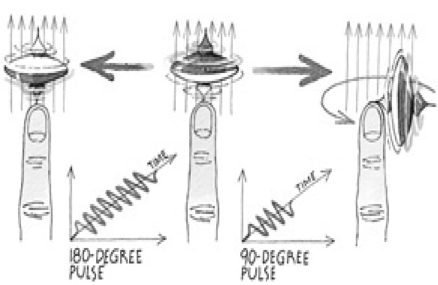
- Developed at IBM by Issac Chaung.
- NMR was thought of in 1996
- Protons and Neutrons have spin.
  - In a normal atoms these spins cancel out.
  - In isotopes there are extra neutrons.
  - These extra neutrons create a net positive or negative spin in an atom.



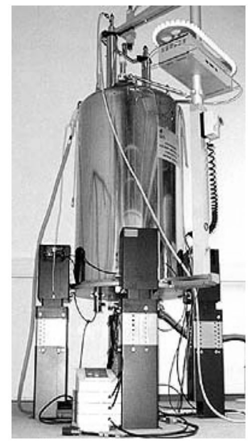
## NMR

- How to implement a logic operation.
- Lining up all the spins
  - A molecule is suspended in a solvent
  - The solvent is then put into a spectrometer's main magnetic field.
  - This magnetic field aligns all the spins.
- Radio frequency pulse.
  - One of the atoms' spins will flip or not flip depending on the spin of the other atoms.
- Multiple pulse sequences.
  - A quantum algorithm.

## NMR




Example of radio frequencies interacting with spin.



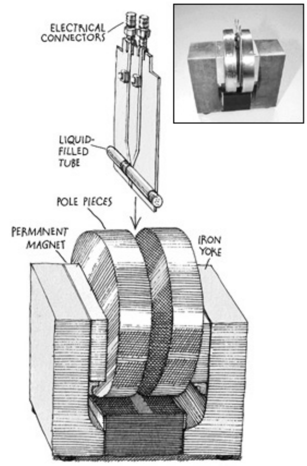
Modern NMR computer

## NMR (Pro's & Con's)

- <u>Pro's</u>
  - Nucleus is naturally protected from outside interference.
    - **Once the spins are lined up they will stay in the proper order for a long time.**
  - Nuclear qubits already exist in nature.
  - Technology for manipulating these qubits already exists.
    - **Hospital magnetic resonance imaging.**
- <u>Con's</u>
  - Very large in size.
    - **Many are 10 feet tall.**

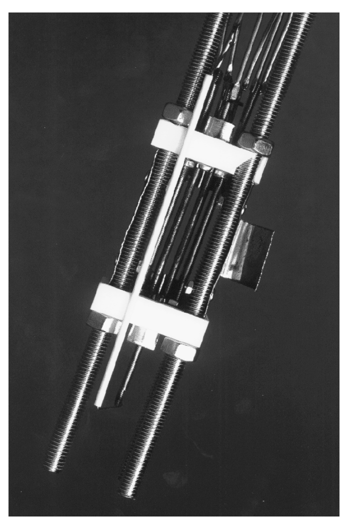
## NMR
## (In The Works)

- Currently NMR machines 3 and 7 qubit machines.
- Development by IBM to create a 10 qubit machine is in the works.
- There is also development of small, room temperature NMR machines for more practical uses.



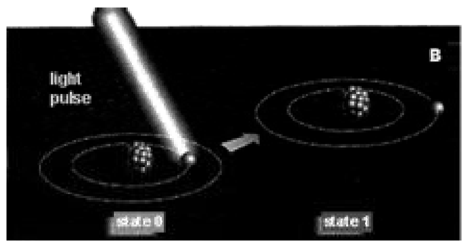

## Ion Traps

- Ions in a radio frequency trap interact by exchanging vibrational excitations. Each ion can be controlled by a polarized, properly focused laser beam.
- Picture shows the electrode structure.
- The electrode is 1mm thick.



## Quantum Dots

- An electron trapped in a group of atoms is hit with a laser beam at the right frequency. This causes the electron to move into a higher state. The higher state can be a one, the lower state a zero.
- The laser light can be thought of as controlled not-gates.




## Current Challenges

- Number of bits in a word.
  - 7-qubit machines is the most advanced to date.
  - Difficulty with large words is too much quantum interaction can produce undesired results. All the atoms interact with each other.
- Physical size of the machines.
  - Current machines are too large to be of practical use to everyday society.
- Error correction.
  - Many advance have been made but this is still an area of intense research.

## Some conventions implicit in Postulate 4

Alice

Bob

If Alice prepares her system in state $|a\rangle$, and Bob prepares his in state $|b\rangle$, then the joint state is $|a\rangle\otimes|b\rangle$.

Conversely, if the joint state is $|a\rangle\otimes|b\rangle$ then we say that Alice's system is in the state $|a\rangle$, and Bob's system is in the state $|b\rangle$.

$$|a\rangle\otimes|b\rangle=\left(e^{iq}|a\rangle\right)\otimes\left(e^{-iq}|b\rangle\right)$$

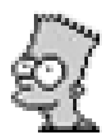
"Alice applies the gate $U$ to her system" means that $(U\otimes I)$ is applied to the joint system.

$$(A\otimes B)|v\rangle\otimes|w\rangle = A|v\rangle\otimes B|w\rangle$$

## Quantum entanglement

Alice

Bob



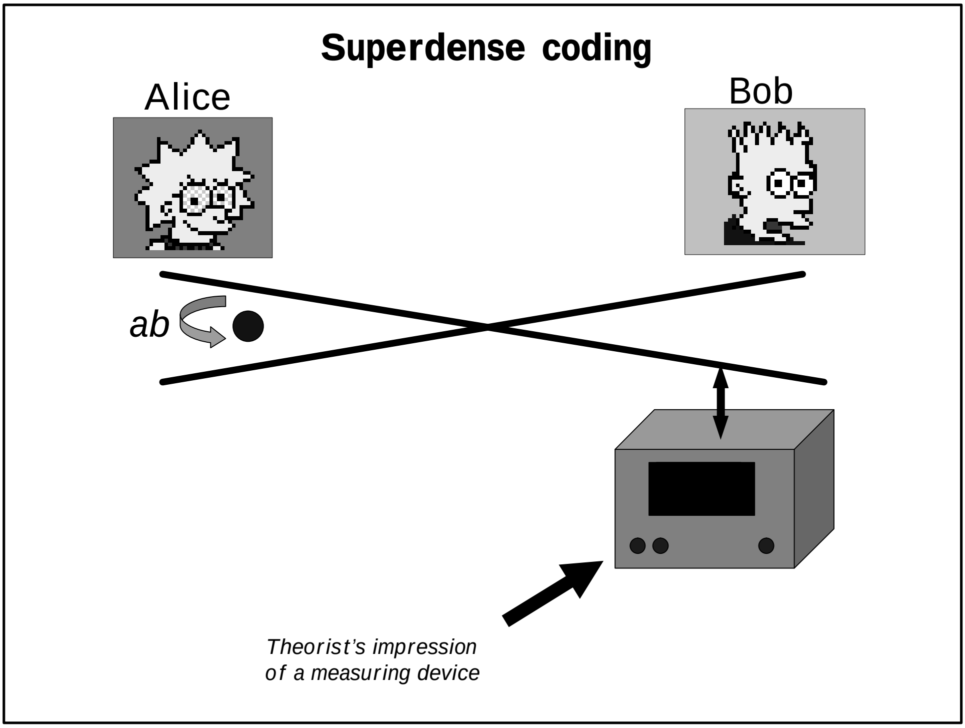
$$|y\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

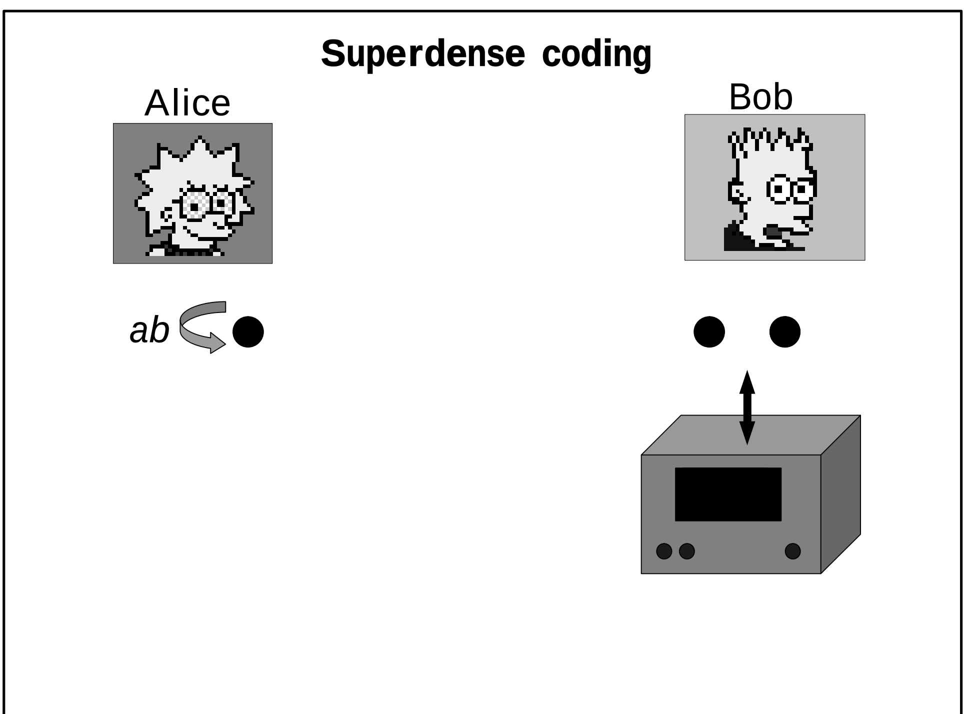
$$|y\rangle \neq |a\rangle|b\rangle \qquad |y\rangle = \left(a|0\rangle + b|1\rangle\right)\left(g|0\rangle + d|1\rangle\right)$$

$$= ag|00\rangle + bg|10\rangle + ad|01\rangle + bd|11\rangle$$

$$\rightarrow b = 0 \text{ or } g = 0.$$

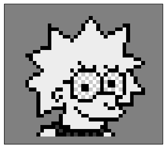
Schroedinger (1935): "I would not call [entanglement] *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."


Superdense coding
Alice
Bob
ab
Theorist's impression
of a measuring device


Superdense coding
Alice
Bob
ab

## Superdense coding

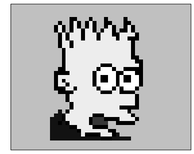
Alice



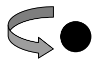
$X|0\rangle = |1\rangle; \quad X|1\rangle = |0\rangle$

$Z|0\rangle = |0\rangle; \quad Z|1\rangle = -|1\rangle$

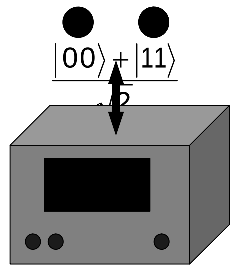
Bob



$ab$



$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



$00$ : Apply $I$ $\quad \frac{|00\rangle + |11\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

$01$ : Apply $Z$ $\quad \frac{|00\rangle + |11\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

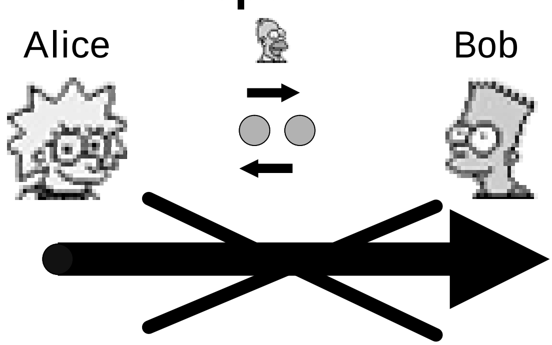
$10$ : Apply $X$ $\quad \frac{|00\rangle + |11\rangle}{\sqrt{2}} \rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}}$

$11$ : Apply $XZ$ $\quad \frac{|00\rangle + |11\rangle}{\sqrt{2}} \rightarrow \frac{|10\rangle - |01\rangle}{\sqrt{2}}$

## Teleportation

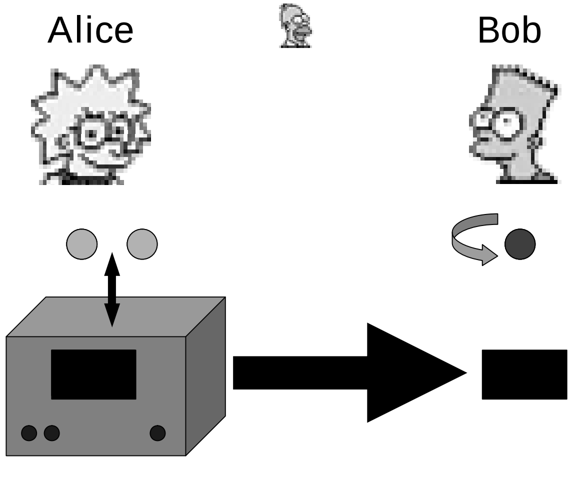
Alice

Bob



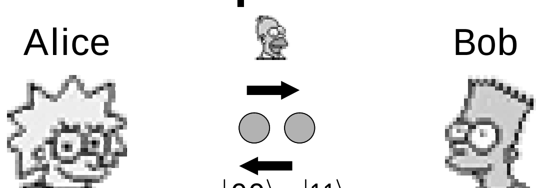
# Teleportation

Alice Bob



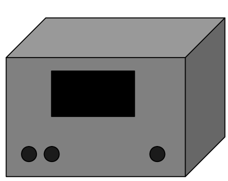
# Teleportation

Alice Bob



$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$a\,|0\rangle + b\,|1\rangle$ 



$$\left(a\,|0\rangle + b\,|1\rangle\right)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

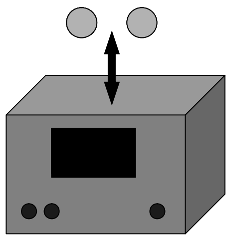
$$= \frac{a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle}{\sqrt{2}}$$

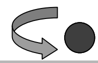
$$|00\rangle = \frac{1}{\sqrt{2}}\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}\left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right) \qquad |10\rangle = \frac{1}{\sqrt{2}}\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) - \frac{1}{\sqrt{2}}\left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right)$$

$$|01\rangle = \frac{1}{\sqrt{2}}\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}\left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right) \qquad |11\rangle = \frac{1}{\sqrt{2}}\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) - \frac{1}{\sqrt{2}}\left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right)$$

# Teleportation

Alice  Bob





$$= \frac{1}{2}\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\boxed{(a\,|0\rangle+b\,|1\rangle)} \xrightarrow{I} (a\,|0\rangle+b\,|1\rangle)$$

$$+\frac{1}{2}\left(\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right)\boxed{(a\,|0\rangle-b\,|1\rangle)} \xrightarrow{z} (a\,|0\rangle+b\,|1\rangle)$$

$$+\frac{1}{2}\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)\boxed{(a\,|1\rangle+b\,|0\rangle)} \xrightarrow{x} (a\,|0\rangle+b\,|1\rangle)$$

$$+\frac{1}{2}\left(\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right)\boxed{(a\,|1\rangle-b\,|0\rangle)} \xrightarrow{zx} (a\,|0\rangle+b\,|1\rangle)$$

# The fundamental question of information science

1. Given a physical resource – energy, time, bits, space, entanglement; and
2. Given an information processing task – data compression, information transmission, teleportation; and
3. Given a criterion for success;

**We ask the question:**
**How much of 1 do I need to achieve 2, while satisfying 3?**

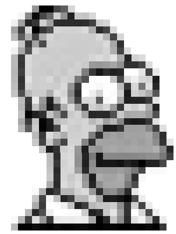
Pursuing this question in the quantum case has led to, and presumably will continue to lead to, interesting new information processing capabilities.

Are there any fundamental scientific questions that can be addressed by this program?

## What fundamental problems are addressed by quantum information science?

**You**

**Your challenger**



Knowing the rules ≠ Understanding the game

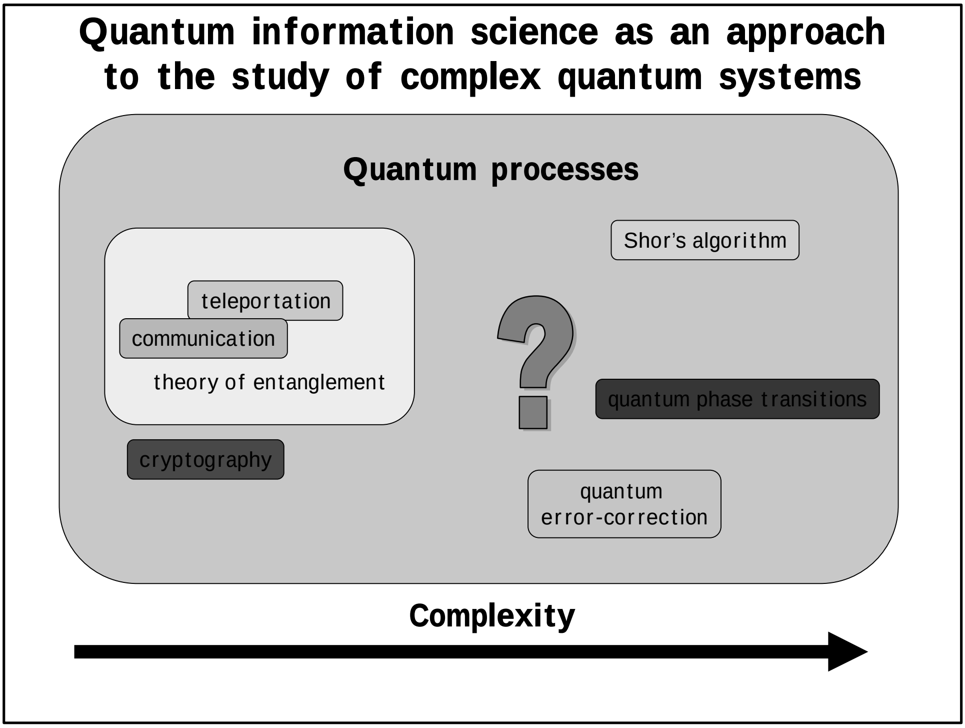
---

Knowing the rules of quantum mechanics

≠

Understanding quantum mechanics

**What high-level principles are implied by quantum mechanics?**


Quantum information science as an approach to the study of complex quantum systems
Quantum processes
Shor's algorithm
teleportation
communication
theory of entanglement
quantum phase transitions
cryptography
quantum error-correction
Complexity