A Quantum Science

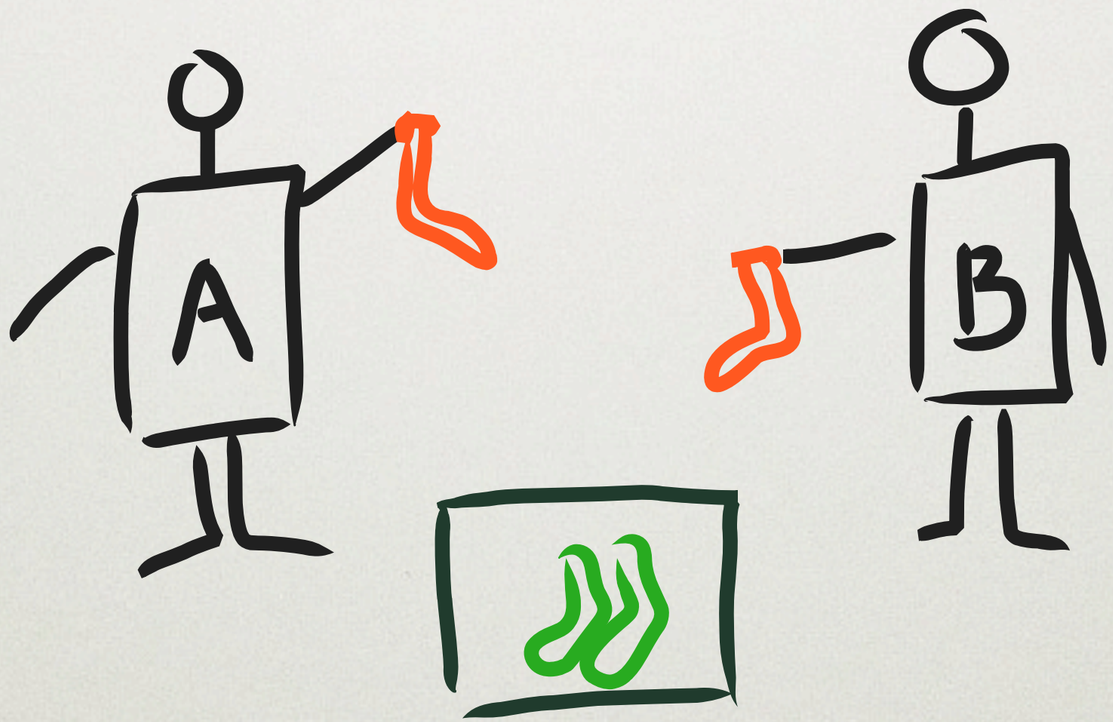
How Quantum Information differs from classical

Robert Helling (@atdotde) at 28c3
Theoretical and Mathematical Physics, LMU München

Plan for today

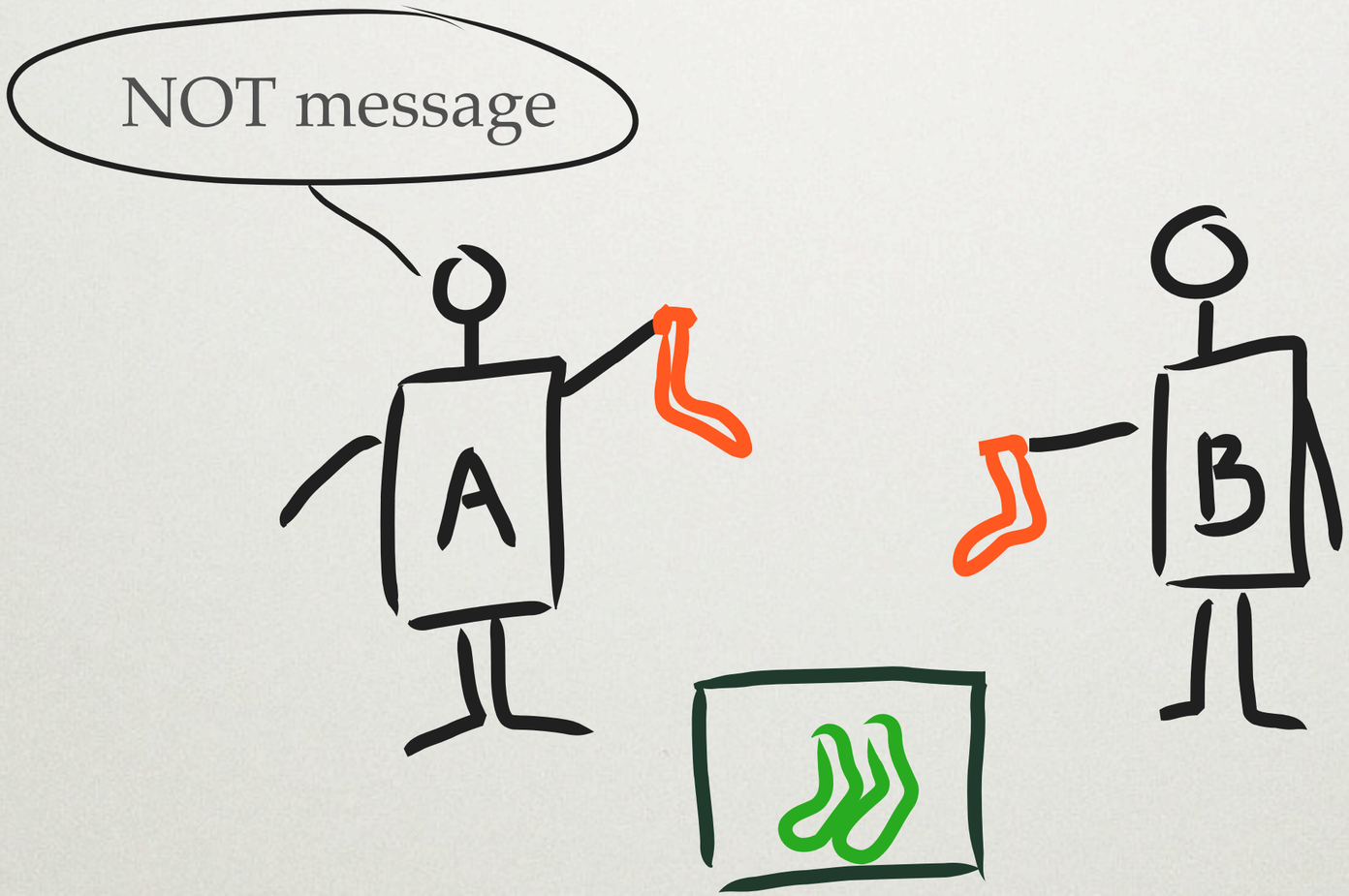
- Classical crypto
- Entanglement experiment
- Quantum mechanics: the formalism
- Quantum crypto
- Is the brain a quantum computer?

Classical Crypto

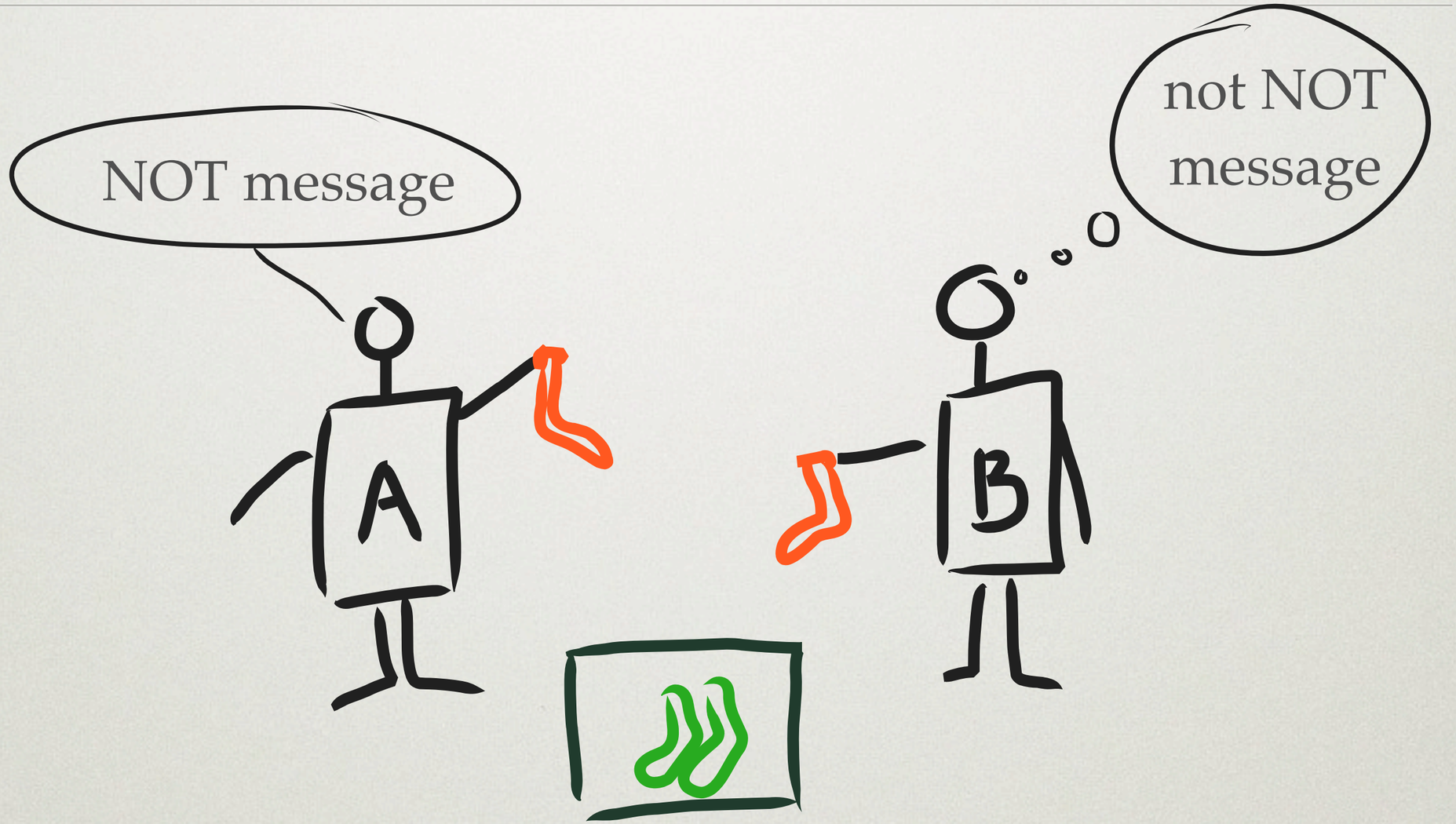


One time pad

Classical Crypto

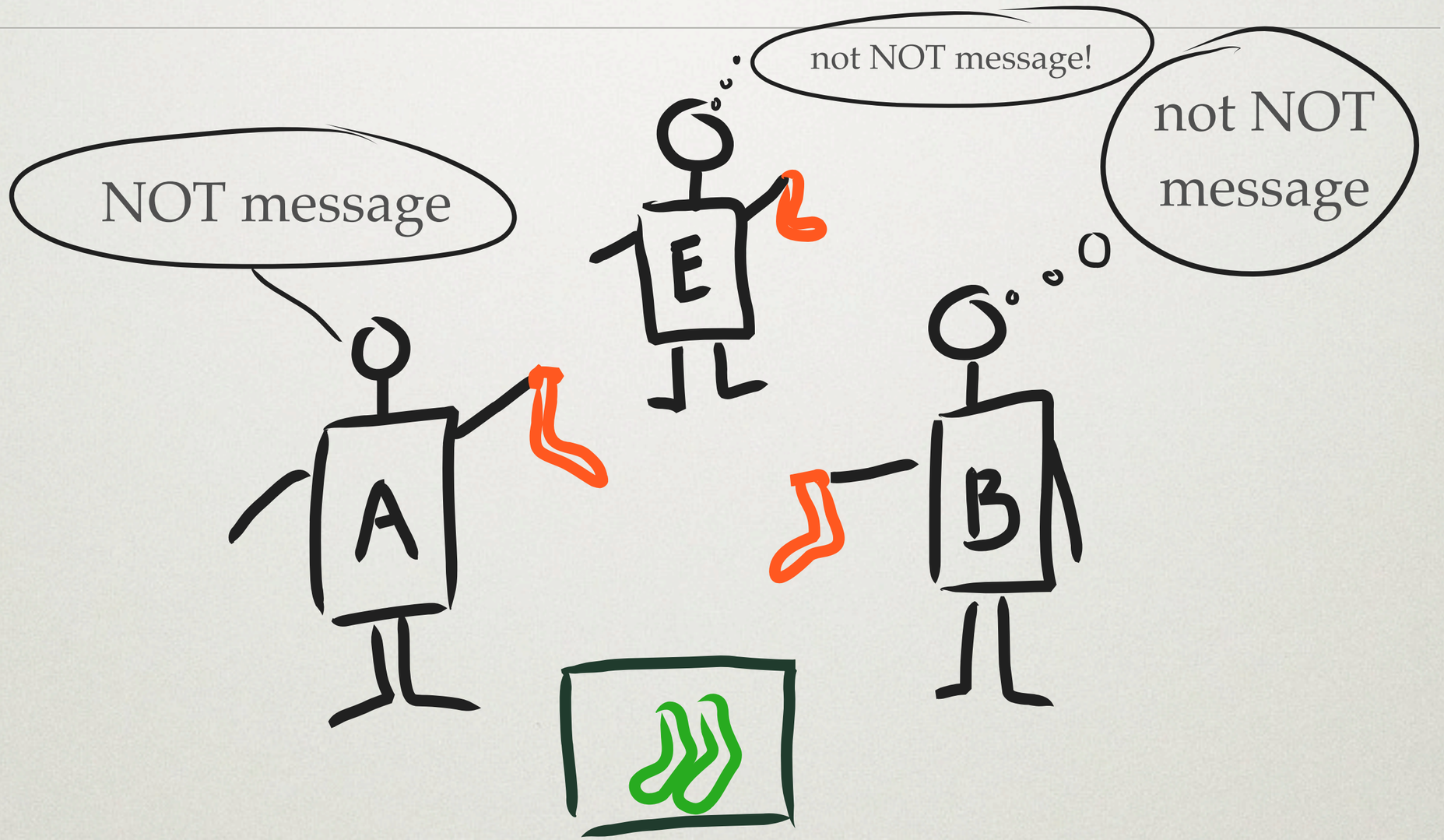


Classical Crypto



One time pad

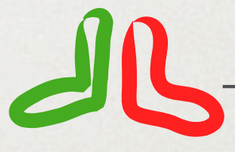
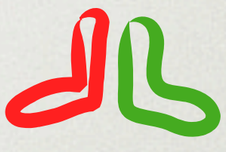
Classical Crypto



One time pad

Classical states

Alice and Bob used socks in the correlated random state

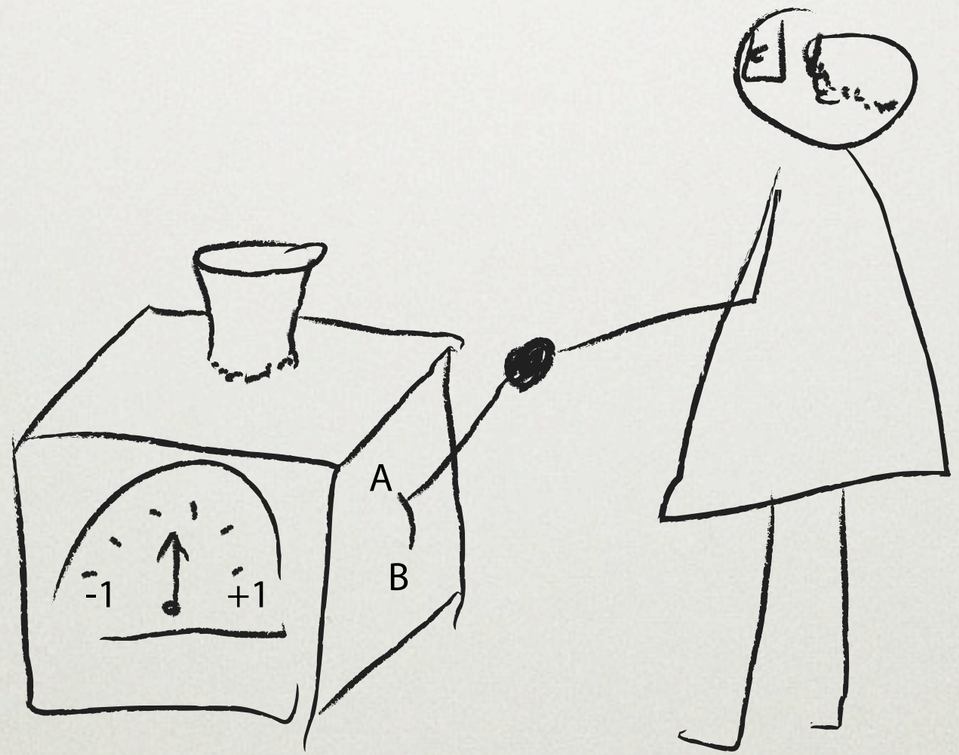
S = 50%  +50%  +0%  +0% 

This state has to be prepared by a trusted entity.

Further assumption:
Public communication is reliable
(example: ad in newspaper)

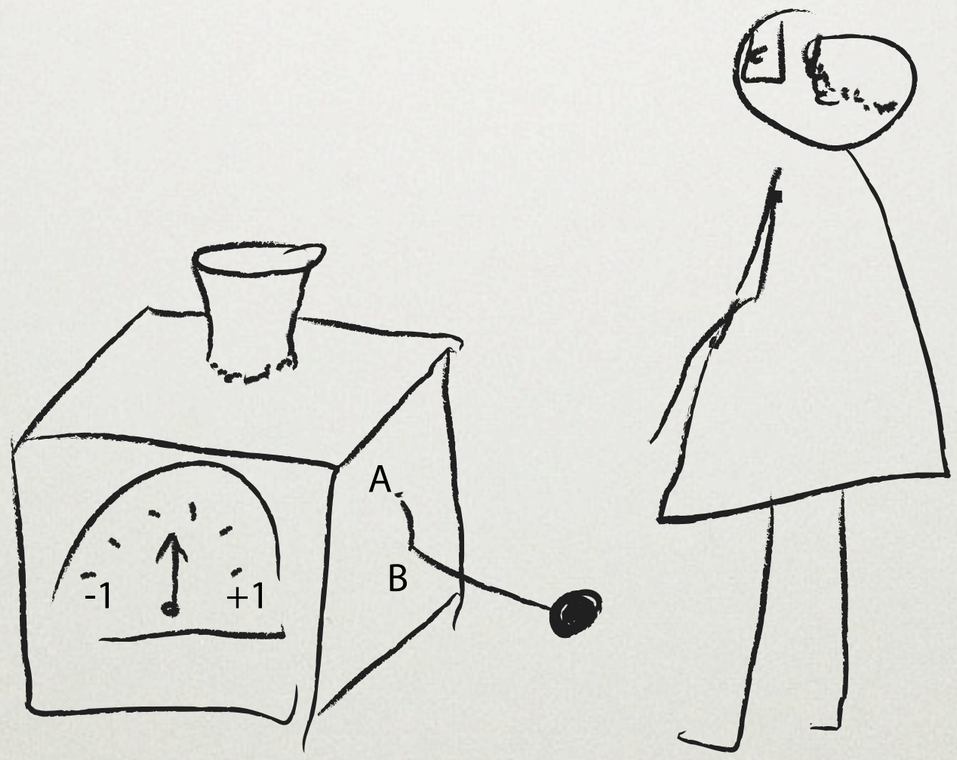
A quantum experiment

Quantum physics not only allows for correlations but for "entanglement".



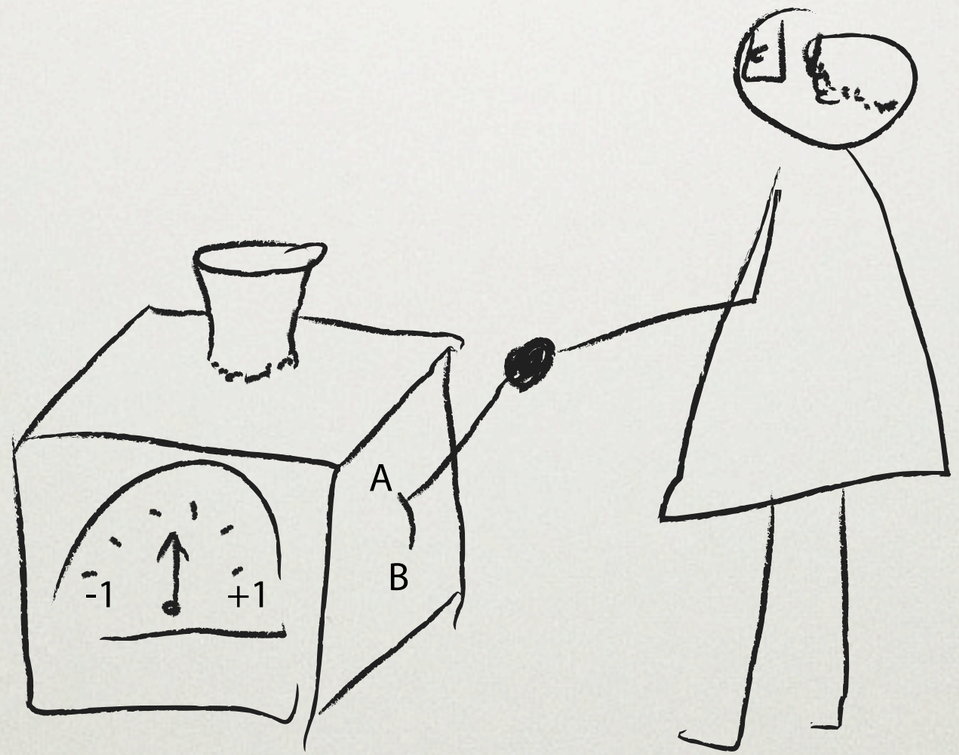
A quantum experiment

Quantum physics not only allows for correlations but for "entanglement".



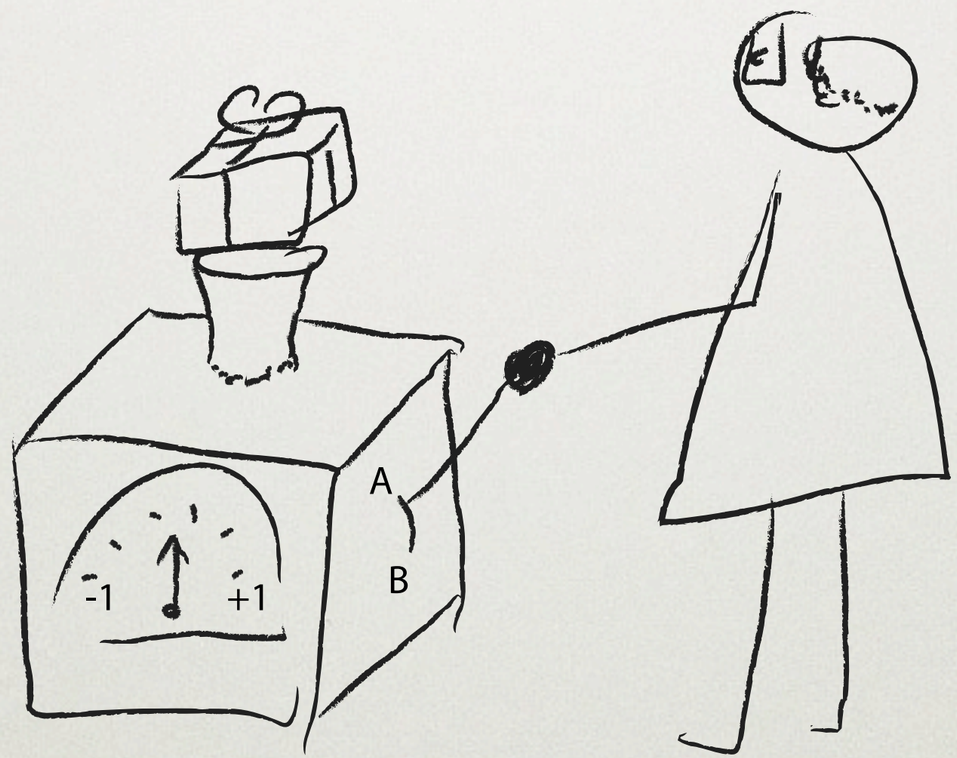
A quantum experiment

Quantum physics not only allows for correlations but for "entanglement".



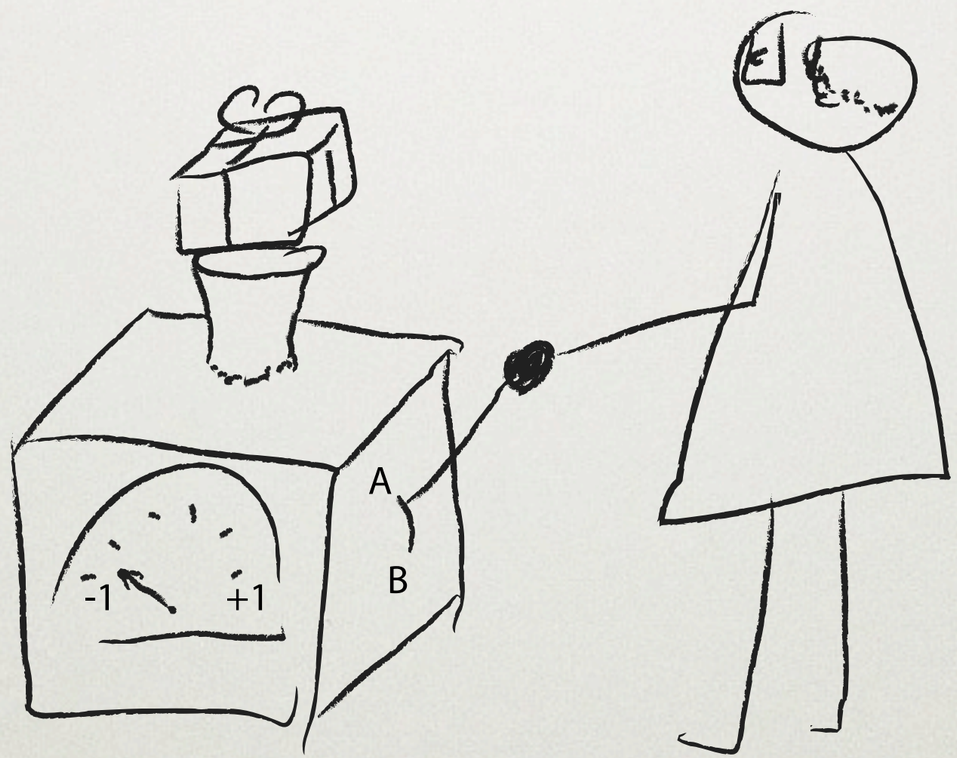
A quantum experiment

Quantum physics not only allows for correlations but for "entanglement".



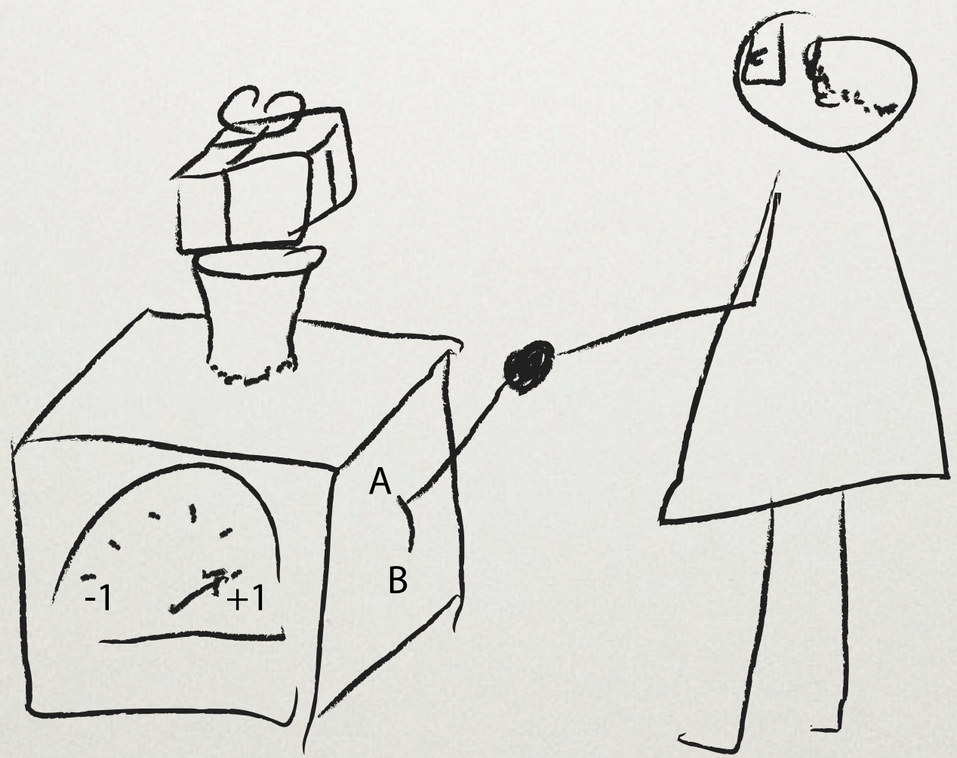
A quantum experiment

Quantum physics not only allows for correlations but for "entanglement".



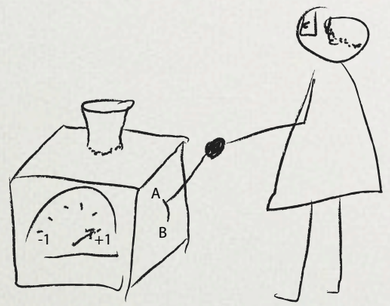
A quantum experiment

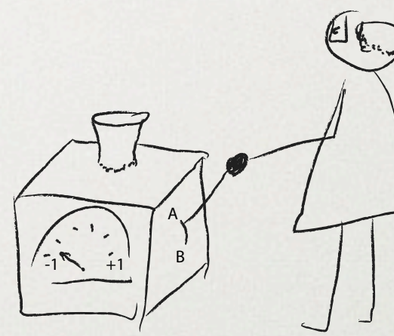
Quantum physics not only allows for correlations but for "entanglement".

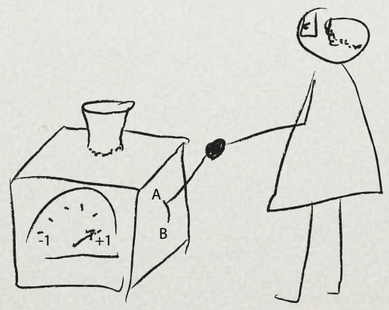


A quantum experiment

Quantum physics not only allows for correlations but for "entanglement".

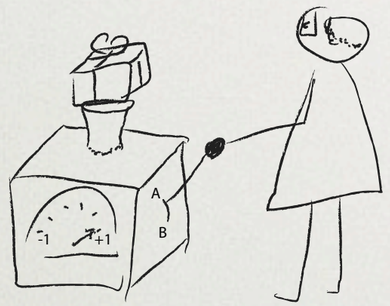


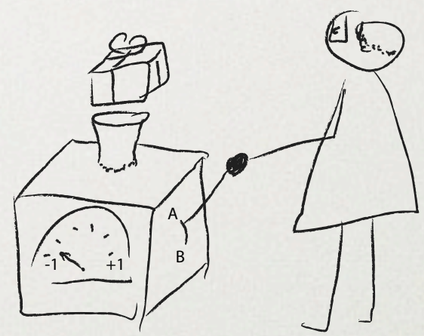


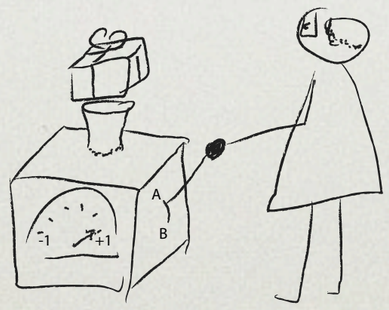


A quantum experiment

Quantum physics not only allows for correlations but for "entanglement".







Lab Log

A_1 A_2 A_3	A_1 A_2 B_3	A_1 B_2 A_3	A_1 B_2 B_3	B_1 A_2 A_3	B_1 A_2 B_3	B_1 B_2 A_3	B_1 B_2 B_3
+ − +	− + +	+ + +	− − +	− − −	− + −	− − +	+ + +
+ − +	− + +	+ − −	+ + +	− + +	− + −	− − +	− − +
− − −	− + +	− − −	+ + +	− − +	+ + +	− − +	− − +
+ + −	+ − +	− − +	+ + +	+ − −	− − +	+ − −	− + −
+ − +	− − −	+ − −	− + −	+ + +	+ − −	− − +	+ − +
+ − +	− + −	− − +	− + −	+ + +	+ + +	− + −	− − −
− − −	+ + −	− − +	+ + +	− + +	+ + +	− + −	+ + −
+ + −	+ + −	− − +	− + −	− + −	− − +	− − +	− + −
+ − +	+ − +	− − −	+ − −	− − −	+ + +	− + −	− − −
− − −	+ − +	+ + −	+ + +	+ − +	− + −	− + −	+ − −
− − −	+ − +	+ + +	+ + +	− + +	+ + +	− + −	− + +
+ + −	− − −	− + +	+ − −	− + +	− + −	+ + +	+ − +
+ + −	− + +	+ − +	− − +	− + −	+ − −	+ + +	+ + −
− + +	− + +	+ − +	+ + +	+ + +	+ + +	+ + +	− + −
− + +	− + +	+ + −	− + −	− + +	+ + +	− − +	− − +
+ − +	− − −	− − −	− + −	+ − −	+ + +	+ − −	− + −
+ + −	+ − +	− + −	+ + +	− + −	+ + +	+ + +	+ − −
− + +	− − −	+ + −	+ − −	− − +	− + −	− + −	− + −

Lab Log

A_1 A_2 A_3	A_1 A_2 B_3	A_1 B_2 A_3	A_1 B_2 B_3	B_1 A_2 A_3	B_1 A_2 B_3	B_1 B_2 A_3	B_1 B_2 B_3
+ − +	− + +	+ + +	− − +	− − −	− + −	− − +	+ + +
+ − +	− + +	+ − −	+ + +	− + +	− + −	− − +	− − +
− − −	− + +	− − −	+ + +	− − +	+ + +	− − +	− − +
+ + −	+ − +	− − +	+ + +	+ − −	− − +	+ − −	− + −
+ − +	− − −	+ − −	− + −	+ + +	+ − −	− − +	+ − +
+ + −	+ + −	− − +	− + −	+ + +	+ + +	− + −	− − −
+ − +	+ + −	− − +	+ + +	− + +	+ + +	− + −	+ + −
+ − +	+ + −	− − +	+ + +	− + −	− − +	− − +	− + −
− − −	+ + −	− − −	+ + +	− − −	− + −	+ − −	+ − −
+ + −	+ + −	− + −	− + −	+ + −	− + −	+ + +	− + −
+ − +	+ − +	− − −	+ − −	− − −	+ + +	− + −	− − −
− − −	+ − +	+ + −	+ + +	+ − +	− + −	− + −	+ − −
− − −	+ − +	+ + +	+ + +	− + +	+ + +	− + −	− + +
+ + −	− − −	− + +	+ − −	− + +	− + −	+ + +	+ − +
+ + −	− + +	+ − +	− − +	− + −	+ − −	+ + +	+ + −
− + +	− + +	+ − +	+ + +	+ + +	+ + +	+ + +	− + −
− + +	− + +	+ + −	− + −	− + +	+ + +	− − +	− − +
+ − +	− − −	− − −	− + −	+ − −	+ + +	+ − −	− + −
+ + −	+ − +	− + −	+ + +	− + −	+ + +	+ + +	+ − −
− + +	− − −	+ + −	+ − −	− − +	− + −	− + −	− + −

odd number of -'s

even number of -'s

Lab Log

A_1 A_2 A_3	A_1 A_2 B_3	A_1 B_2 A_3	A_1 B_2 B_3	B_1 A_2 A_3	B_1 A_2 B_3	B_1 B_2 A_3	B_1 B_2 B_3
+ − +	− + +	+ + +	− − +	− − −	− + −	− − +	+ + +
+ − +	− + +	+ − −	+ + +	− + +	− + −	− − +	− − +
− − −	− + +	− − −	+ + +	− − +	+ + +	− − +	− − +
+ + −	+ − +	− − +	+ + +	+ − −	− − +	+ − −	− + −
+ − +	− − −	+ − −	− + −	+ + +	+ − −	− − +	+ − +
+ − +	− − −	+ − −	− + −	+ + +	+ − −	− − +	+ − +
+ + −	+ + −	− − +	− + −	+ + +	+ + +	− + −	− − −
+ − +	+ + −	− − +	+ + +	− + +	− + −	− + −	− − −
+ − +	+ + −	− − +	+ + +	− + −	− + −	+ − −	+ − −
− − −	+ − +	− − −	+ + +	− − −	− + −	+ + +	− + −
+ + −	+ − +	− − −	− + −	+ + +	− + −	− − −	− − −
+ − +	+ − +	+ + +	+ + +	− + −	− + −	− + −	− − +
− − −	+ − +	+ + −	+ + +	+ − +	− + −	− + −	+ − −
− − −	+ − +	+ + +	+ + +	− + +	+ + +	− + −	− − +
+ + −	− − −	− + +	+ − −	− + +	− + −	+ + +	+ − +
+ + −	− + +	+ − +	− − +	− + −	+ − −	+ + +	+ + −
− + +	− + +	+ − +	+ + +	+ + +	+ + +	+ + +	− + −
− + +	− + +	+ + −	− + −	− + +	+ + +	− − +	− − +
+ − +	− − −	− − −	− + −	+ − −	+ + +	+ − −	− + −
+ + −	+ − +	− + −	+ + +	− + −	+ + +	+ + +	+ − −
− + +	− − −	− + −	− − −	− − +	− + −	− + −	− + −

The impossible experiment

odd number of -'s $\Leftrightarrow$ $A_1 \cdot A_2 \cdot A_3 = -1$

even number of -'s $\Leftrightarrow$ $A_1 \cdot B_2 \cdot B_3 = +1$

$B_1 \cdot A_2 \cdot B_3 = +1$

$B_1 \cdot B_2 \cdot A_3 = +1$

The impossible experiment

odd number of -'s $\Leftrightarrow$ $A_1 \cdot A_2 \cdot A_3 = -1$

even number of -'s $\Leftrightarrow$ $A_1 = B_2 \cdot B_3$

$A_2 = B_1 \cdot B_3$

$A_3 = B_1 \cdot B_2$

The impossible experiment

odd number of -'s $\Leftrightarrow$ $A_1 \cdot A_2 \cdot A_3 = -1$

even number of -'s $\Leftrightarrow$ $A_1 = B_2 \cdot B_3$

$A_2 = B_1 \cdot B_3$

$A_3 = B_1 \cdot B_2$

$$A_1 \cdot A_2 \cdot A_3 = (B_1 \cdot B_2 \cdot B_3)^2 = +1$$

The impossible experiment

odd number of -'s $\Leftrightarrow$ $A_1 \cdot A_2 \cdot A_3 = -1$

even number of -'s $\Leftrightarrow$ $A_1 = B_2 \cdot B_3$

$A_2 = B_1 \cdot B_3$

$A_3 = B_1 \cdot B_2$

$A_1 \cdot A_2 \cdot A_3 = (B_1 \cdot B_2 \cdot B_3)^2 = +1$

This cannot happen for a local, realistic measurement!
Quantum physics for the rescue

Quantum States

- States are represented by vectors

- "Qubit" $\psi = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ with $|v_1|^2 + |v_2|^2 = 1$

- For example $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \uparrow$ $\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \rightarrow$

Think of polarized light

Quantum Observables

Observable: Possible measurement of an aspect of a system, represented by an "operator" (a matrix)

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \text{ with } m_{12} = m_{21}^*$$

We will need these three examples:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Measurements

What is the result of a measurement of M in state ψ?

That's difficult

But it is simple if ψ happens to be an eigenvector of M. That is there is a real number λ with

$$M\psi = \lambda\psi$$

i.e.

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} m_{11}v_1 + m_{12}v_2 \\ m_{21}v_1 + m_{22}v_2 \end{pmatrix} = \begin{pmatrix} \lambda v_1 \\ \lambda v_2 \end{pmatrix}$$

In that case, the measurement (always) yields λ.

Eigenvector Example 1

Let's take $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Here, $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \uparrow$ is eigenvector:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ with } \lambda = 1$$

Similar:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ with } \lambda = -1$$

But in general:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} v_1 \\ -v_2 \end{pmatrix}$$

In short:

$$Z \uparrow = \uparrow, \quad Z \rightarrow = - \rightarrow$$

Eigenvector example 2

Next consider $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. It acts as

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} v_2 \\ v_1 \end{pmatrix}$$

Eigenvectors are obviously

$$\nearrow = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \text{ with } \lambda = 1$$

$$\nwarrow = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} \text{ with } \lambda = -1$$

What about states that are not eigenvectors?

For every M, one can always find two eigenvectors

$$M\psi_1 = \lambda_1\psi_1$$

$$M\psi_2 = \lambda_2\psi_2$$

Any given state can then be expressed (uniquely) as a weighted sum $\psi = c_1\psi_1 + c_2\psi_2$

A measurement of M yields the result λ_1 with probability $|c_1|^2$ and the result λ_2 with probablity $|c_2|^2$.

The measurement changes the state to the corresponding eigenvector.

Another example

We saw that in the state $\nearrow$ a measurement of X always yields +1. But what about measuring Z? Since

$$\nearrow = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

So the result is +1 or -1, each with probability 50%.

After this measurement, measuring X yields random results as

$$\uparrow / \rightarrow = \frac{1}{\sqrt{2}} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \pm \frac{1}{\sqrt{2}} \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

X and Z cannot have an exact value at the same time!

N Qubits

You can have more than one qubit. The states look like

$$c_1\psi_1 \otimes \psi_2 \otimes \cdots \otimes \psi_N + c_2\psi'_1 \otimes \psi'_2 \otimes \cdots \otimes \psi'_N + \cdots$$

A joint measurement is described by

$$M_1 \otimes M_2 \otimes \cdots \otimes M_N$$

measuring M_i on the i-th qubit and then multiplying the results.
M_i can of course be the trivial measurement I that always yields 1.

The singlet state

Let us consider the 2 qubit state

$$\psi_2 = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right]$$

Just measuring Z on the first component (*I* on the other) gives +1 and -1 each with 50% probability.

But it is an +1 eigenstate of both $Z \otimes Z$ and $X \otimes X$.

Thus we know that measuring either Z or X on both qubits gives the same result even if Z and X do not have simultaneous values!

Quantum Socks

This observation is key to quantum cryptography:

Alice and Bob can share two qubits in this singlet state and decide later if the Z or the X measurements are their shared secret.

Each one is random but not both can be determined at the same time (contrary to colour and size of socks).

What about Eve?

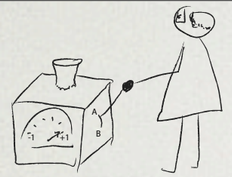
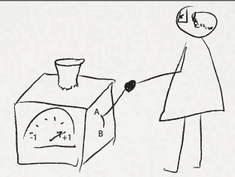
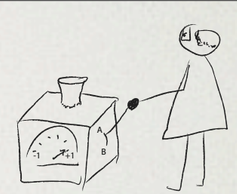
Why can't Eve have her copy of the secret?
She could try to prepare the state

$$\psi_3 = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right]$$

This would still be a +1 eigenstate of $Z \otimes Z \otimes I$ and $Z \otimes I \otimes Z$ and thus give her a copy of the secret if it is the measurement of Z.
But this state fails to be an eigenstate of $X \otimes X \otimes I$ and thus Alice and Bob would not anymore find the same result when measuring X!

The Quantum Crypto Protocol

i) Alice and Bob ask Eve to distribute N copies of the singlet state ψ_2.
ii) They pick a subset of M of the qubits randomly. For each, they determine randomly if they both measure Z or X.
iii) They announce the results publicly. If they all agree they know they really have ψ_2's and not ψ_3's or similar.
iv) They use the remaining (N-M) qubits with simultaneous random Z or X measurements to determine their shared secret.

The Quantum experiment

What the professor distributed were the three quibits of

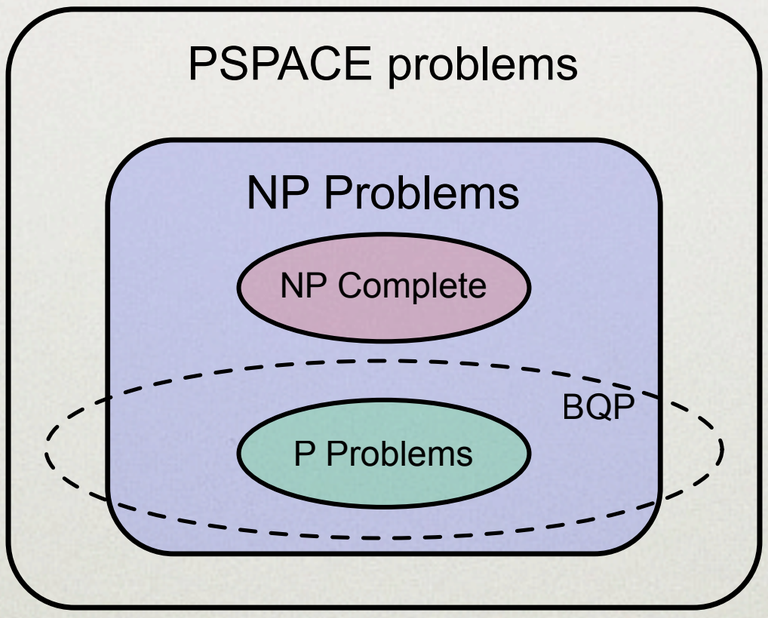
$$\psi_E = \frac{1}{2}\left[\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} + \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \right]$$

This is a -1 eigenstate of $Z \otimes Z \otimes Z$and a +1 eigenstate of $X \otimes X \otimes Z$, $X \otimes Z \otimes X$ and $Z \otimes X \otimes X$ as required.

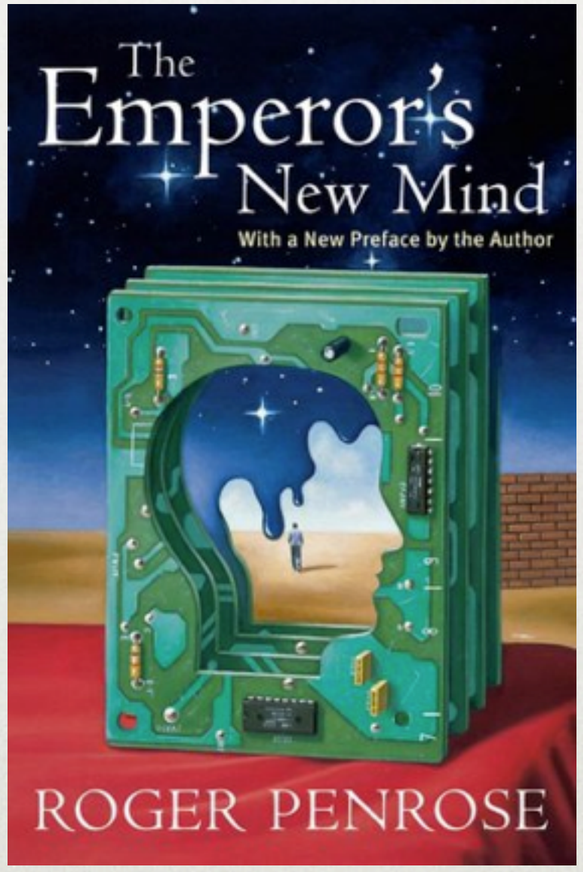
This shows that in the quantum world devices are possible that are impossible classically.

(Nothing on)
Quantum Computing

Grover's algorithm (database search): quadratic speed-up
Shor's algorithm (factorization): exponential speed-up
Simon's algorithm (black box): exponential speed-up



Is the human brain a quantum computer?



Idea: The brain can do much more complex things than any computer.

Is the human brain a quantum computer?

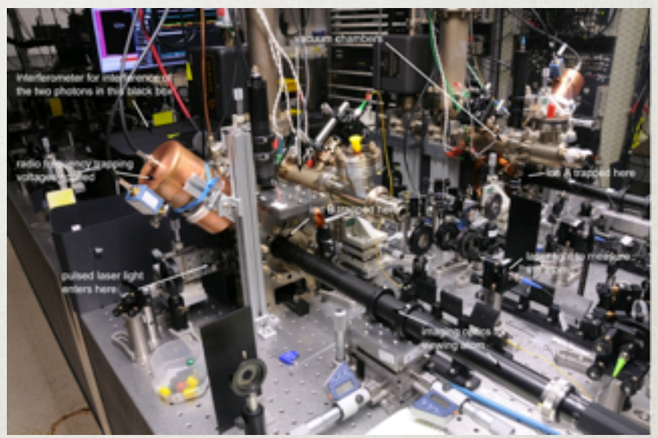
A: Obviously not!

Is the human brain a quantum computer?

A: Obviously not!

It is a brain,
not a computer

vs



Is the human brain a quantum computer?

A: Obviously yes!

Is the human brain a quantum computer?

A: Obviously yes!

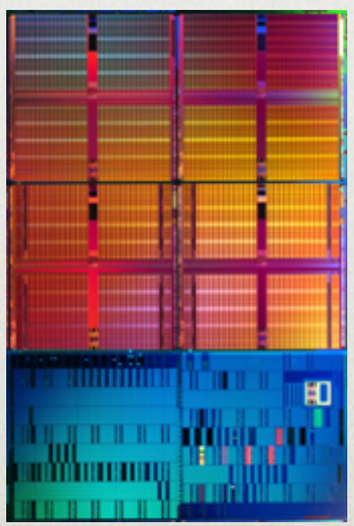
It consists of atoms
and molecules that
are governed by
quantum physics

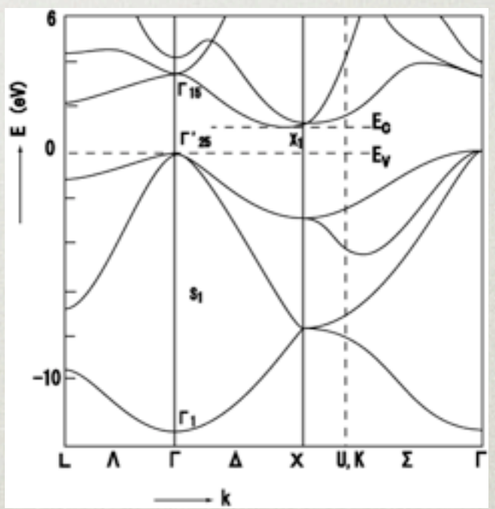
Is the human brain a quantum computer?

A: Obviously yes!

It consists of atoms and molecules that are governed by quantum physics

But so does a silicon based computer.





Is the human brain a quantum computer?

A: Obviously not!

Is the human brain a quantum computer?

A: Obviously not!

$$i\frac{\partial\psi}{\partial t} = -\frac{1}{2m}\Delta\psi + V\psi$$

We can always resort to simulating all the atoms of the brain on a Turing machine to arbitrary precision.

Is the human brain a quantum computer?

A: Obviously not!

$$i\frac{\partial\psi}{\partial t} = -\frac{1}{2m}\Delta\psi + V\psi$$

We can always resort to simulating all the atoms of the brain on a Turing machine to arbitrary precision.

But so does every specific traveling salesman problem with 2.000.000 cities take only $O(1)$ time to solve.

Is the human brain a quantum computer?

A: I have no idea!

Is the human brain a quantum computer?

A: I have no idea!

The question should mean:
Can I simulate N brains effectively with a number of Turing machines that is polynomial in N?

Thank you

Kudos to #schneider of μCCC for ACAB lamps!

Questions, comments & more info:

helling@atdotde.de

@atdotde

http://atdotde.blogspot.com