Introduction to Quantum Computing

K. Grover

Outline

- 1 History and Motivation
- 2 Classical vs Quantum Computing
- 3 A small example
- 4 Quantum > Classical
- 5 Cool Things

Disclaimer

I am STILL not an expert on quantum stuff.

History and Motivation

History and Motivation

•000

■ It all started in late 19th and early 20th century.

History and Motivation

- It all started in late 19th and early 20th century.
- Light behaves like particles (Photoelectric effect [1905]).

History and Motivation

- It all started in late 19th and early 20th century.
- Light behaves like particles (Photoelectric effect [1905]).
- Classical theories are not applicable, new theories required.

History and Motivation

- It all started in late 19th and early 20th century.
- Light behaves like particles (Photoelectric effect [1905]).
- Classical theories are not applicable, new theories required.
- Quantum mechanics was born.

History and Motivation

- It all started in late 19th and early 20th century.
- Light behaves like particles (Photoelectric effect [1905]).
- Classical theories are not applicable, new theories required.
- Quantum mechanics was born.
- Most theories in classical physics can be derived from quantum mechanics as an approximation valid at large (macroscopic) scale.

History and Motivation

1980 Paul Benioff proposed quantum mechanical model of a Turing machine.

History and Motivation

- 1980 Paul Benioff proposed quantum mechanical model of a Turing machine.
- 1982 Richard Feynman and Yuri Manin suggested: QC > CC.

- 1980 Paul Benioff proposed quantum mechanical model of a Turing machine.
- 1982 Richard Feynman and Yuri Manin suggested: QC > CC.
- 1994 Shor's factoring algorithm.

- 1980 Paul Benioff proposed quantum mechanical model of a Turing machine.
- 1982 Richard Feynman and Yuri Manin suggested: QC > CC.
- 1994 Shor's factoring algorithm.
- 1996 Grover's algorithm.

History and Motivation

- 1980 Paul Benioff proposed quantum mechanical model of a Turing machine.
- 1982 Richard Feynman and Yuri Manin suggested: QC > CC.
- 1994 Shor's factoring algorithm.
- 1996 Grover's algorithm.
- 1997 I was born.

- 1980 Paul Benioff proposed quantum mechanical model of a Turing machine.
- 1982 Richard Feynman and Yuri Manin suggested: QC > CC.
- 1994 Shor's factoring algorithm.
- 1996 Grover's algorithm.
- 1997 I was born.
- 2019 Google proved quantum supremacy. (200 seconds vs 10,000 years)

- 1980 Paul Benioff proposed quantum mechanical model of a Turing machine.
- 1982 Richard Feynman and Yuri Manin suggested: QC > CC.
- 1994 Shor's factoring algorithm.
- 1996 Grover's algorithm.
- 1997 I was born.
- 2019 Google proved quantum supremacy. (200 seconds vs 10,000 years)
- 2019 IBM said bullshit!

- 1980 Paul Benioff proposed quantum mechanical model of a Turing machine.
- 1982 Richard Feynman and Yuri Manin suggested: QC > CC.
- 1994 Shor's factoring algorithm.
- 1996 Grover's algorithm.
- 1997 I was born.
- 2019 Google proved quantum supremacy. (200 seconds vs 10,000 years)
- 2019 IBM said bullshit!
- 2021 USTC proved quantum supremacy. Boson sampling with 76 photos. (20 seconds vs 600 million years)

Why is QC important?

■ Classical computers are getting smaller and more powerful day by day.

- Classical computers are getting smaller and more powerful day by day.
- Transistors (5 nm) are approaching the size of an atom (0.1 nm).

Why is QC important?

- Classical computers are getting smaller and more powerful day by day.
- \blacksquare Transistors (5 nm) are approaching the size of an atom (0.1 nm).
- Quantum tunneling -> bad transistors.

History and Motivation

- Classical computers are getting smaller and more powerful day by day.
- Transistors (5 nm) are approaching the size of an atom (0.1 nm).
- Quantum tunneling -> bad transistors.
- Use Shor's algorithm.

- Classical computers are getting smaller and more powerful day by day.
- \blacksquare Transistors (5 nm) are approaching the size of an atom (0.1 nm).
- Quantum tunneling -> bad transistors.
- Use Shor's algorithm.
- Use Grover's algorithm.

Why is QC important?

History and Motivation

- Classical computers are getting smaller and more powerful day by day.
- Transistors (5 nm) are approaching the size of an atom (0.1 nm).
- Quantum tunneling -> bad transistors.
- Use Shor's algorithm.
- Use Grover's algorithm.
- Simulate quantum mechanical systems. Speed up biological research by giving new insights on proteins.

Classical vs Quantum Computing

■ Dirac delta notation:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

■ Dirac delta notation:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

■ What are the operations on a single bit?

Operations on a single bit

■ Identity:

$$0 \longrightarrow 0$$

$$1 \longrightarrow 1$$

■ Negation:

$${}^0_1 > < {}^0_1$$

■ Constant 0:

$$0 \longrightarrow 0$$

■ Constant 1:

$$0 \longrightarrow 0$$

$$1 \longrightarrow 1$$

Operations on a single bit using matrices

■ Identity:

$$|0\rangle \to |0\rangle \qquad \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

■ Negation:

$$\begin{array}{c|c} |0\rangle & |0\rangle & & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}$$

■ Constant 0:

$$\begin{vmatrix}
|0\rangle \rightarrow |0\rangle \\
|1\rangle & |1\rangle
\end{vmatrix}$$

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

■ Constant 1:

$$\begin{array}{c|c} |0\rangle & |0\rangle & & & \begin{pmatrix} 0 & 1 \\ 1\rangle & \rightarrow |1\rangle & & & \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \end{array}$$

Operations on a single bit using matrices

■ Identity:

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

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

■ Negation:

$$\frac{|0\rangle}{|1\rangle} > \mathbf{x} \frac{|0\rangle}{|1\rangle}$$

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

■ Constant 0:

$$\begin{vmatrix} |0\rangle \rightarrow |0\rangle \\ |1\rangle \end{vmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

■ Constant 1:

$$\begin{array}{c|c} |0\rangle & |0\rangle \\ |1\rangle & |1\rangle \end{array}$$

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

2 bits

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |0\rangle$$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix} = |0\rangle$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |1\rangle$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |2\rangle$$

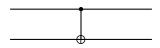
$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |3\rangle$$

Operations on 2 bits

CNOT operation:

$$\begin{array}{ccc} |00\rangle & \longrightarrow & |00\rangle \\ |01\rangle & \longrightarrow & |01\rangle \\ \\ |10\rangle & & & |10\rangle \\ |11\rangle & & & |11\rangle \end{array}$$

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



$$|010...01\rangle = |i\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \leftarrow (i-1) \text{th index}$$

Qubits

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle$$
$$|\alpha|^2 + |\beta|^2 = 1$$

Qubits

$$egin{pmatrix} lpha \ eta \end{pmatrix} = lpha egin{pmatrix} 1 \ 0 \end{pmatrix} + eta egin{pmatrix} 0 \ 1 \end{pmatrix} = lpha |0
angle + eta |1
angle \ |lpha|^2 + |eta|^2 = 1 \end{pmatrix}$$

Some examples:
$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{\sqrt{3}}{2}\iota \\ \frac{1}{2}\iota \end{pmatrix}$$

$$egin{pmatrix} lpha \ eta \end{pmatrix} = lpha egin{pmatrix} 1 \ 0 \end{pmatrix} + eta egin{pmatrix} 0 \ 1 \end{pmatrix} = lpha |0
angle + eta |1
angle \ |lpha|^2 + |eta|^2 = 1 \end{pmatrix}$$

Some examples:
$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix} \begin{pmatrix} -\frac{\sqrt{3}}{2}\iota \\ \frac{1}{2}\iota \end{pmatrix}$$

- Polarization of a photon.
- Current in a supercondutor.
- Spin of an electron.
- Collection of anyons.

Qubits

$$\begin{pmatrix} \alpha_{11} \\ \alpha_{12} \end{pmatrix} \otimes \begin{pmatrix} \alpha_{21} \\ \alpha_{22} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} \alpha_{n1} \\ \alpha_{n2} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{2^n-1} \end{pmatrix}$$

$$\begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{2^n-1} \end{pmatrix} \neq \begin{pmatrix} \delta_{11} \\ \delta_{12} \end{pmatrix} \otimes \begin{pmatrix} \delta_{21} \\ \delta_{22} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} \delta_{n1} \\ \delta_{n2} \end{pmatrix}$$

Recap

■ History and Motivation.

Quantum Supremacy.

- History and Motivation.
- Dirac delta notation for representing cbits and qubits.

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv e^{\iota \phi} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} -\frac{\sqrt{3}}{2} \iota \\ \frac{1}{2} \iota \end{pmatrix}$$

Recap

- History and Motivation.
- Dirac delta notation for representing cbits and qubits.
- Superposition.

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv e^{\iota \phi} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} -\frac{\sqrt{3}}{2} \iota \\ \frac{1}{2} \iota \end{pmatrix}$$

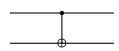
Recap

- History and Motivation.
- Dirac delta notation for representing cbits and qubits.
- Superposition.
- Tensor product for multiple qubits.

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha & \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \\ \beta & \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \end{pmatrix}$$
$$= \begin{pmatrix} \alpha \gamma \\ \alpha \delta \\ \beta \gamma \end{pmatrix}$$

- History and Motivation.
- Dirac delta notation for representing cbits and qubits.
- Superposition.
- Tensor product for multiple qubits.
- Only reversible operations in QC e.g CNOT.

1	/1	0	0	0/
	0	1	0	0
	0	0	0	1
١	0	0	1	0/



A small example •00

A small example

Hadamard Gate

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = |+\rangle$$

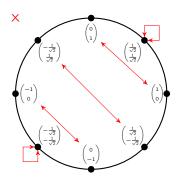
$$H|+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

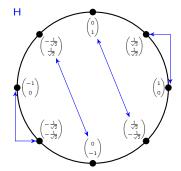
A state machine example

1 Qubit and only "bit-flip" and "hadamard" operator.

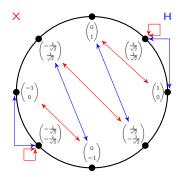
A state machine example

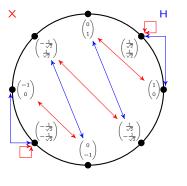
1 Qubit and only "bit-flip" and "hadamard" operator.





A state machine example



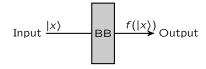




Quantum > Classical

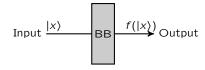
Deutsch Oracle problem

How many queries to find the one-bit operation?



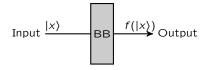
Deutsch Oracle problem

How many queries to find the one-bit operation?



How many queries to find if the one-bit operation was a constant function or not?

How many queries to find the one-bit operation?

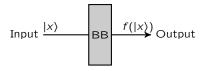


How many queries to find if the one-bit operation was a constant function or not?

How to do it in a single query?

Deutsch Oracle problem

How many queries to find the one-bit operation?



How many queries to find if the one-bit operation was a constant function or not?

How to do it in a single query? Let's take a look at how these operations look on a quantum computer.

Non-reversible computing on quantum computer

Identify input by looking at the output.

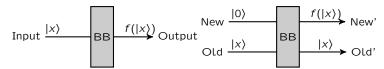
Non-reversible computing on quantum computer

Identify input by looking at the output. Output the input also.

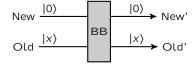
Quantum > Classical 00000000000

Non-reversible computing on quantum computer

Identify input by looking at the output. Output the input also.

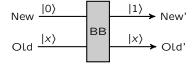


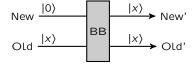
Constant-0

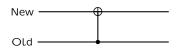


New —

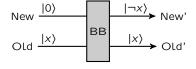
Old —

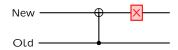




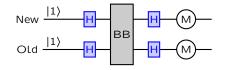


Negation





Deutsch oracle problem



Output: $|11\rangle \rightarrow$ Constant operation

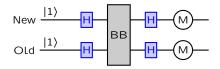
 $|01\rangle \rightarrow Variable operation$

Notation: |old, new>

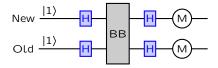
New |1> |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1| |1|</td

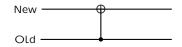
Output: |11>

Constant 1



Output: |11>



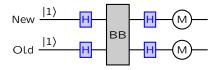


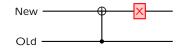
Output: |01>

Quantum > Classical 000000000000

$$C\left(\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}\right) = C\begin{pmatrix} \frac{\frac{1}{2}}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{\frac{1}{2}}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

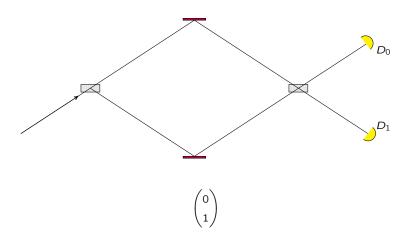
Negation



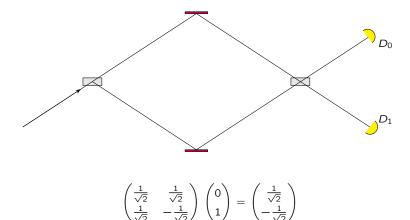


Output: |01>

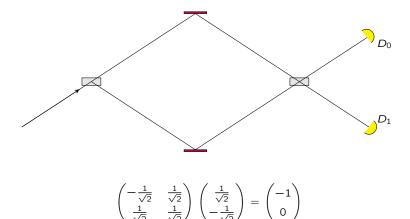
Cool Things

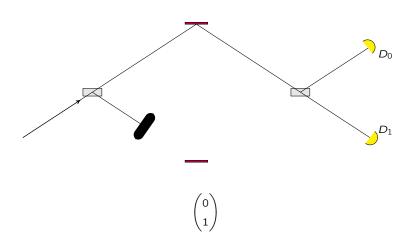


Mach-Zehnder Interferometer

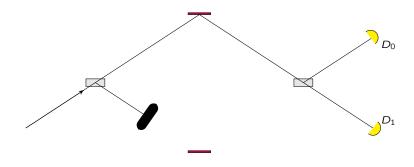


Mach-Zehnder Interferometer



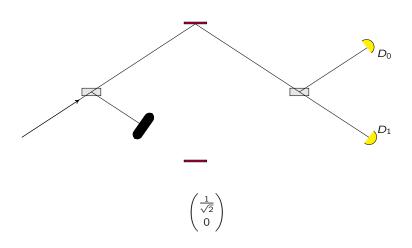


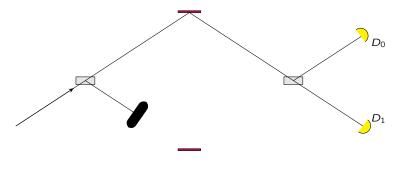
Mach-Zehnder Interferometer



$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Mach-Zehnder Interferometer

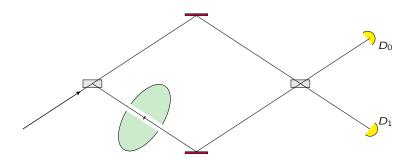




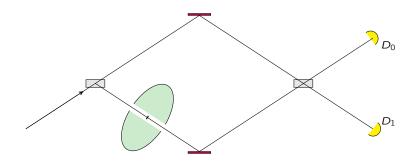
$$\begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$



Bomb doesn't work



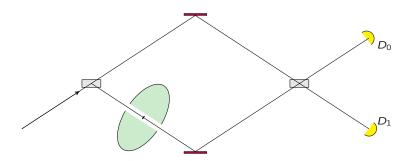
Bomb works



 $\mathcal{P}(Photon detected at bomb) = \frac{1}{2}$

Bomb explodes (Works)

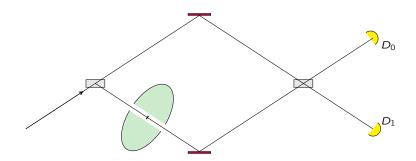
Bomb works



 $\mathcal{P}(Photon detected at bomb) = \frac{1}{2}$ $\mathcal{P}(\text{Photon detected at } D_0) = \frac{1}{4}$

Bomb explodes (Works) Bomb doesn't explode (Don't know)

Bomb works



 $\mathcal{P}(Photon detected at bomb) = \frac{1}{2}$ $\mathcal{P}(\text{Photon detected at } D_0) = \frac{1}{4}$ $\mathcal{P}(\mathsf{Photon}\ \mathsf{detected}\ \mathsf{at}\ D_1) = \frac{1}{4}$

Bomb explodes (Works) Bomb doesn't explode (Don't know) Bomb doesn't explode (Works)

■ If we cannot factor two bits, they are said to be **entangled**.

Quantum Entanglement

If we cannot factor two bits, they are said to be entangled.

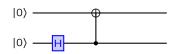
e.g.
$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

$$ac = \frac{1}{\sqrt{2}}$$

$$ad = 0$$

$$bc = 0$$

$$bd = \frac{1}{\sqrt{2}}$$



$$CH_1\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=C\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=C\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}$$

Spooky action at a distance!

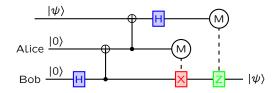
■ Einstein, Podolsky and Rosen gave the idea of Quantum entanglement.

Spooky action at a distance!

- Einstein, Podolsky and Rosen gave the idea of Quantum entanglement.
- Principle of locality would be violated.

- Einstein, Podolsky and Rosen gave the idea of Quantum entanglement.
- Principle of locality would be violated.
- Experiments show that Quantum entanglement happens.

Transferring (state of) a qubit from one location to other.



- No cloning theorem.
- Not faster than light.

Next time?

- Better understanding of quantum state machines.
- Verification of quantum systems.
- What can we do?

Sources:

- Youtube video titled "Quantum computing for computer scientists" by Microsoft Research.
- John Preskill's (Caltech) lectures on quantum computing.
- Model Checking Quantum Systems by M. Ying and Y. Feng.
- A lot of other youtube videos and wikipedia pages on quantum stuff.