Introduction to Quantum Computing

K. Grover

Outline

1. Classical vs Quantum Computing
2. Quantum > Classical
3. Cool Things

Disclaimer

I am not an expert on quantum computing.

Classical vs Quantum Computing

Representing bits as vectors

bra-ket notation

- **ket** vector:

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

- **bra** vector:

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

2 bits

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

2 bits

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |0\rangle \qquad |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |1\rangle$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |2\rangle \qquad |11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |3\rangle$$

n bits

$$|010\ldots01\rangle = |i\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \leftarrow i\text{th index}$$

$$\text{Length} = 2^n$$

Operations on a single bit

- Identity:

$$\begin{tikzcd} 0 \arrow[r] & 0 \\ 1 \arrow[r] & 1 \end{tikzcd}$$

- Negation:

$$\begin{tikzcd} 0 \arrow[dr] & 0 \\ 1 \arrow[ur] & 1 \end{tikzcd}$$

- Constant 0:

$$\begin{tikzcd} 0 \arrow[r] & 0 \\ 1 \arrow[ur] & 1 \end{tikzcd}$$

- Constant 1:

$$\begin{tikzcd} 0 \arrow[dr] & 0 \\ 1 \arrow[r] & 1 \end{tikzcd}$$

Operations on a single bit using matrices

- Identity:

$$\begin{tikzcd}[row sep=small] |0\rangle \arrow[r] & |0\rangle \\ |1\rangle \arrow[r] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- Negation:

$$\begin{tikzcd}[row sep=small] |0\rangle \arrow[dr] & |0\rangle \\ |1\rangle \arrow[ur] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Constant 0:

$$\begin{tikzcd}[row sep=small] |0\rangle \arrow[r] & |0\rangle \\ |1\rangle \arrow[ur] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

- Constant 1:

$$\begin{tikzcd}[row sep=small] |0\rangle \arrow[dr] & |0\rangle \\ |1\rangle \arrow[r] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

Operations on a single bit using matrices

- Identity:

$$\begin{tikzcd} |0\rangle \arrow[r] & |0\rangle \\ |1\rangle \arrow[r] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

- Negation:

$$\begin{tikzcd} |0\rangle \arrow[dr] & |0\rangle \\ |1\rangle \arrow[ur] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Constant 0:

$$\begin{tikzcd} |0\rangle \arrow[r] & |0\rangle \\ |1\rangle \arrow[ur] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

- Constant 1:

$$\begin{tikzcd} |0\rangle \arrow[dr] & |0\rangle \\ |1\rangle \arrow[r] & |1\rangle \end{tikzcd} \qquad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

Operations on 2 bits

CNOT operation:

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

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

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

Operations on 2 bits

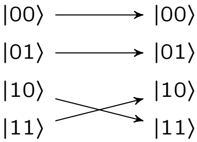
CNOT operation:

$$\begin{tikzcd}[row sep=small]
{|00\rangle} \arrow[r] & {|00\rangle} \\
{|01\rangle} \arrow[r] & {|01\rangle} \\
{|10\rangle} \arrow[dr] & {|10\rangle} \\
{|11\rangle} \arrow[ur] & {|11\rangle}
\end{tikzcd}
\qquad
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

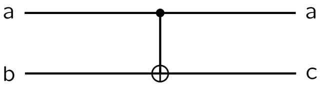
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Operations on 2 bits

CNOT operation:



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



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

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

$$|\alpha|^2 + |\beta|^2 = 1$$

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

Qubits

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

$$|\alpha|^2 + |\beta|^2 = 1$$

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

Total phase does not matter: $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = e^{i\theta}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$

2 Qubits

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

n Qubits

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

n Qubits

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

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

Hadamard Gate

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

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

What is a quantum algorithm

A circuit of quantum gates.

What is a quantum algorithm

A circuit of quantum gates.

Universal gates set:

CNOT, H, X, Z, $\frac{\pi}{8}$ rotation.

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the “bit-flip" operator.

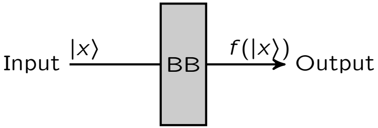
Recap

- Bra-ket notation.
- Tensor products.
- Qubits.
- CNOT, Hadamard and bit-flip gates.

Quantum > Classical

Deutsch Oracle problem

How many queries to find the one-bit operation?



Deutsch Oracle problem

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

Deutsch Oracle problem

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 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 a quantum computer

Identify input by looking at the output.

Non-reversible computing on a quantum computer

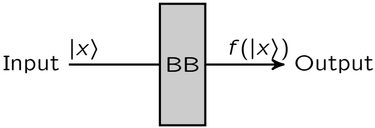
Identify input by looking at the output.

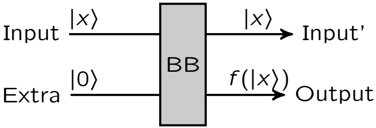
Output the input also.

Non-reversible computing on a quantum computer

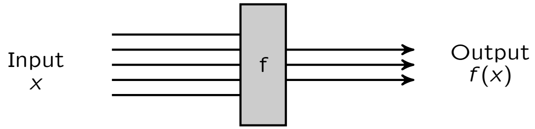
Identify input by looking at the output.

Output the input also.

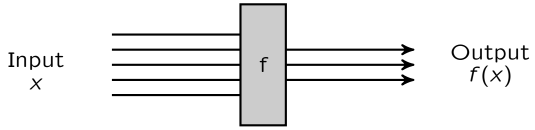


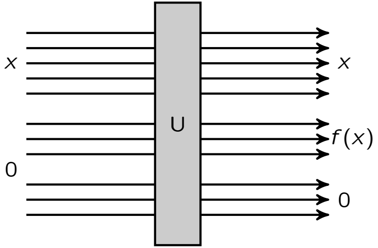


Non-reversible computing on a quantum computer

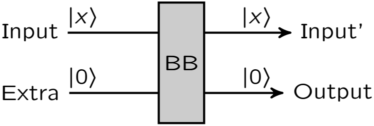


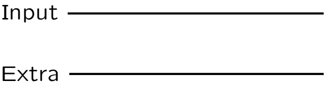
Non-reversible computing on a quantum computer



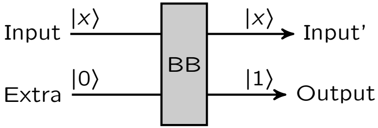


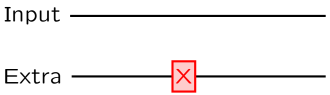
Constant-0


Input
$|x\rangle$
$|x\rangle$
Input'
BB
Extra
$|0\rangle$
$|0\rangle$
Output

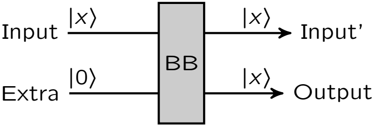

Input
Extra

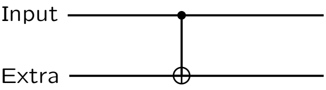
Constant-1


Input
$|x\rangle$
$|x\rangle$
Input'
BB
Extra
$|0\rangle$
$|1\rangle$
Output

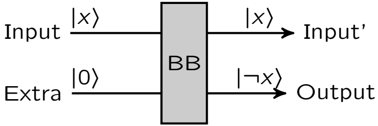

Input
Extra
X

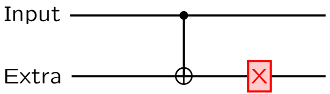
Identity


Input
$|x\rangle$
BB
$|x\rangle$
Input'
Extra
$|0\rangle$
$|x\rangle$
Output


Input
Extra

Negation


Input
$|x\rangle$
BB
$|x\rangle$
Input'
Extra
$|0\rangle$
$|\neg x\rangle$
Output


Input
Extra
X

Deutsch oracle problem

The black box contains one of the four circuits.

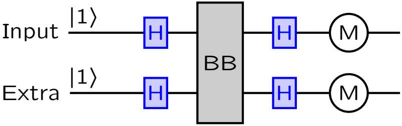
Deutsch oracle problem

The black box contains one of the four circuits.

Our problem is reduced to identifying which circuit.

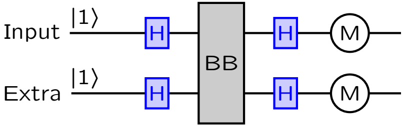
Constant or **Variable**.

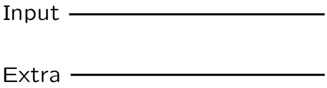
Deutsch oracle problem



Output: $|11\rangle \rightarrow$ Constant operation
$|01\rangle \rightarrow$ Variable operation

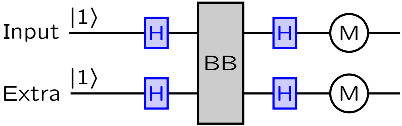
Constant 0

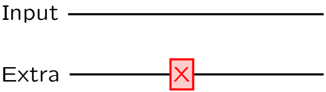




Output: $|11\rangle$

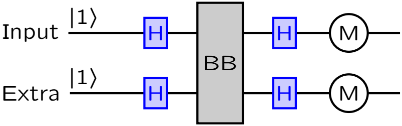
Constant 1

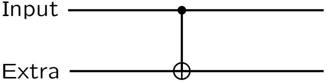




Output: $|11\rangle$

Identity



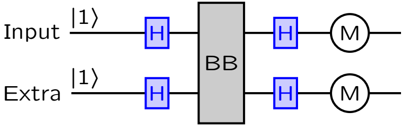


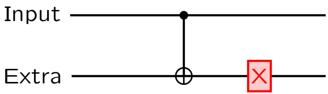
Output: $|01\rangle$

Identity

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

Negation





Output: $|01\rangle$

Is it useful?

- Deutsch-Jozsa algorithm.
- Simon's periodicity problem.
- Shor's algorithm.

Quantum Complexity

BQP

Quantum Complexity

$$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP}$$

Quantum Complexity

$$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$$

Quantum Complexity

$$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$$

$$\mathbf{NP} \subseteq \mathbf{BQP}?$$
$$\mathbf{BPP} \subsetneq \mathbf{BQP}?$$

Quantum Complexity

$$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$$

$$\mathbf{NP} \subseteq \mathbf{BQP}?$$
$$\mathbf{BPP} \subsetneq \mathbf{BQP}?$$

Conjecture:
Fourier sampling, Fourier checking $\in$ **BQP**
but $\notin$ **PH**

Recap

- Non-reversible computation on a quantum computer.
- Deutsch oracle problem.
- BQP.

Cool Things

Quantum Entanglement

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

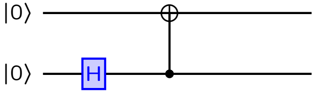
Quantum Entanglement

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

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

$$ac = \frac{1}{\sqrt{2}}$$
$$ad = 0$$
$$bc = 0$$
$$bd = \frac{1}{\sqrt{2}}$$

Quantum Entanglement



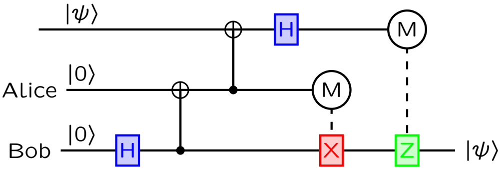
$$CH_1\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=C\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=C\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}$$

Spooky action at a distance!

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Quantum Teleportation

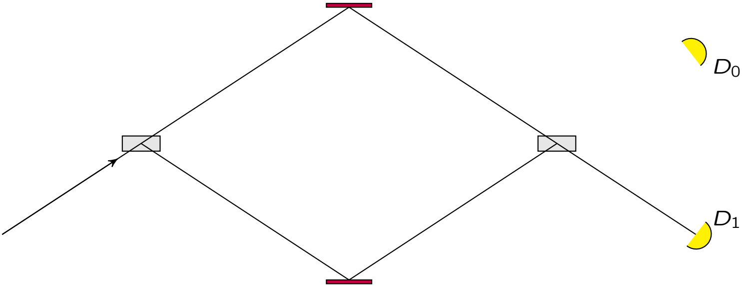
Transferring (state of) a qubit from one location to other.



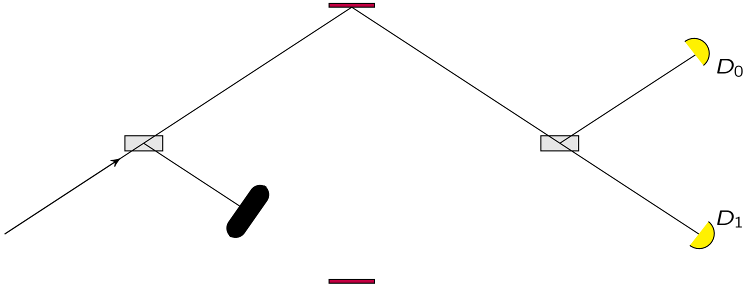
Quantum Teleportation

- No cloning theorem.
- Not faster than light.

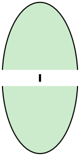
Mach-Zehnder Interferometer



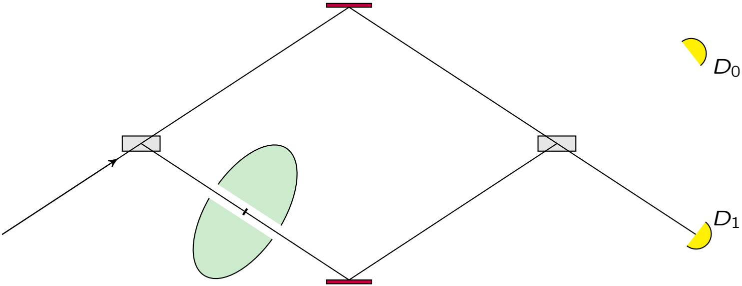
Mach-Zehnder Interferometer



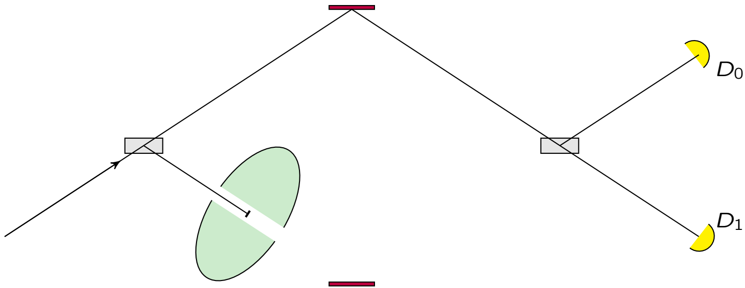
Elitzur-Vaidman Bombs



Bomb doesn't work



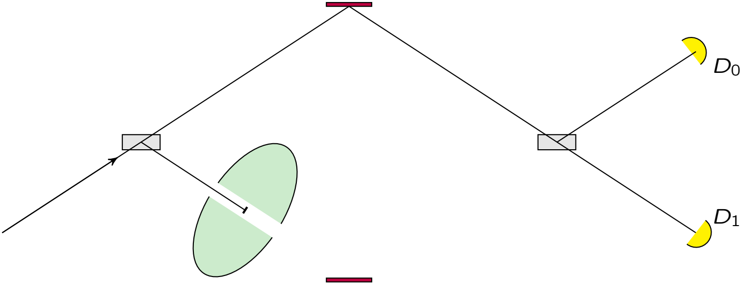
Bomb works



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

Bomb explodes (Works)

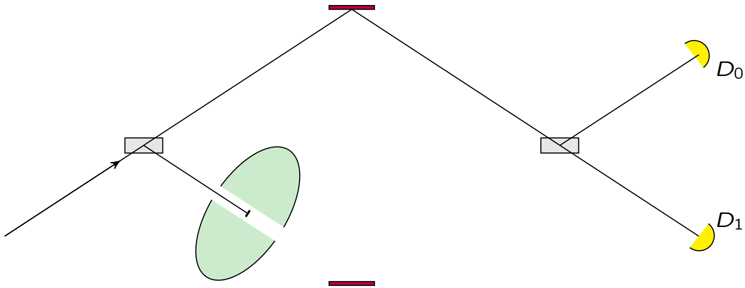
Bomb works



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

$\mathcal{P}$(Photon detected at D_0) $= \frac{1}{4}$ Bomb doesn't explode (Don't know)

Bomb works



$\mathcal{P}$(Photon detected at bomb) $= \frac{1}{2}$	Bomb explodes (Works)
$\mathcal{P}$(Photon detected at D_0) $= \frac{1}{4}$	Bomb doesn't explode (Don't know)
$\mathcal{P}$(Photon detected at D_1) $= \frac{1}{4}$	Bomb doesn't explode (Works)

Recap

- Quantum entanglement.
- Quantum teleportation.
- Elitzur-Vaidman bombs.

Thank You!

Sources:

- Youtube video titled "Quantum computing for computer scientists" by Microsoft Research.
- Umesh Vazirani's (UC Berkeley) lectures on quantum computing.
- 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.