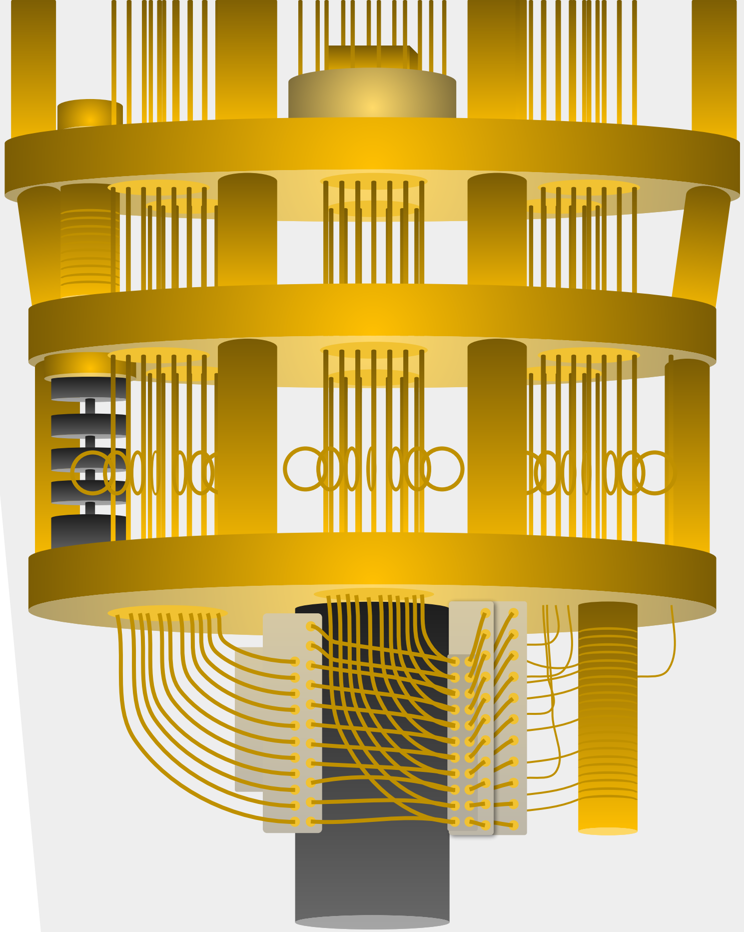
# Quantum Computing Basics (continued)



Barak Nehoran
Postdoc, CS Department, Columbia University

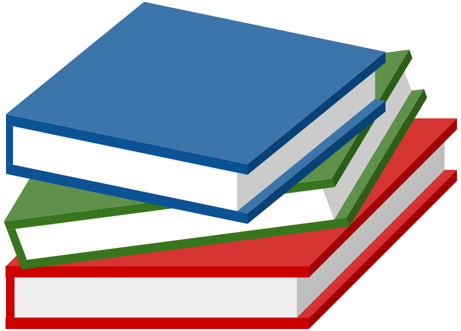
COMS 4281:
Intro to Quantum Computing
Sep 25, 2026

## Classical Information

## Quantum Information

Barak Nehoran (Postdoc, CS Department, Columbia University)

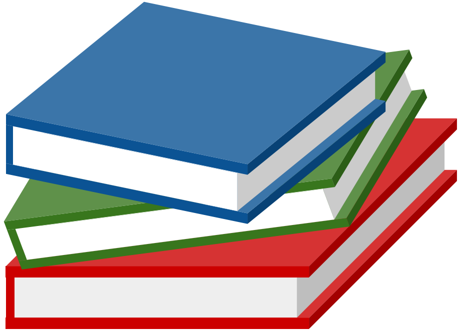
## Classical Information



## Quantum Information

Barak Nehoran (Postdoc, CS Department, Columbia University)

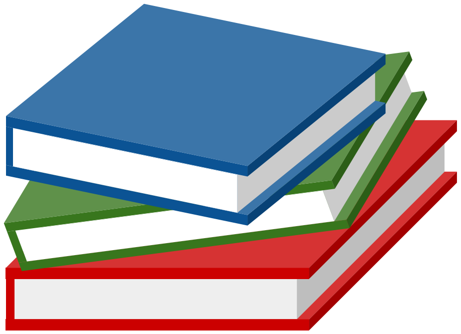
## Classical Information



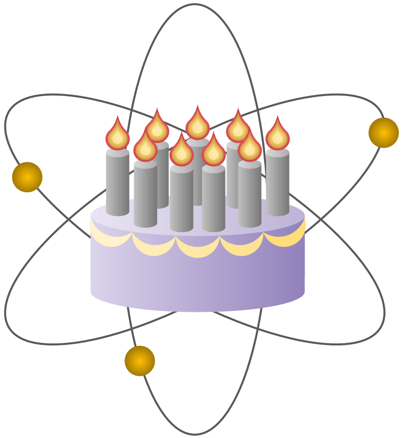
## Quantum Information

Barak Nehoran (Postdoc, CS Department, Columbia University)

## Classical Information

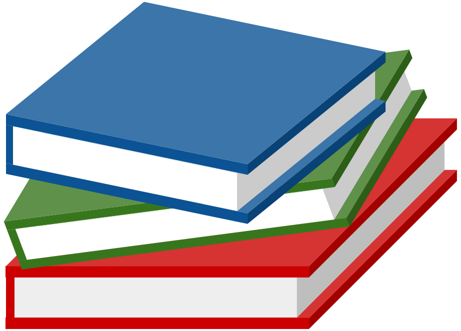


## Quantum Information



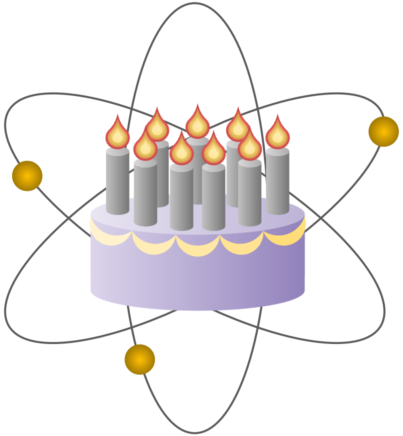
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Classical Information



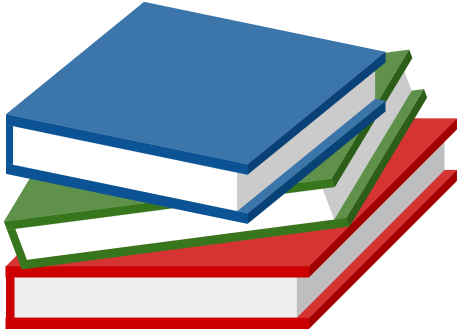
You can

# Quantum Information



By contrast,

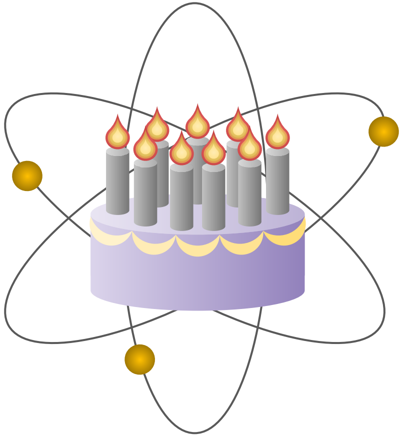
## Classical Information



You can

1. read it 

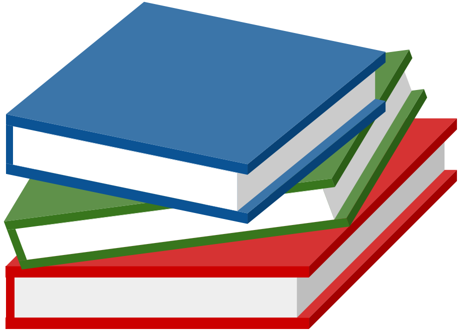
## Quantum Information



By contrast,

Barak Nehoran (Postdoc, CS Department, Columbia University)

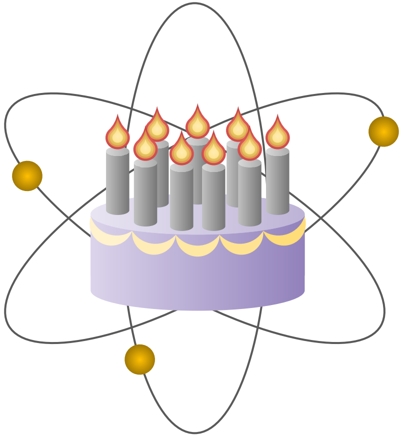
## Classical Information



You can

1. read it 

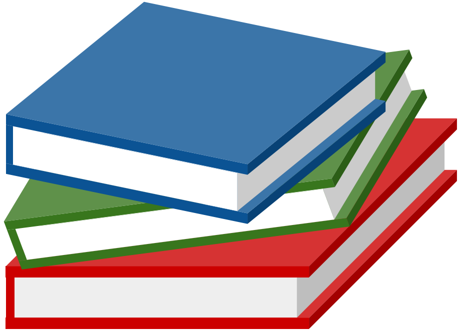
## Quantum Information



By contrast,

1. You can ***taste*** it, but it will destroy the cake!

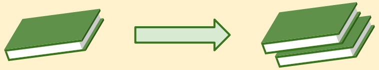
## Classical Information



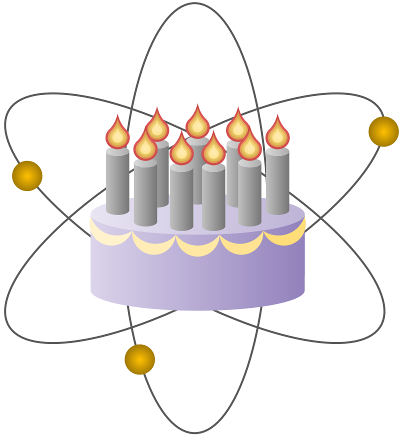
You can

1. read it 

2. make copies of it



## Quantum Information

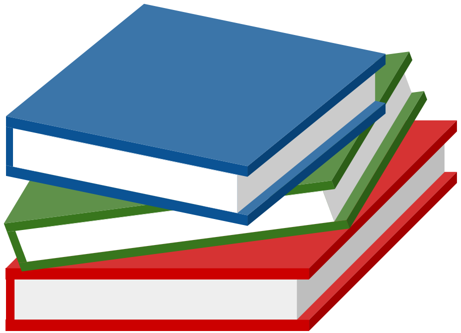


By contrast,

1. You can ***taste*** it, but it will destroy the cake!

Barak Nehoran (Postdoc, CS Department, Columbia University)

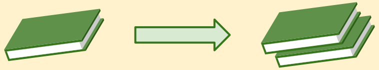
## Classical Information



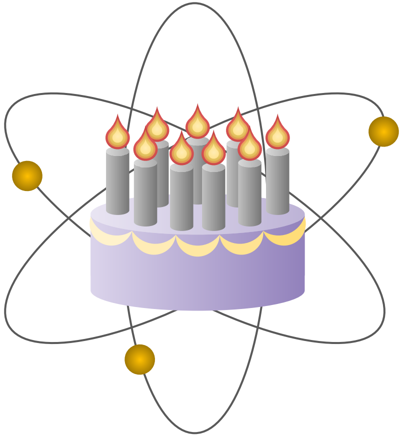
You can

1. read it 

2. make copies of it



## Quantum Information

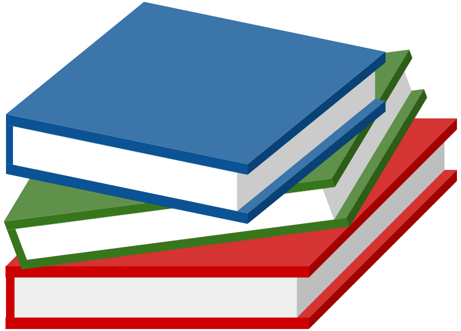


By contrast,

1. You can ***taste*** it, but it will destroy the cake!
2. **Can't make a copy** without the recipe!

Barak Nehoran (Postdoc, CS Department, Columbia University)

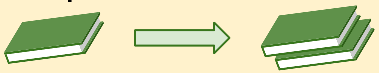
## Classical Information



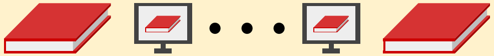
You can

1. read it

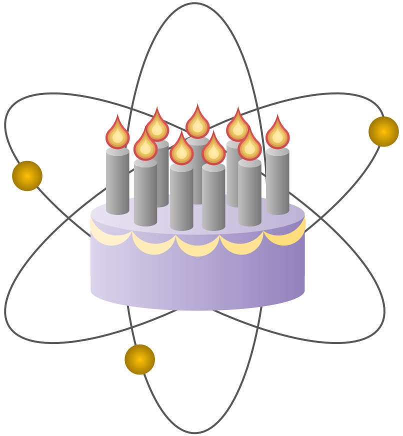
2. make copies of it



3. send it over the internet



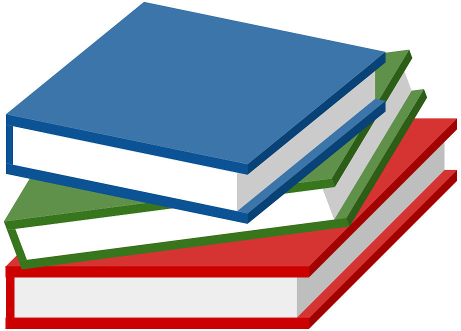
## Quantum Information



By contrast,

1. You can ***taste*** it, but it will destroy the cake!
2. **Can't make a copy** without the recipe!

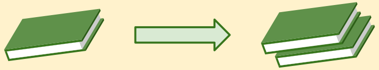
## Classical Information



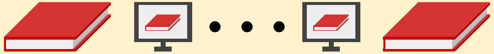
You can

1. read it

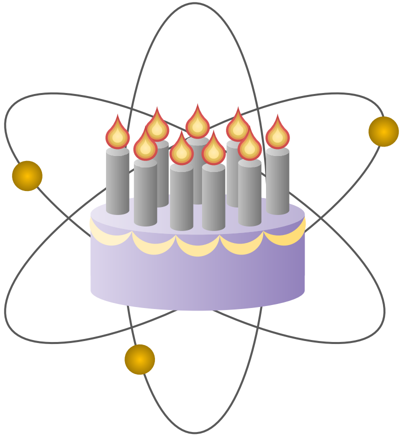
2. make copies of it



3. send it over the internet



## Quantum Information

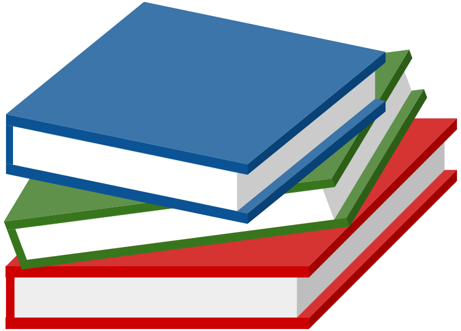


By contrast,

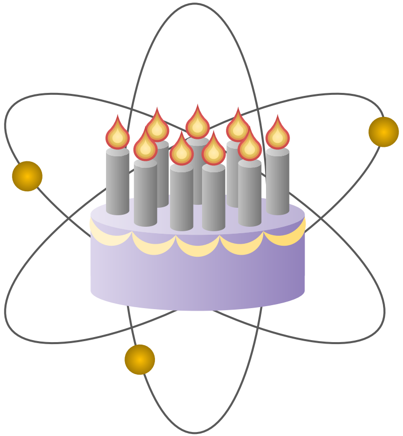
1. You can ***taste*** it, but it will destroy the cake!
2. **Can't make a copy** without the recipe!
3. Good luck **emailing** a cake...

Barak Nehoran (Postdoc, CS Department, Columbia University)


## Classical Information



## Quantum Information



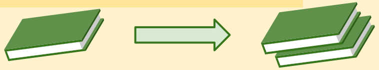
Measurement

Cloning

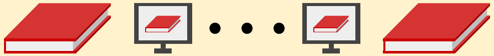
You can

1. read it

2. make copies of it



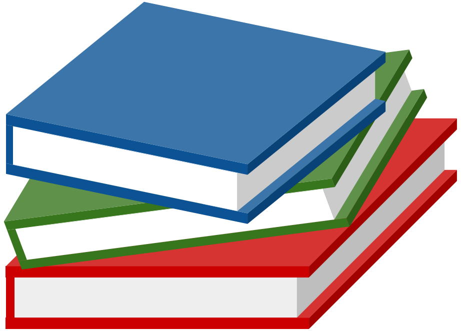
3. send it over the internet



By contrast,

1. You can ***taste*** it, but it will destroy the cake!
2. **Can't make a copy** without the recipe!
3. Good luck **emailing** a cake...

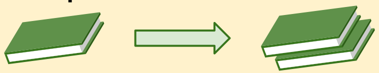
## Classical Information



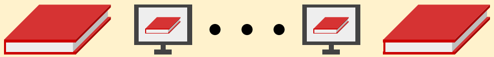
You can

1. read it 

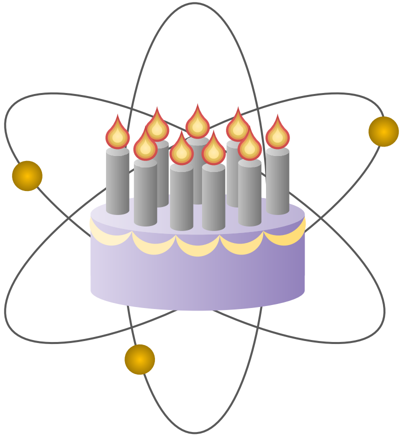
2. make copies of it



3. send it over the internet



## Quantum Information



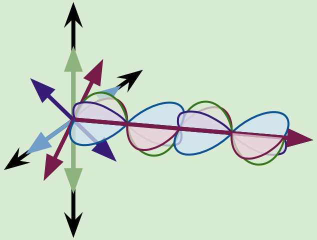
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Outline

Barak Nehoran (Postdoc, CS Department, Columbia University)

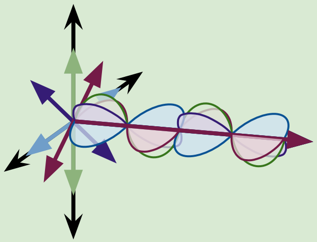
# Outline

1 The Qubit

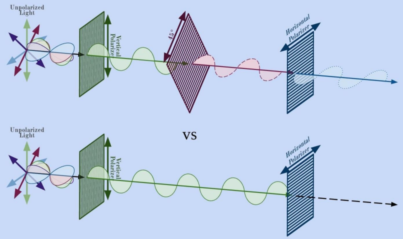


# Outline

1 **The Qubit**



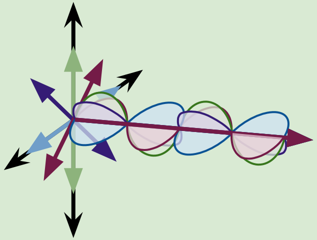
2 **Quantum Measurement**



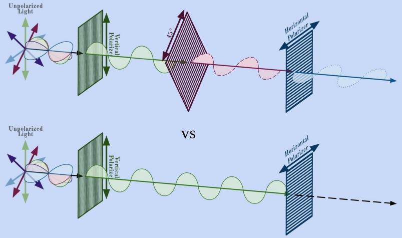
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Outline

1 **The Qubit**



2 **Quantum Measurement**



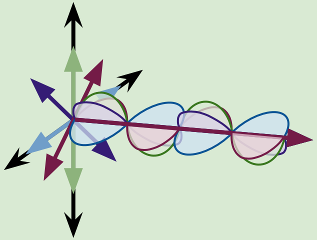

3 **Quantum Entanglement & Many Qubits**

First qubit  Second qubit

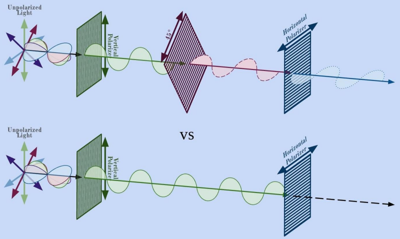
$$\frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

# Outline

1 The Qubit



2 Quantum Measurement

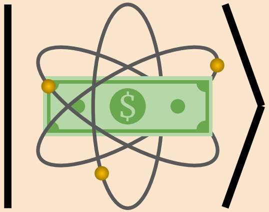



3 Quantum Entanglement & Many Qubits

First qubit Second qubit

$$\frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

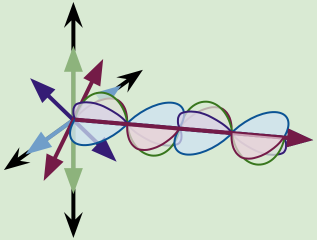
4 No Cloning and Quantum Money



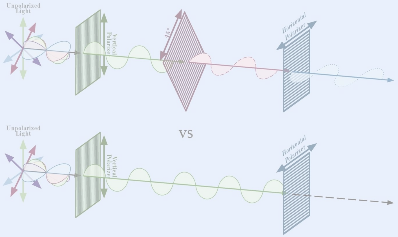
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Outline

## 1 The Qubit



## 2 Quantum Measurement

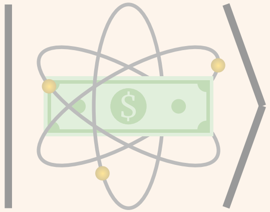



## 3 Quantum Entanglement & Many Qubits

First qubit Second qubit

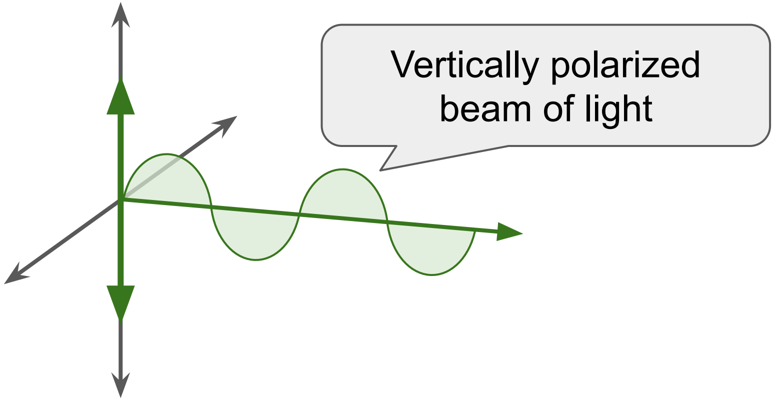
$$\frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

## 4 No Cloning and Quantum Money



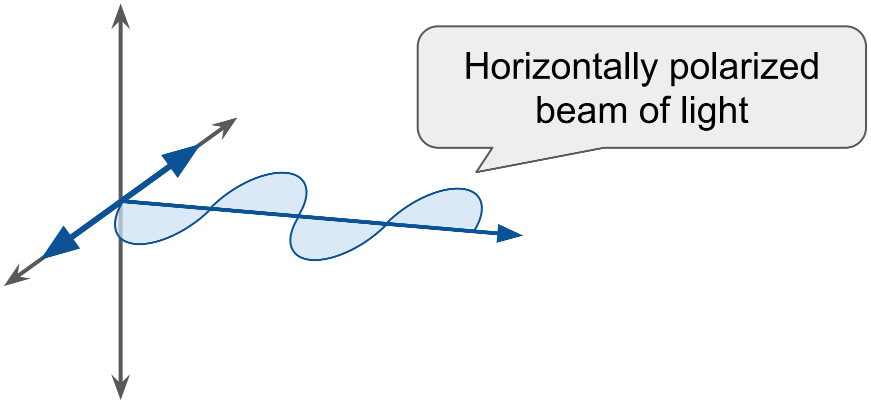
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum States and the Qubit: *Using light polarization as a running intuition*



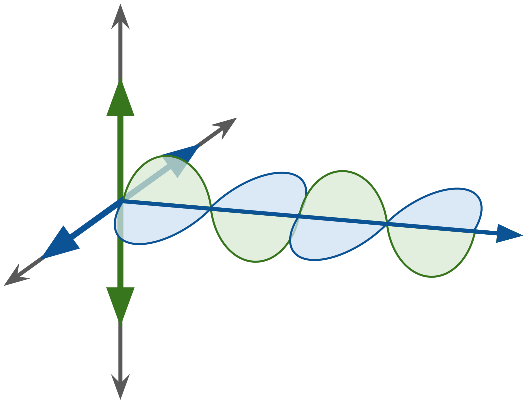
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum States and the Qubit: *Using light polarization as a running intuition*



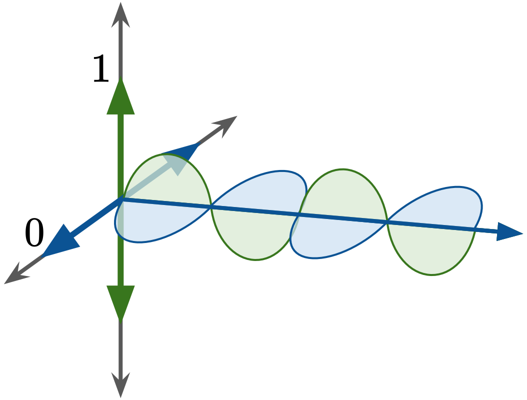
Barak Nehoran (Postdoc, CS Department, Columbia University)

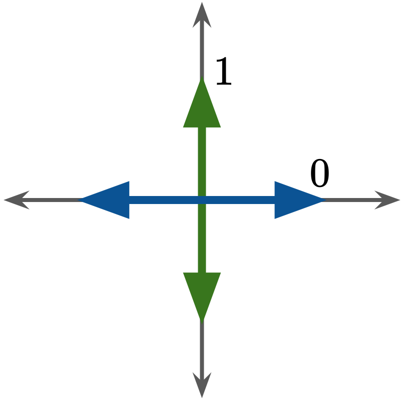
# Quantum States and the Qubit: *Using light polarization as a running intuition*



Barak Nehoran (Postdoc, CS Department, Columbia University)

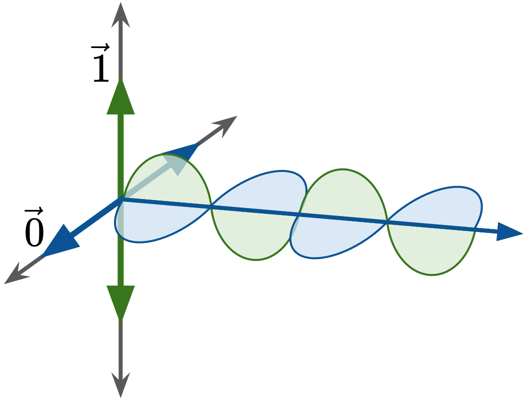
# Quantum States and the Qubit: *Using light polarization as a running intuition*

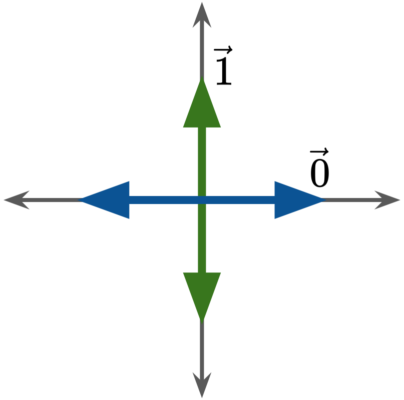



Representation of a **bit**

# Quantum States and the Qubit: *Using light polarization as a running intuition*



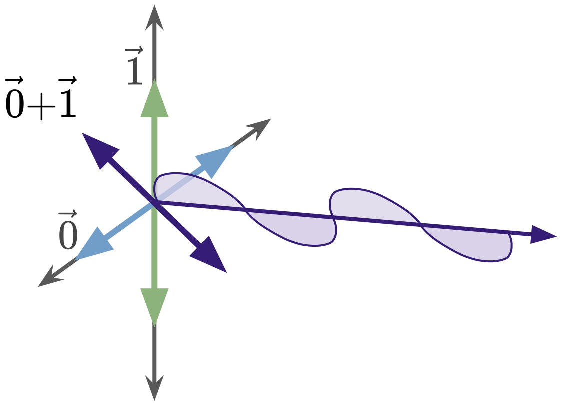

Representation of a *quantum* bit or "***qubit***"!

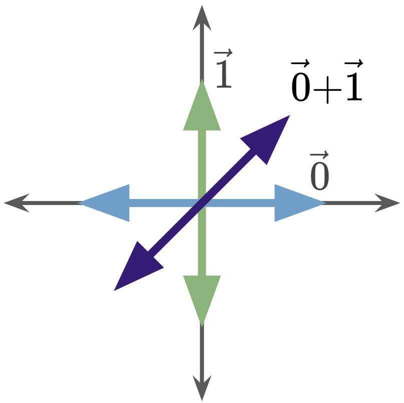
$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

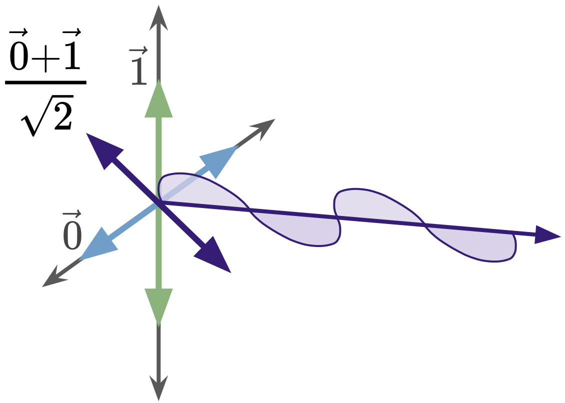
# Quantum States and the Qubit: *Using light polarization as a running intuition*

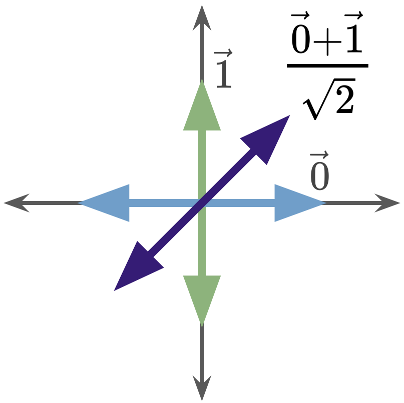


Barak Nehoran (Postdoc, CS Department, Columbia University)

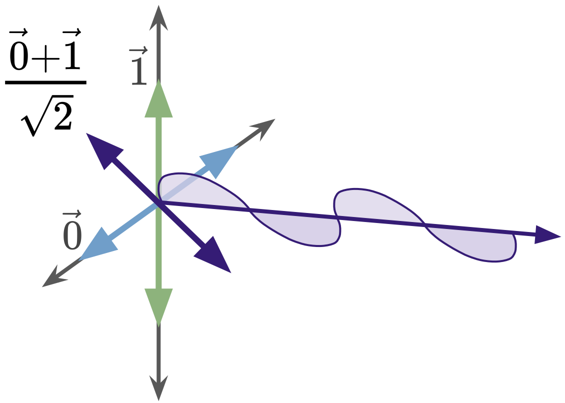
# Quantum States and the Qubit: *Using light polarization as a running intuition*

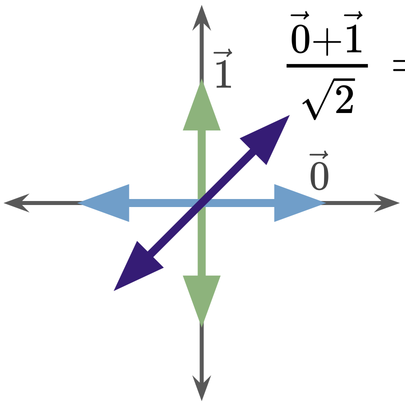


Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum States and the Qubit: *Using light polarization as a running intuition*

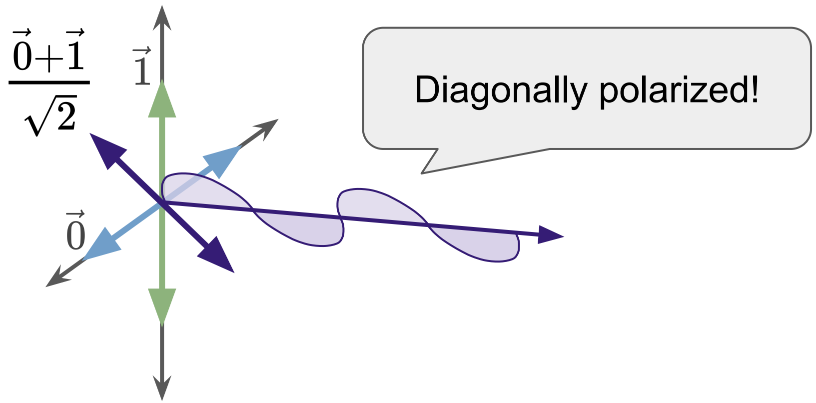


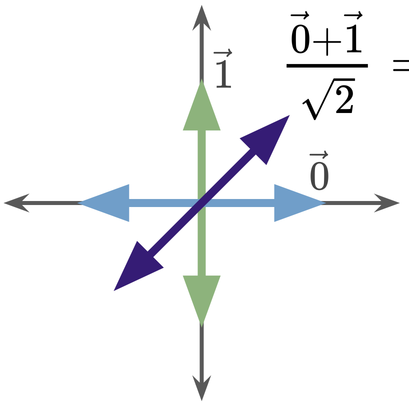




$$\frac{\vec{0}+\vec{1}}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum States and the Qubit: *Using light polarization as a running intuition*

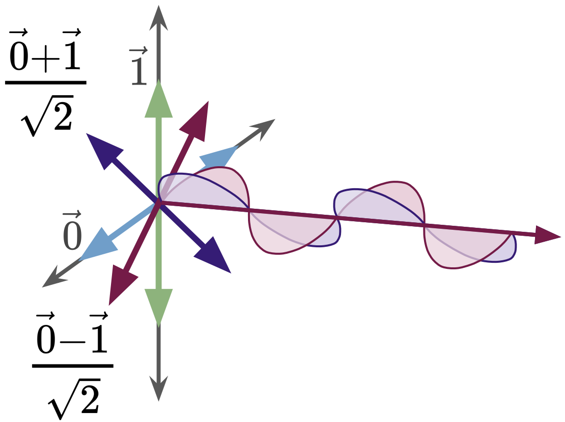


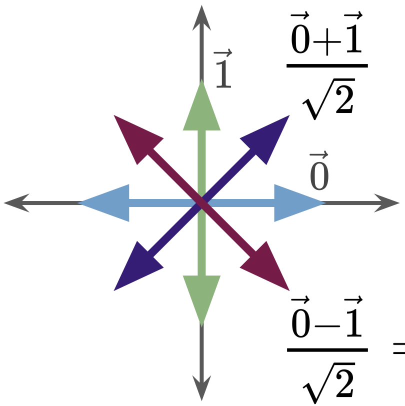




$$\frac{\vec{0}+\vec{1}}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

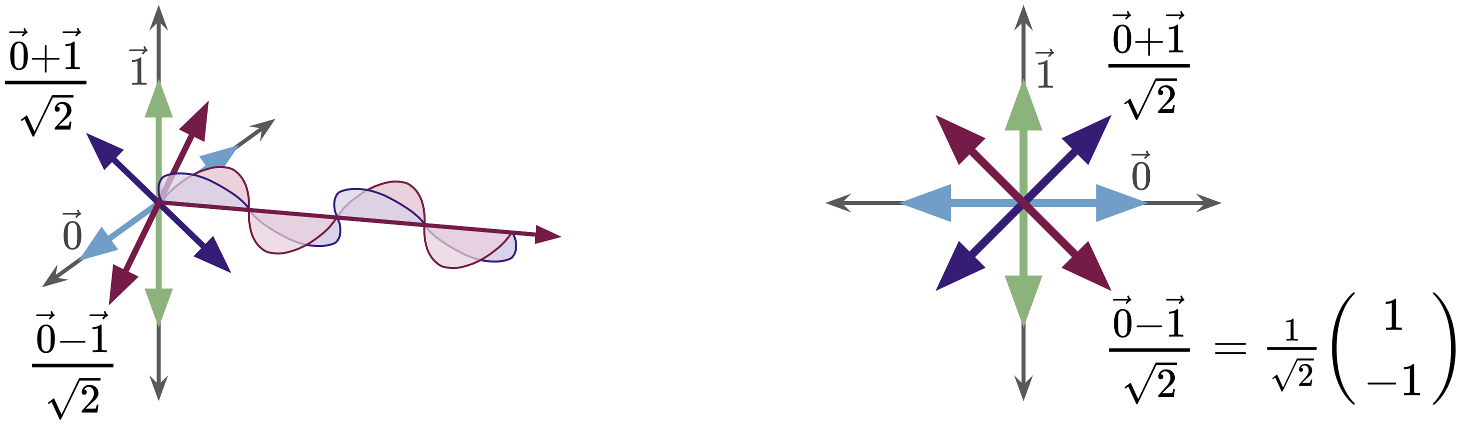
# Quantum States and the Qubit: *Using light polarization as a running intuition*




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

# Quantum States and the Qubit: *Using light polarization as a running intuition*



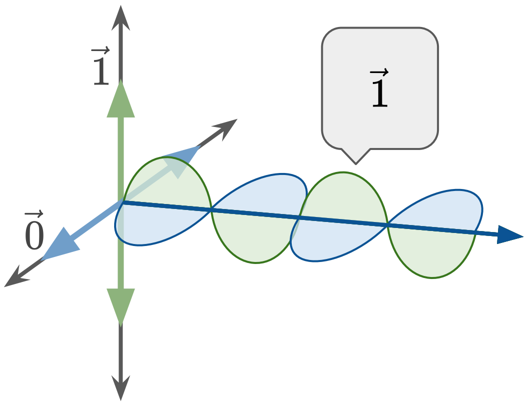

You may have heard this described as

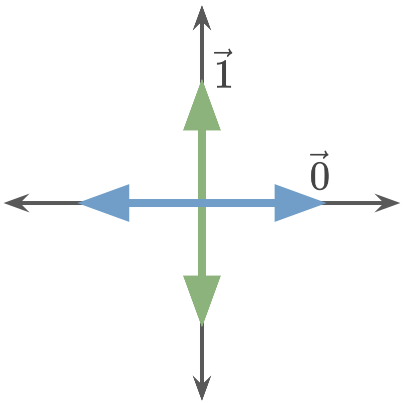
"***being simultaneously in both the zero and the one state***."

These linear combinations are really just another unit vector in a different direction!

Barak Nehoran (Postdoc, CS Department, Columbia University)

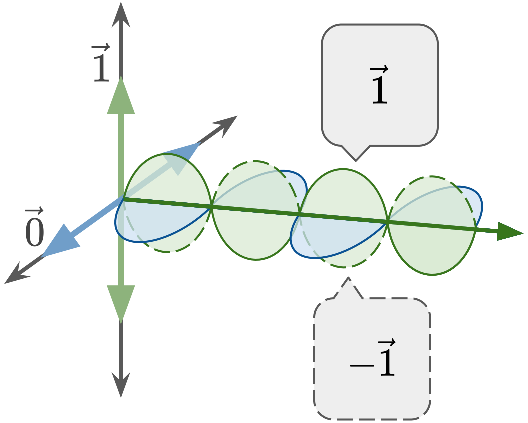
# Quantum States and the Qubit: *Using light polarization as a running intuition*

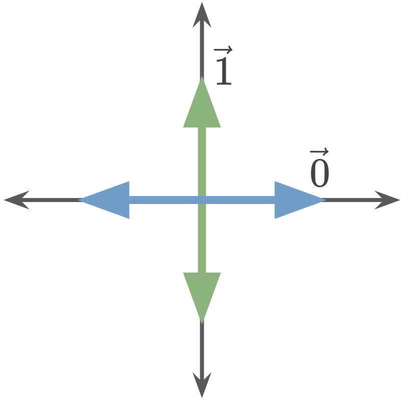


Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum States and the Qubit: *Using light polarization as a running intuition*

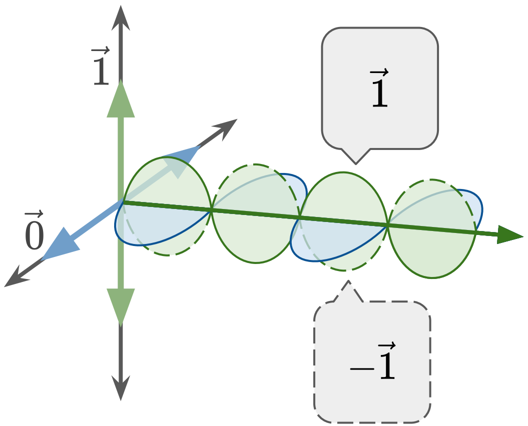


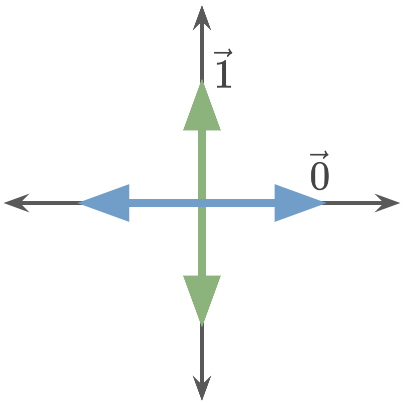




Observe that **negating a state** vector leaves it **polarized the same way**.

It merely **changes the phase!** $-\vec{v} \equiv \vec{v}$

# Quantum States and the Qubit: *Using light polarization as a running intuition*



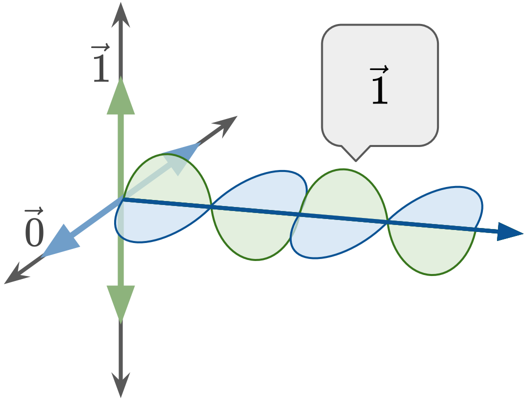

Observe that **negating a state** vector leaves it **polarized the same way**.

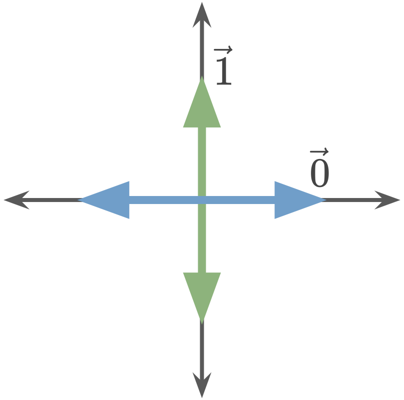
It merely **changes the phase**! $-\vec{v} \equiv \vec{v}$

In fact, that's the case in general for *any complex coefficient of unit norm*.

$$e^{i\theta}\vec{v} \equiv \vec{v} \ \ \forall\theta$$

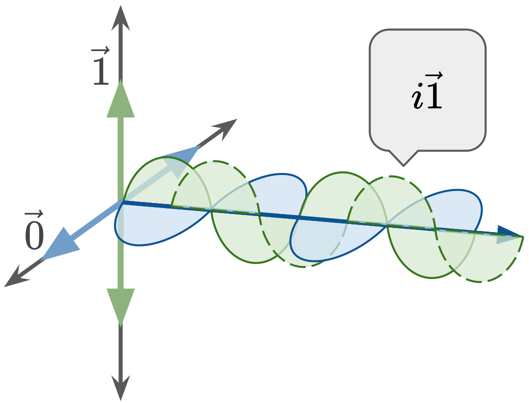
# Aside: Complex Number Coefficients

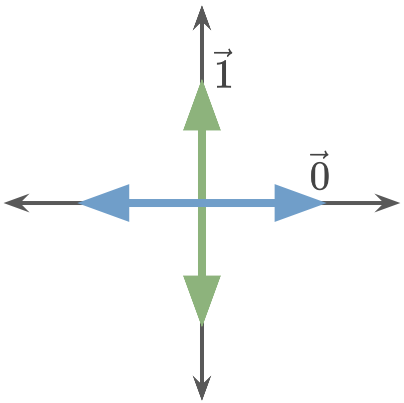


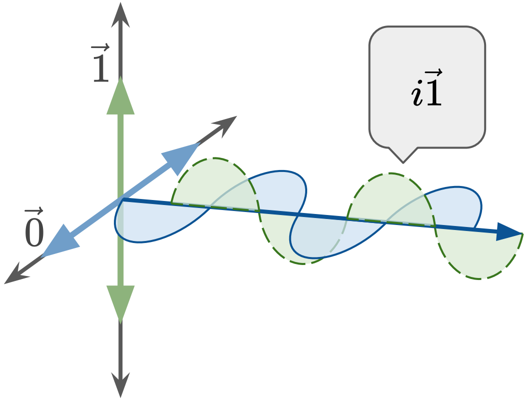
Barak Nehoran (Postdoc, CS Department, Columbia University)

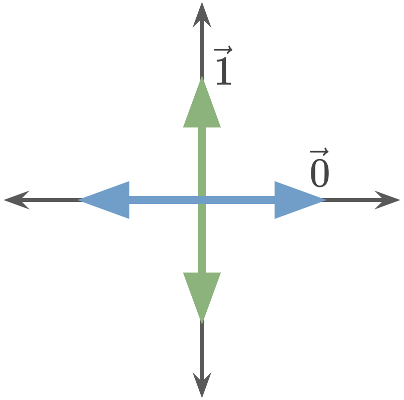
# Aside: Complex Number Coefficients



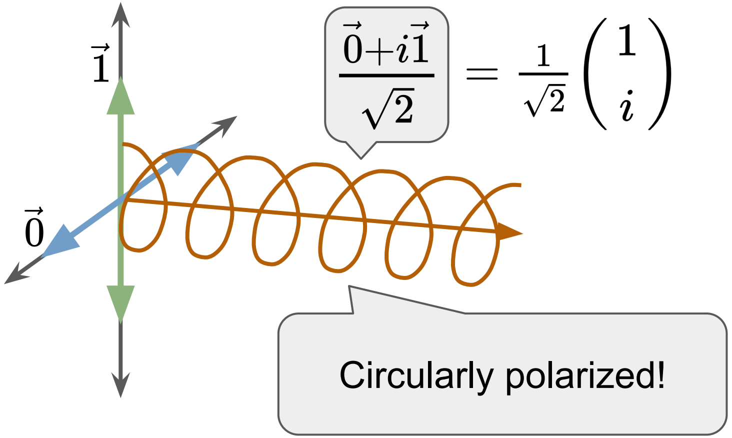



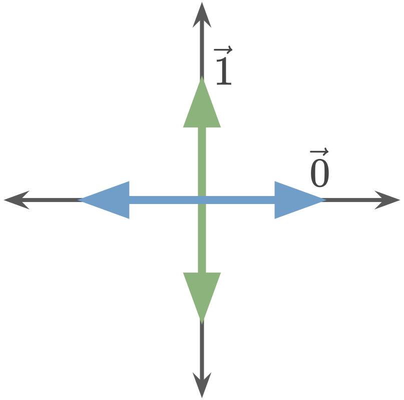
# Aside: Complex Number Coefficients



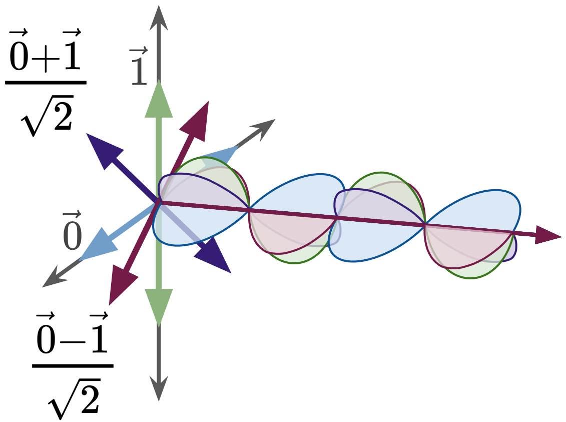



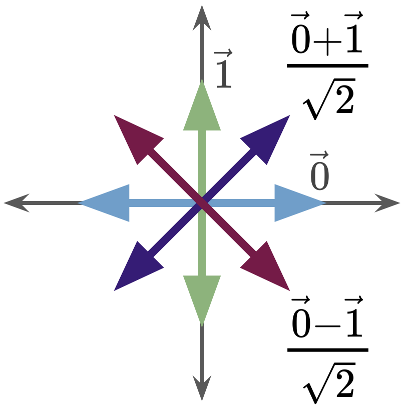
# Aside: Complex Number Coefficients



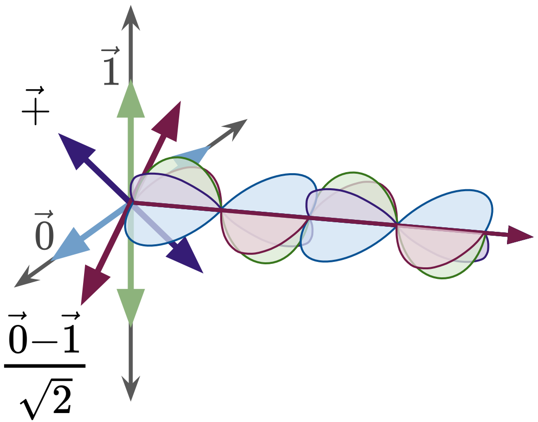



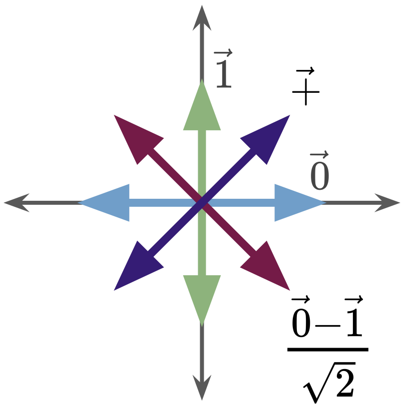
# Quantum States and the Qubit: *Using light polarization as a running intuition*



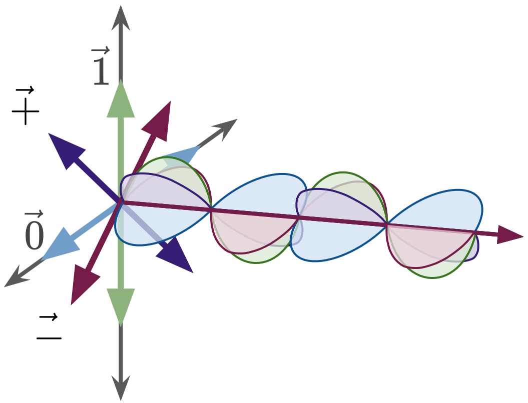
# Quantum States and the Qubit: *Using light polarization as a running intuition*

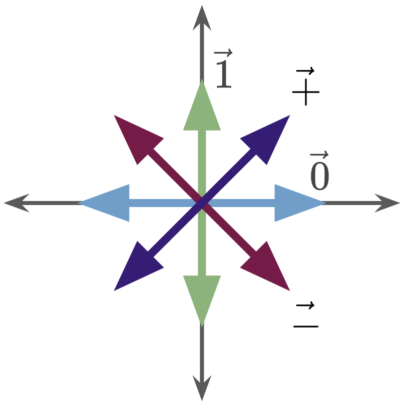


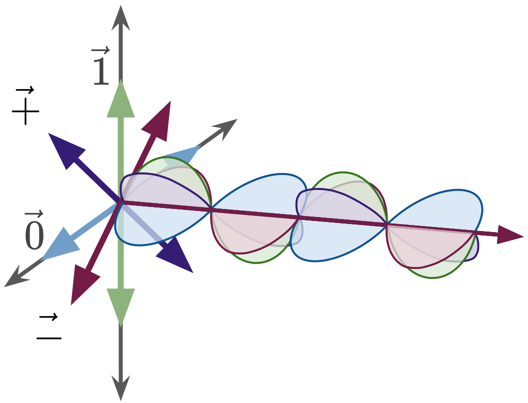
Barak Nehoran (Postdoc, CS Department, Columbia University)

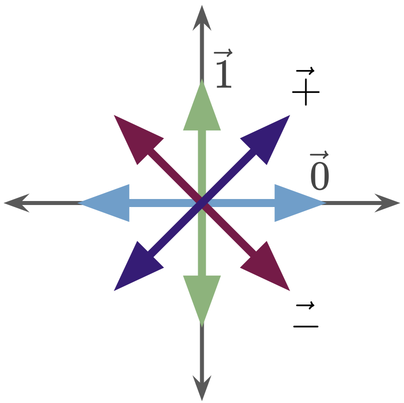
# Quantum States and the Qubit: *Using light polarization as a running intuition*



# Quantum States and the Qubit: *Using light polarization as a running intuition*



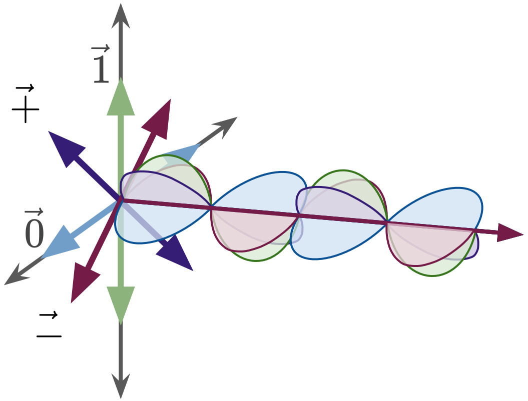




## Takeaways:

- A quantum state is represented by a **unit vector**.
- Any normalized linear combinations of quantum states is also a valid quantum state. This is called **superposition**.

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization

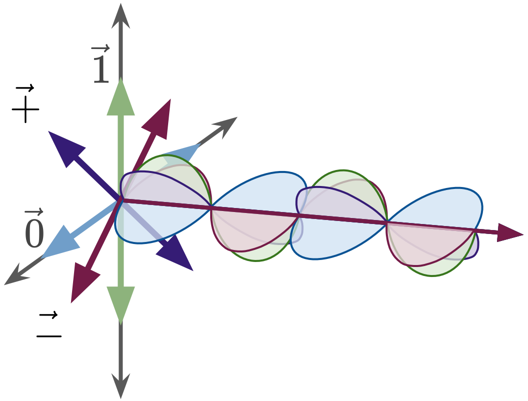



The **qubit** is the basic unit of **quantum information**.

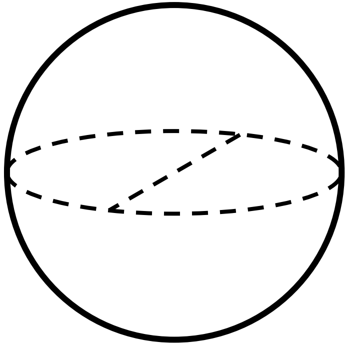
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization




Electron Spin



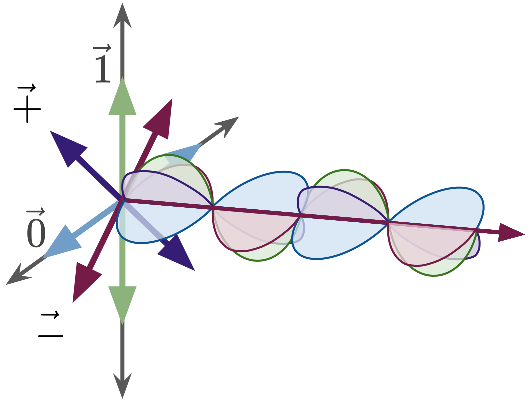
The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

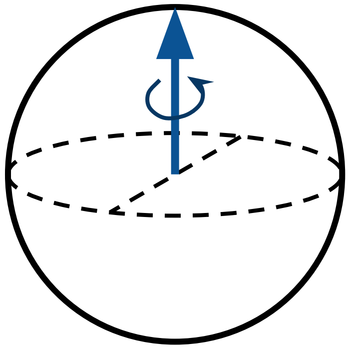
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization




Electron Spin



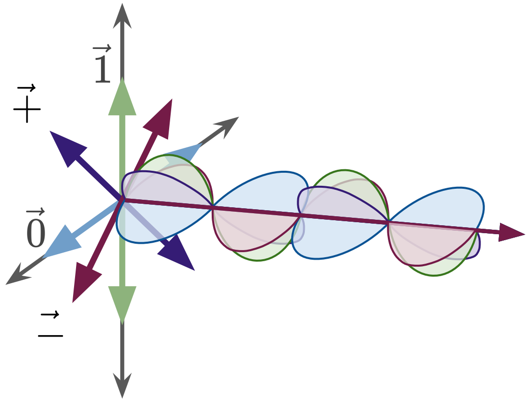
The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

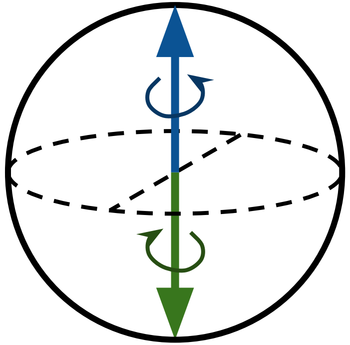
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization




Electron Spin

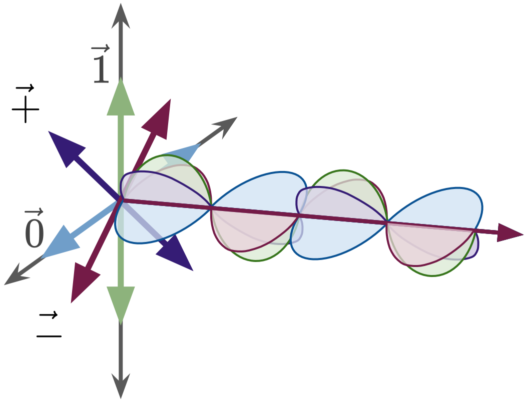


The **qubit** is the basic unit of **quantum information**.

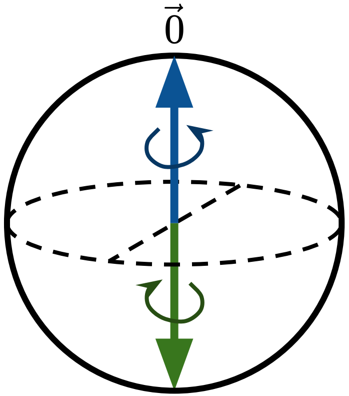
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization




Electron Spin

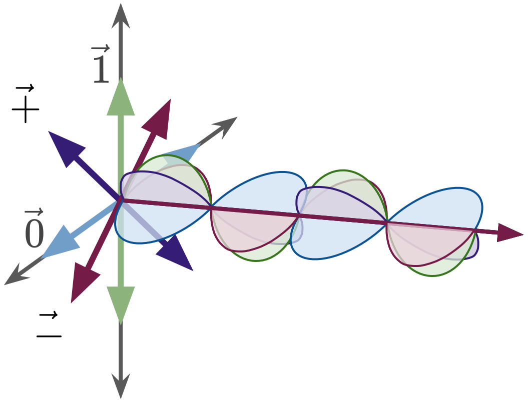



The **qubit** is the basic unit of **quantum information**.

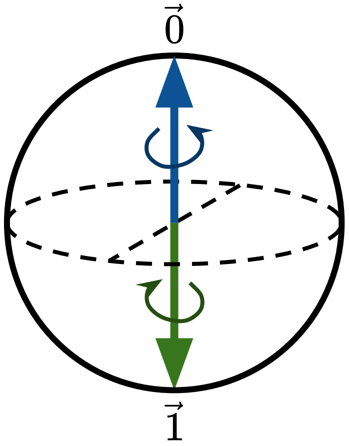
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization




Electron Spin

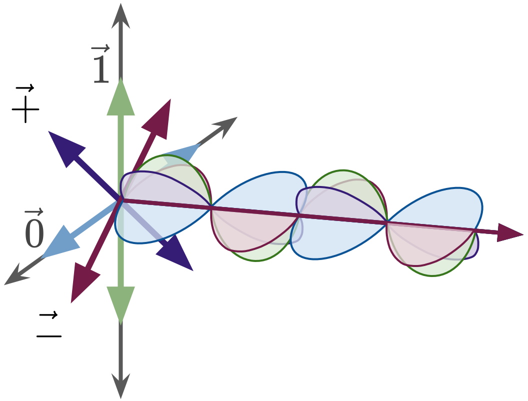



The **qubit** is the basic unit of **quantum information**.

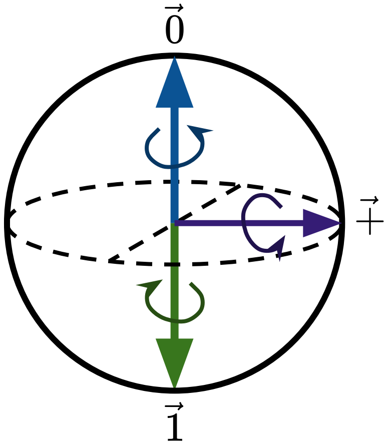
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization




Electron Spin

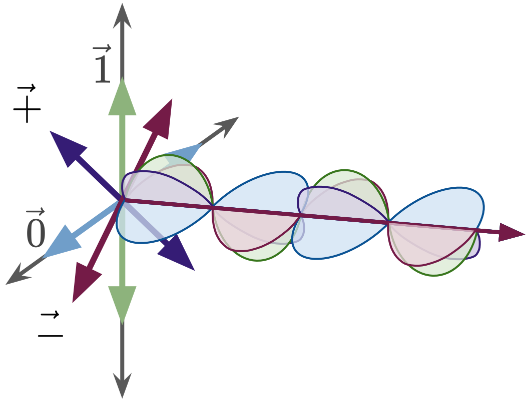



The **qubit** is the basic unit of **quantum information**.

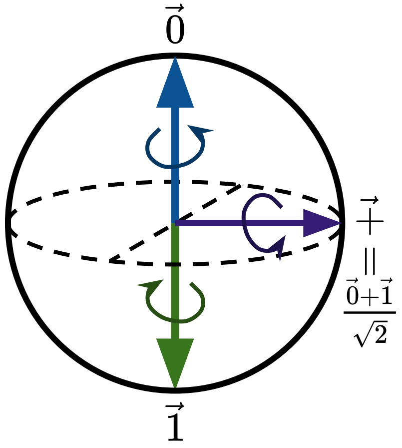
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization



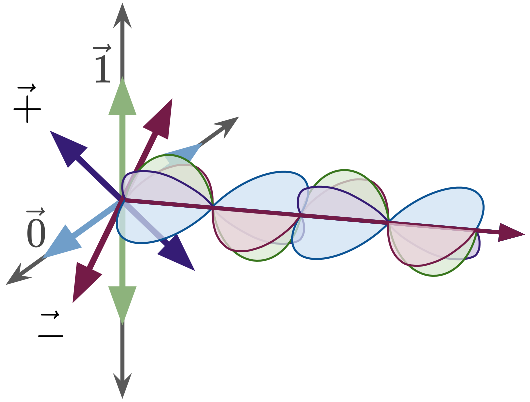

Electron Spin

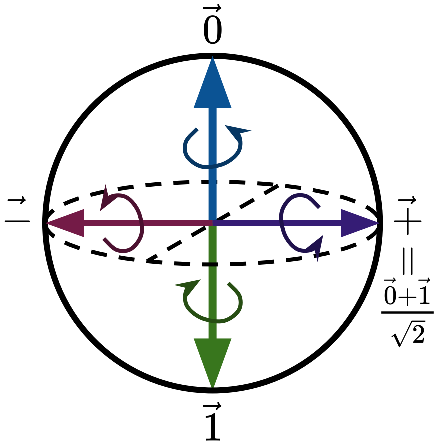



The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*



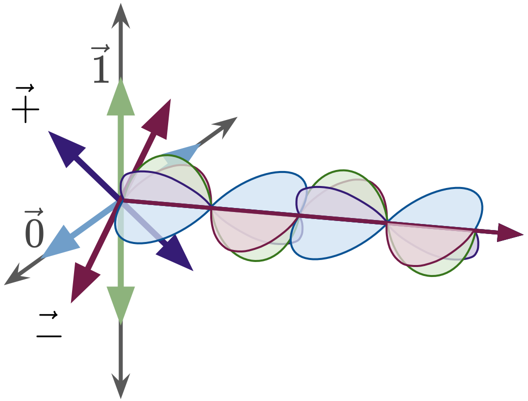

The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

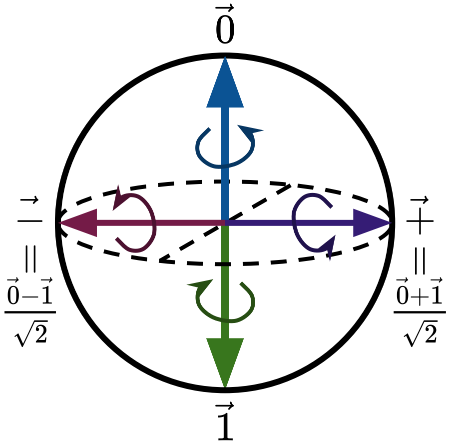
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Examples of Qubits: *Qubits are everywhere!*

Light Polarization




Electron Spin

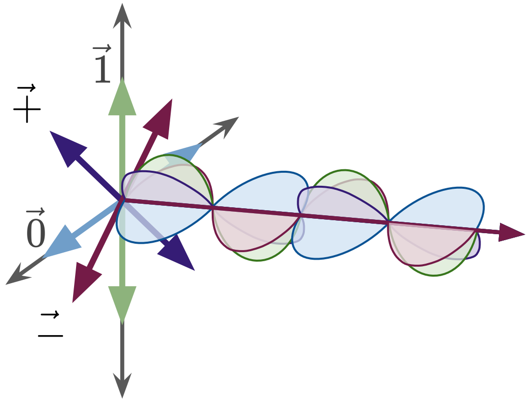



The **qubit** is the basic unit of **quantum information**.

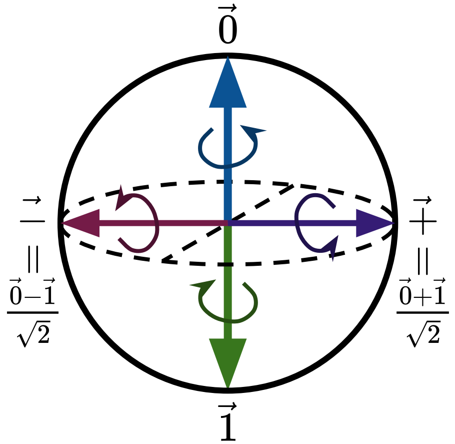
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

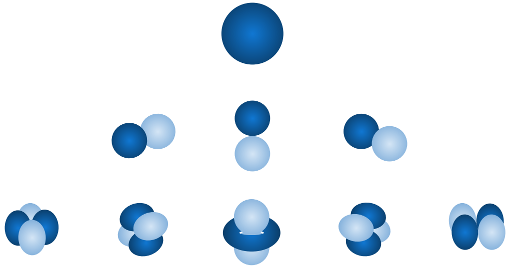
Light Polarization




Electron Spin




Electron Orbitals

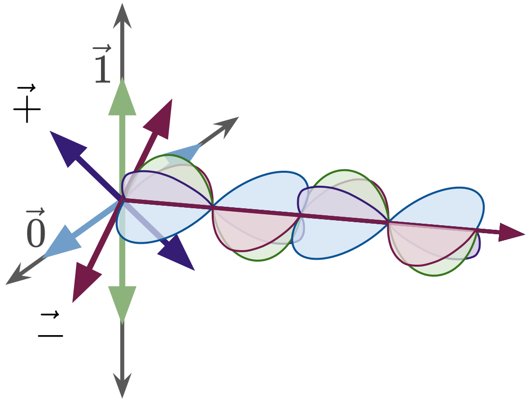


The **qubit** is the basic unit of **quantum information**.

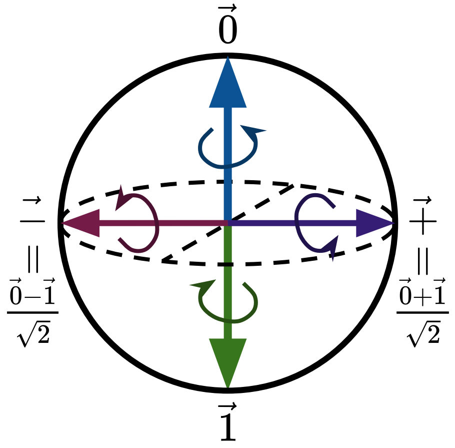
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

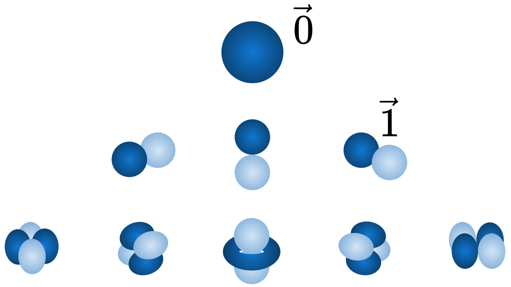
Light Polarization




Electron Spin




Electron Orbitals

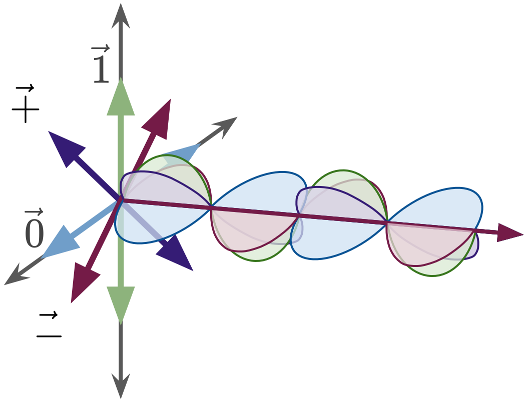



The **qubit** is the basic unit of **quantum information**.

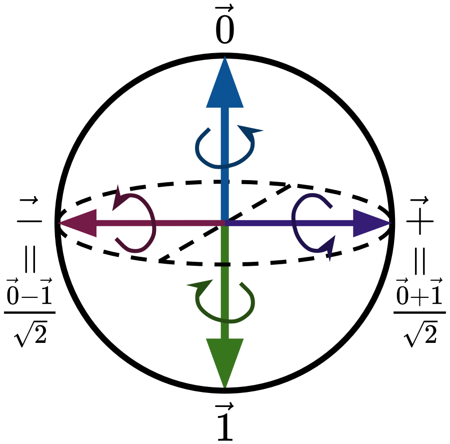
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

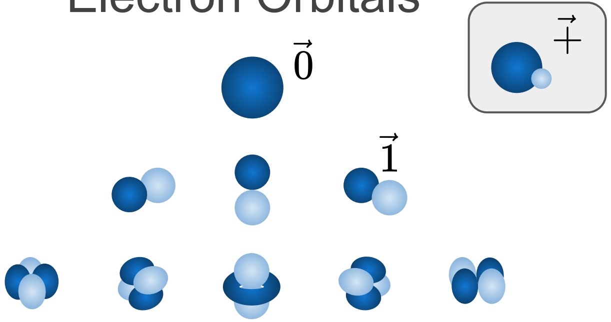
Light Polarization




Electron Spin




Electron Orbitals

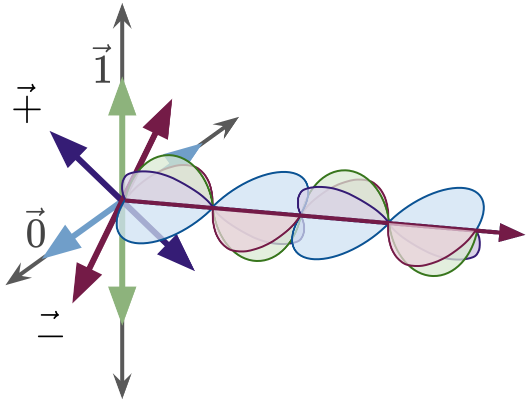



The **qubit** is the basic unit of **quantum information**.

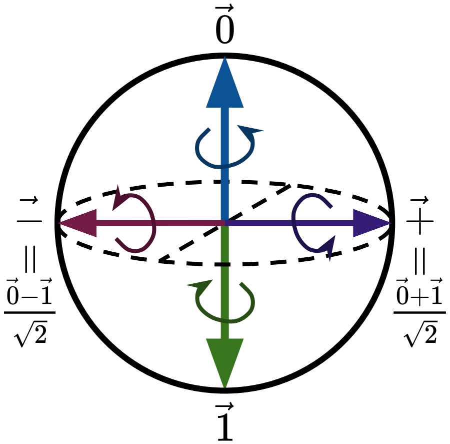
It is a quantum state on **any two-level system**.

# Examples of Qubits: *Qubits are everywhere!*

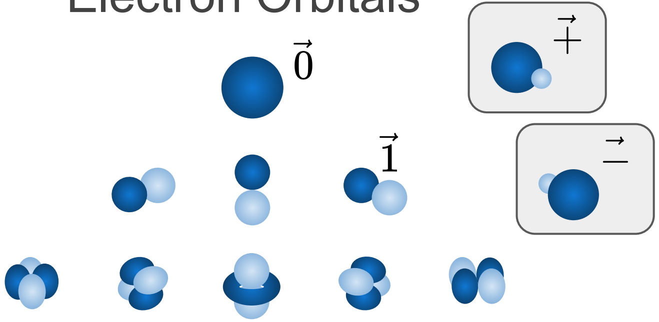
### Light Polarization




### Electron Spin




### Electron Orbitals



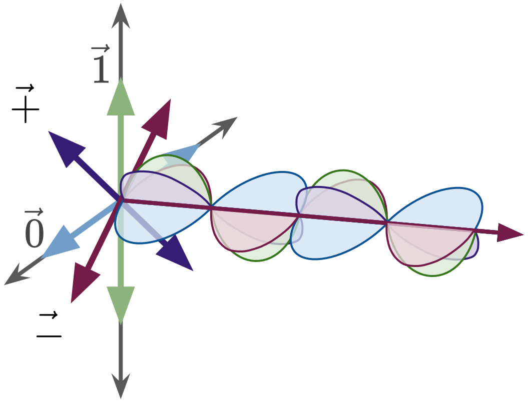

The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

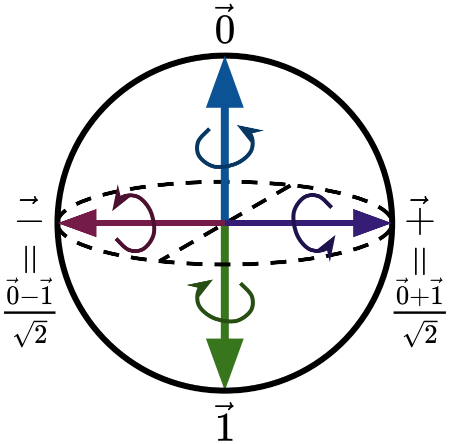
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Examples of Qubits: *Qubits are everywhere!*

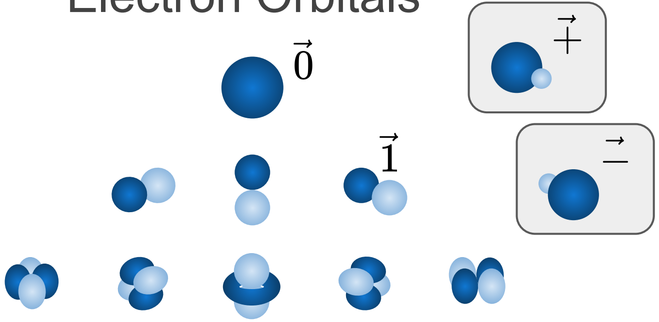
Light Polarization



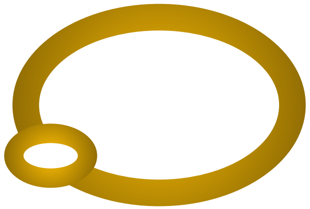

Electron Spin




Electron Orbitals




Superconducting Currents



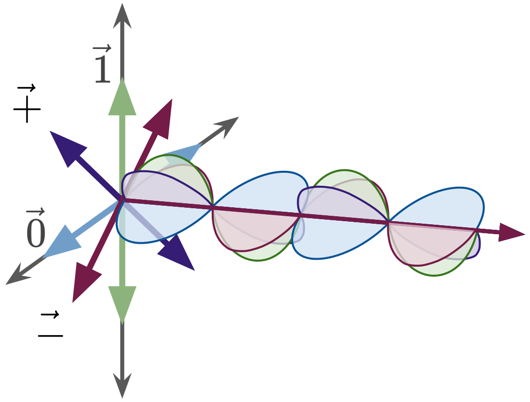
The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

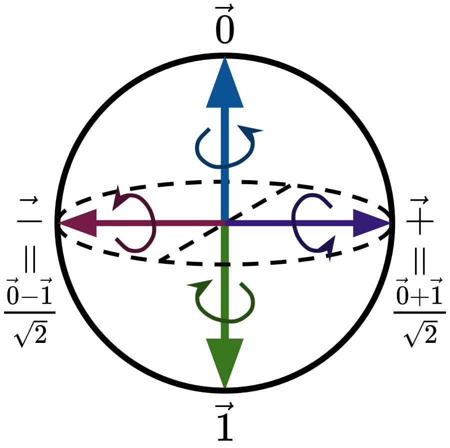
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Examples of Qubits: *Qubits are everywhere!*

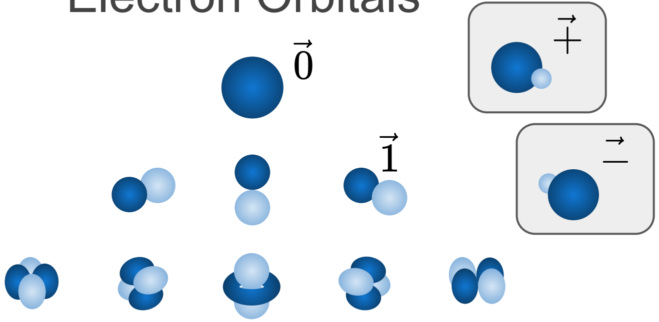
### Light Polarization



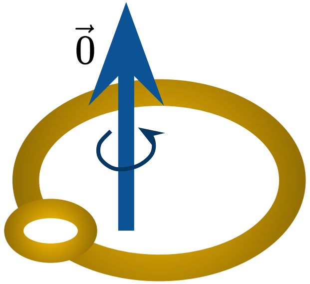

### Electron Spin




### Electron Orbitals




### Superconducting Currents



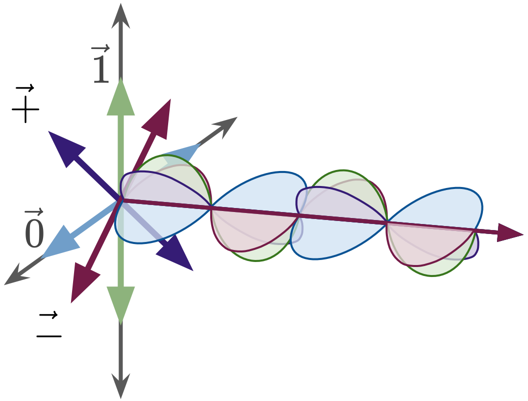

The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

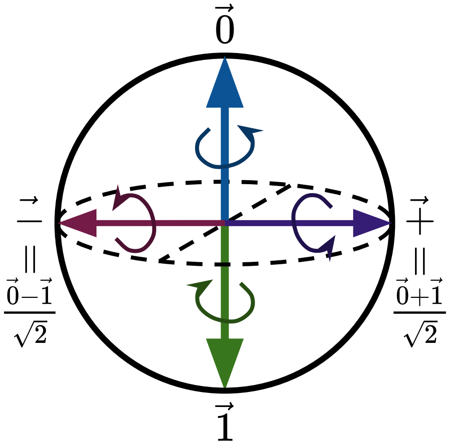
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Examples of Qubits: *Qubits are everywhere!*

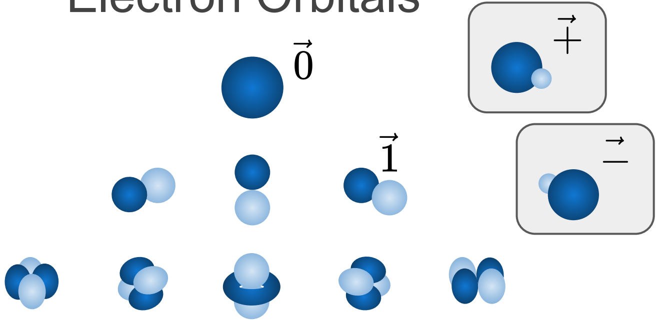
## Light Polarization



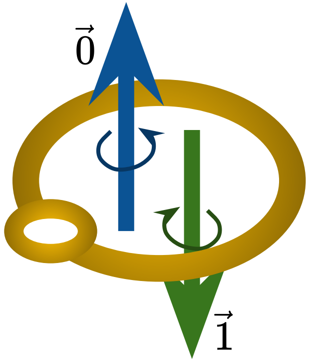

## Electron Spin




## Electron Orbitals




## Superconducting Currents



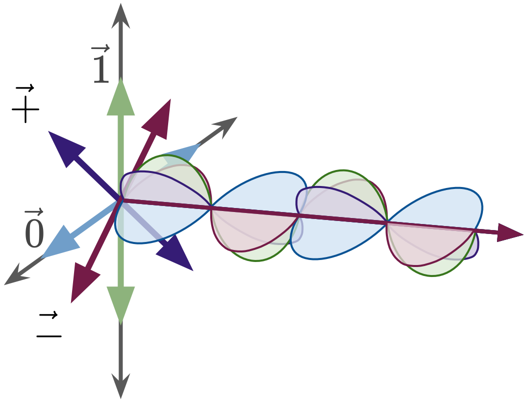

The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

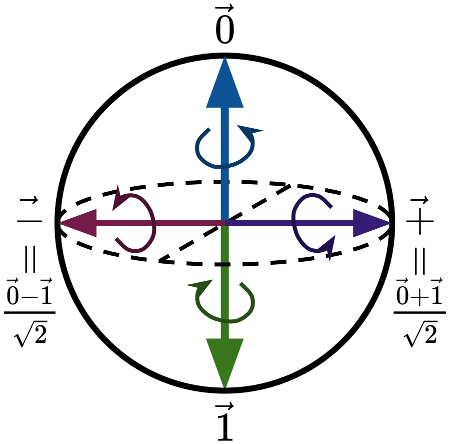
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Examples of Qubits: *Qubits are everywhere!*

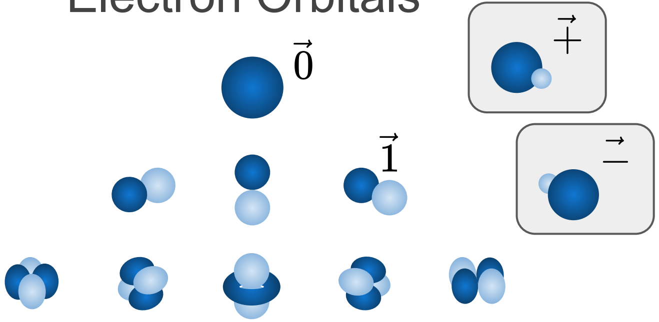
### Light Polarization



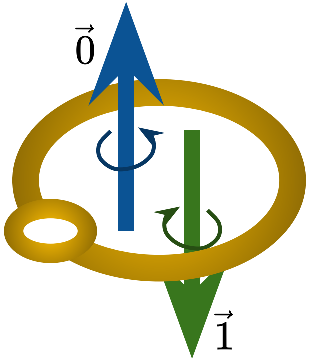

### Electron Spin




### Electron Orbitals




### Superconducting Currents



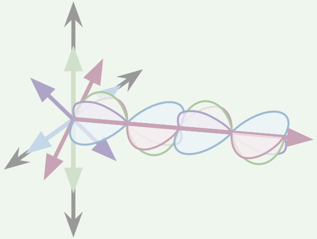

The **qubit** is the basic unit of **quantum information**.

It is a quantum state on **any two-level system**.

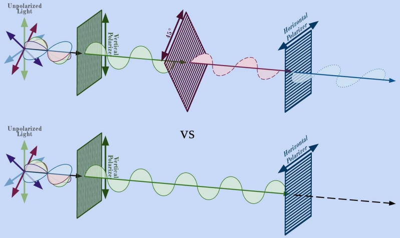
**We abstract a qubit as a unit vector on a 2D space.**

# Outline

1 The Qubit



2 Quantum Measurement

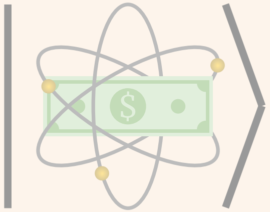



3 Quantum Entanglement & Many Qubits

First qubit Second qubit

$$\frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

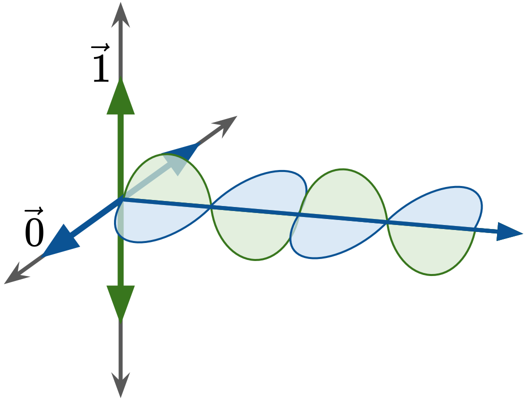
4 No Cloning and Quantum Money

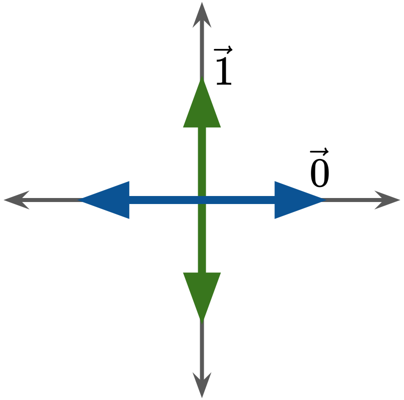


Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Measurement



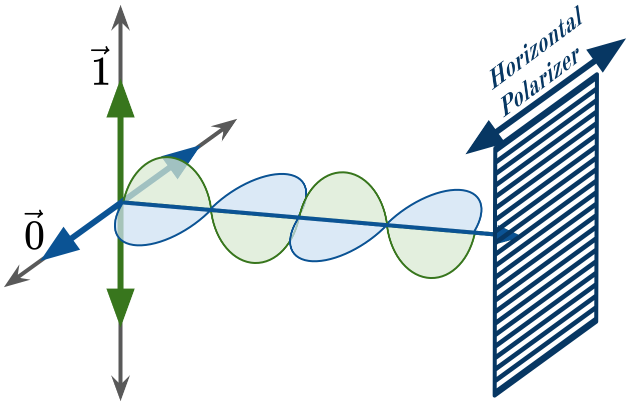



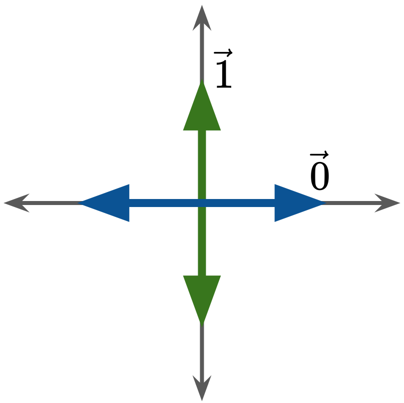

Suppose we have a **single photon** in *either* the **0 state** or the **1 state**, and we don't know which. How do we find out?

Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Measurement

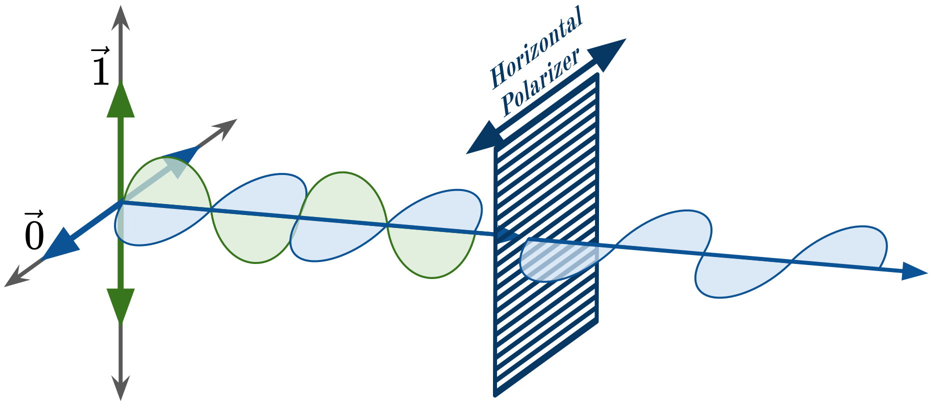


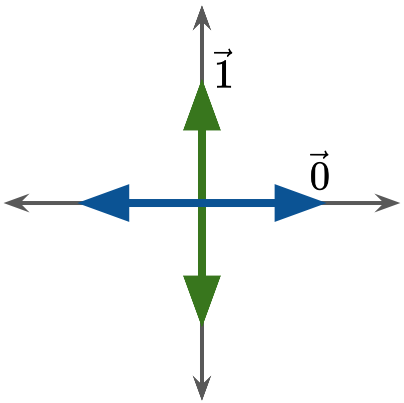




Suppose we have a **single photon** in *either* the **0 state** or the **1 state**, and we don't know which. How do we find out?

We send it through a **polarizing filter** (a.k.a. a **polarizer**)

# Quantum Measurement



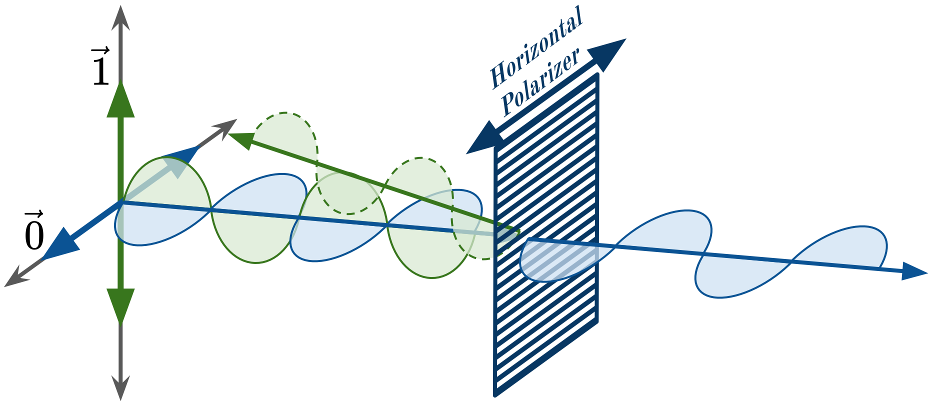



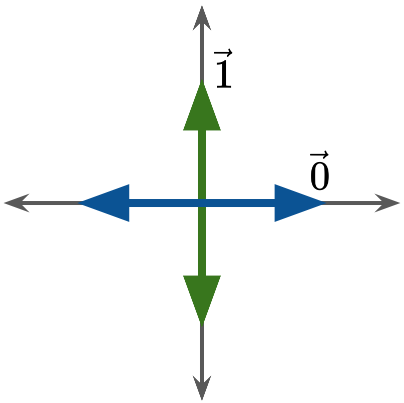

Suppose we have a **single photon** in *either* the **0 state** or the **1 state**, and we don't know which. How do we find out?

We send it through a **polarizing filter** (a.k.a. a **polarizer**)

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

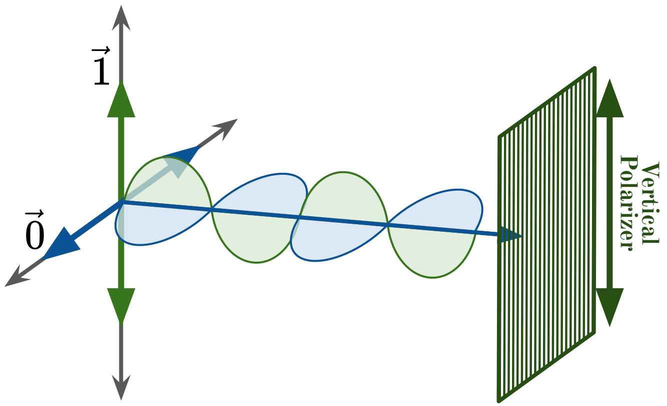


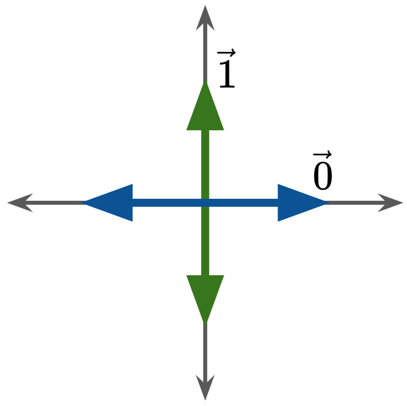




Suppose we have a **single photon** in *either* the **0 state** or the **1 state**, and we don't know which. How do we find out?

We send it through a **polarizing filter** (a.k.a. a **polarizer**)

# Quantum Measurement



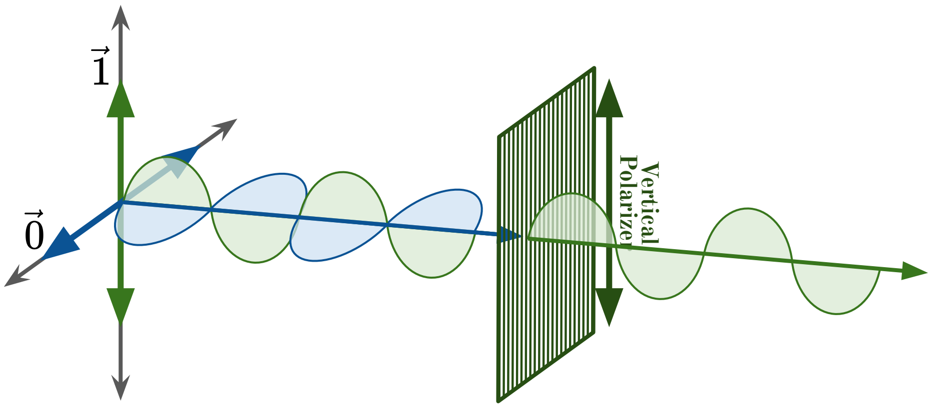



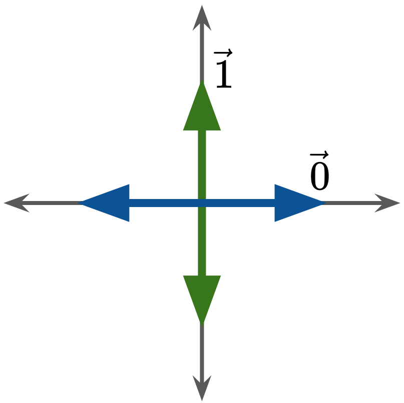

Suppose we have a **single photon** in *either* the **0 state** or the **1 state**, and we don't know which. How do we find out?

We send it through a **polarizing filter** (a.k.a. a **polarizer**)

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

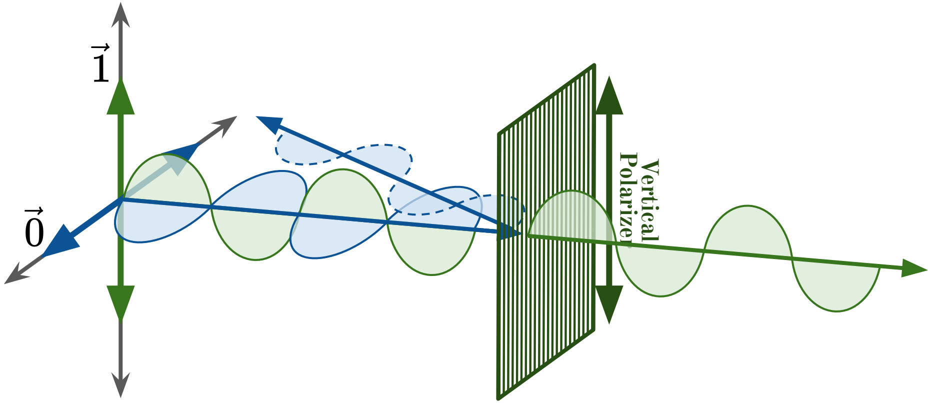


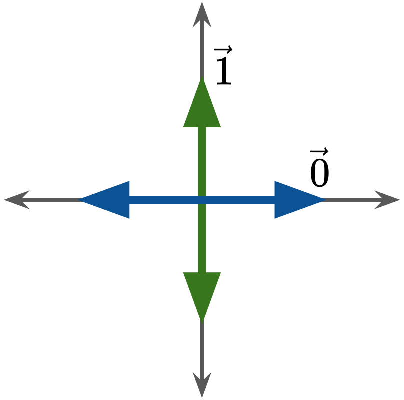




Suppose we have a **single photon** in *either* the **0 state** or the **1 state**, and we don't know which. How do we find out?

We send it through a **polarizing filter** (a.k.a. a **polarizer**)

# Quantum Measurement

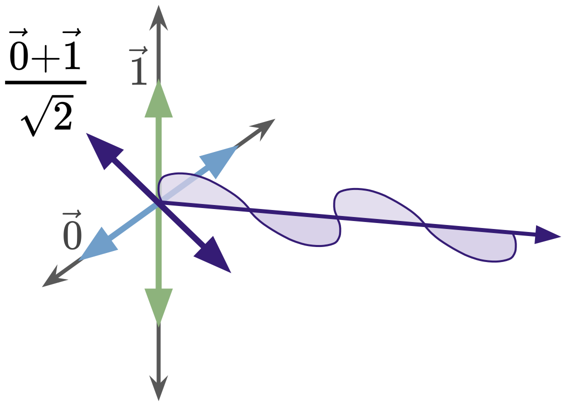


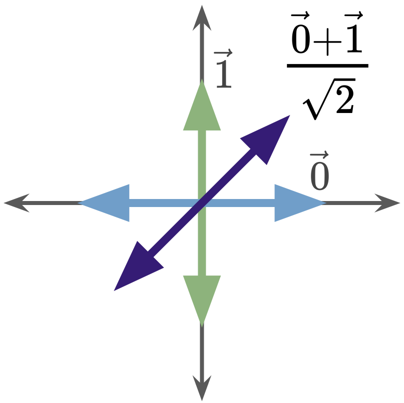




Suppose we have a **single photon** in *either* the **0 state** or the **1 state**, and we don't know which. How do we find out?

We send it through a **polarizing filter** (a.k.a. a **polarizer**)

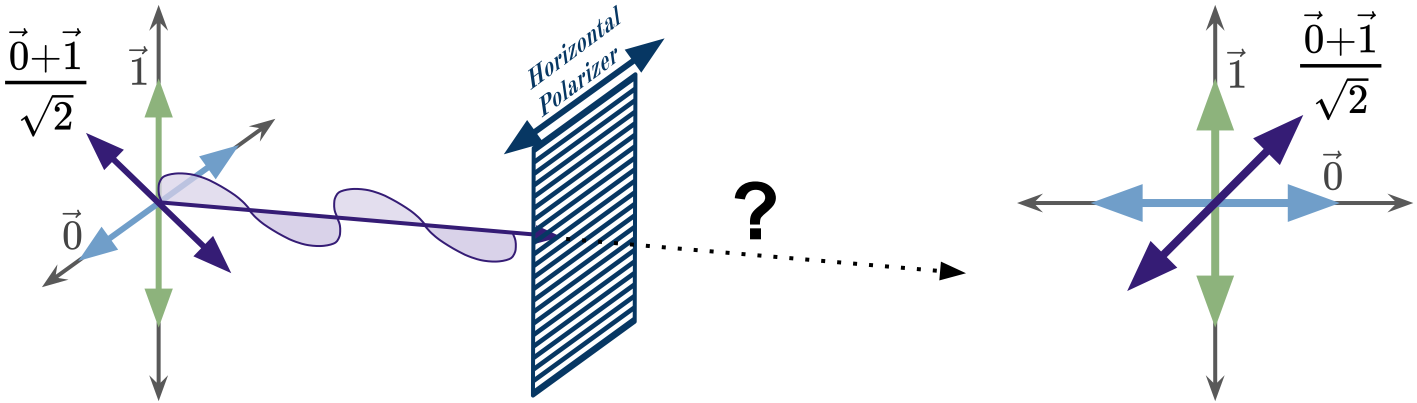
# Quantum Measurement




What happens if we send a **single photon** in the **+ state**...

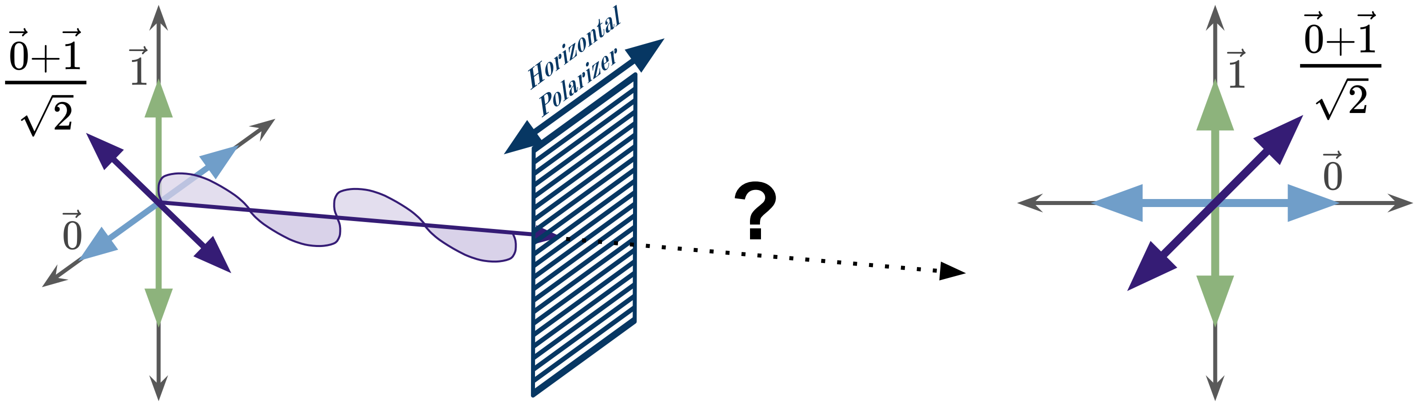
# Quantum Measurement




What happens if we send a **single photon** in the **+ state** through a **horizontal polarizer**?

(a) It **reflects** off the polarizer
(b) It **passes through** the polarizer
(c) It changes its polarization to **vertical**
(d) It changes its polarization to **horizontal**

# Quantum Measurement

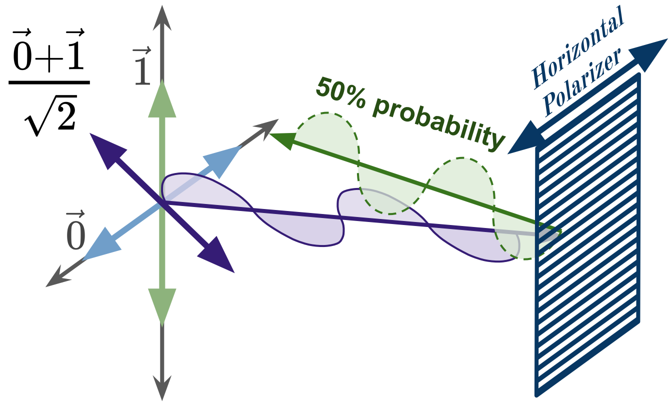


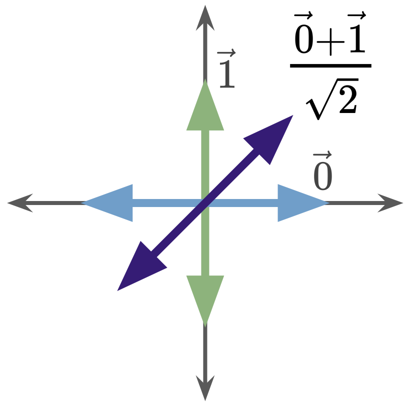

What happens if we send a **single photon** in the **+ state** through a **horizontal polarizer**?

(a) It **reflects** off the polarizer
(b) It **passes through** the polarizer
(c) It changes its polarization to **vertical**
(d) It changes its polarization to **horizontal**

?

# Quantum Measurement



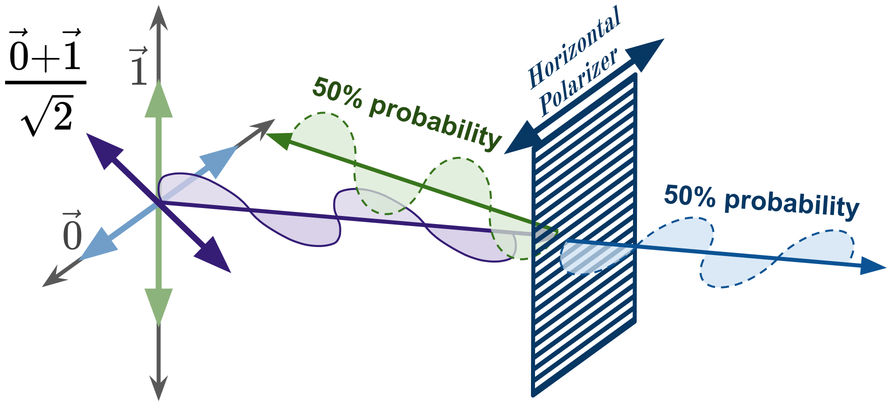

What happens if we send a **single photon** in the **+ state** through a **horizontal polarizer**?

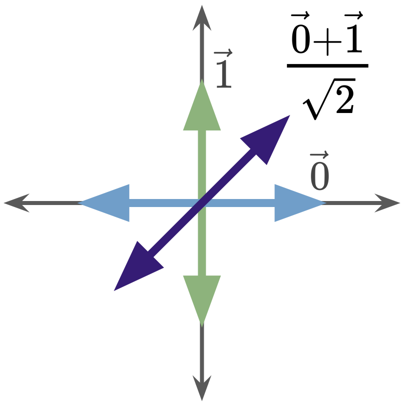
(a) It **reflects** off the polarizer
(b) It **passes through** the polarizer
(c) It changes its polarization to **vertical**
(d) It changes its polarization to **horizontal**

**50% probability**

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement




What happens if we send a **single photon** in the **+ state** through a **horizontal polarizer**?

(a) It **reflects** off the polarizer

(b) It **passes through** the polarizer

(c) It changes its polarization to **vertical**

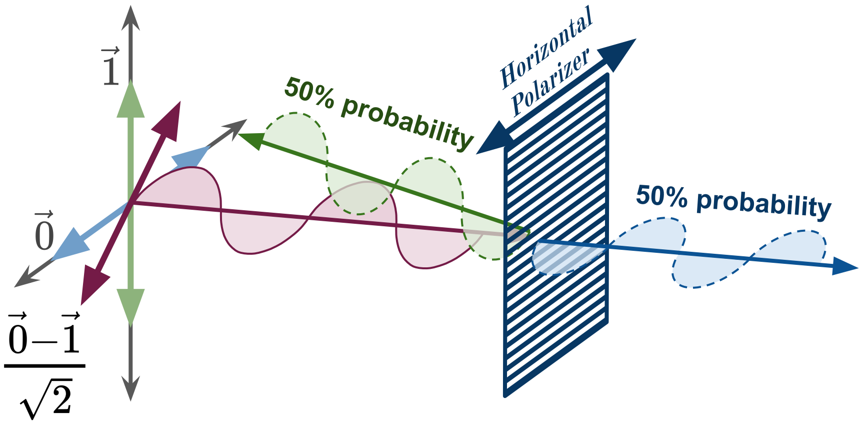
(d) It changes its polarization to **horizontal**

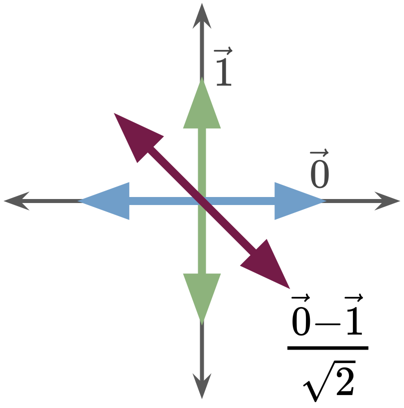
**50% probability**

**50% probability**

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement




What happens if we send a **single photon** in the **– state** through a **horizontal polarizer**?

(a) It **reflects** off the polarizer

(b) It **passes through** the polarizer

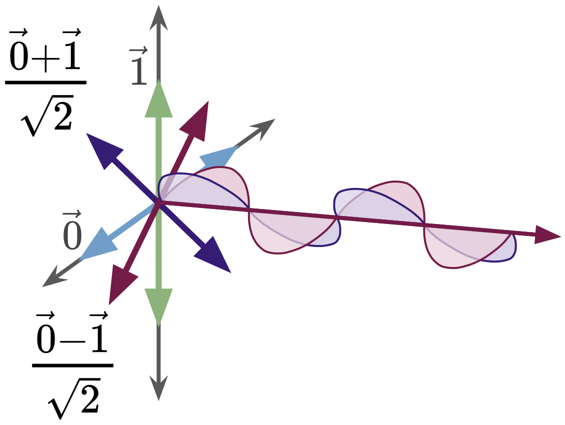
(c) It changes its polarization to **vertical**

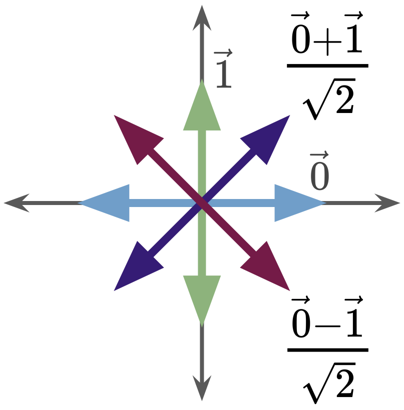
(d) It changes its polarization to **horizontal**

**50% probability**

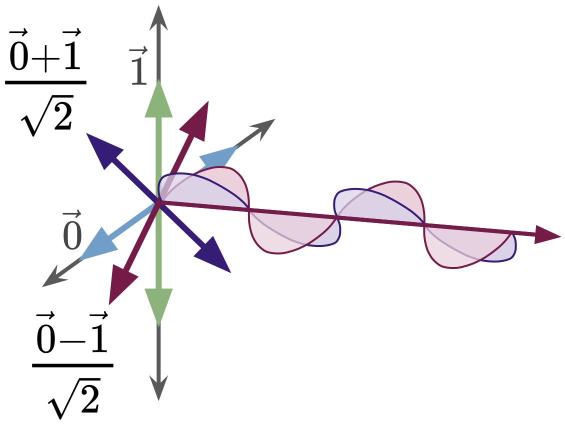
**50% probability**

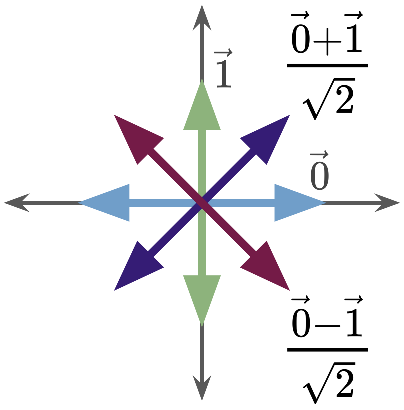
# Quantum Measurement



# Quantum Measurement

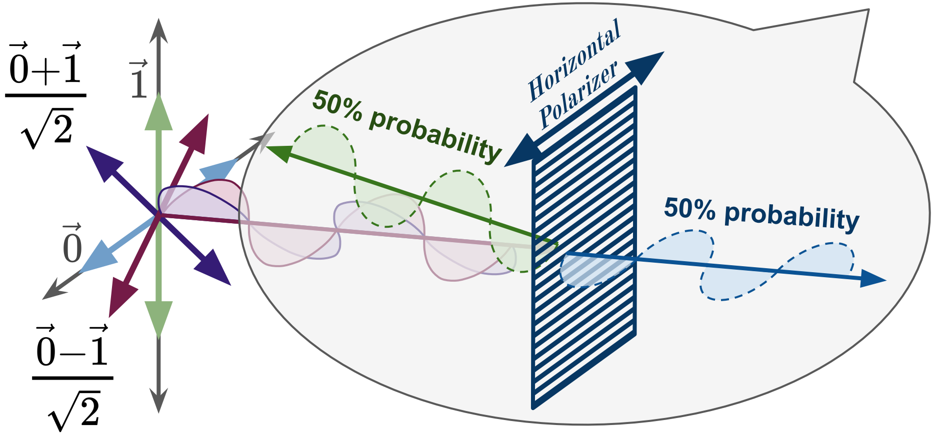


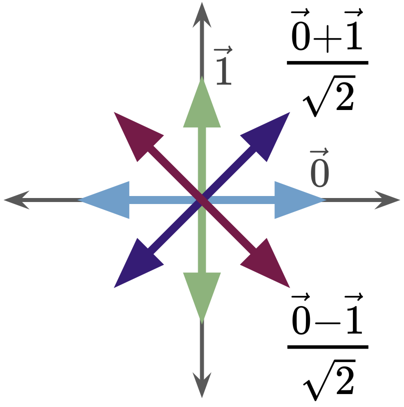




Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.
**Can we distinguish** between the two diagonal polarizations?

# Quantum Measurement

*A horizontal polarizer does not distinguish!*

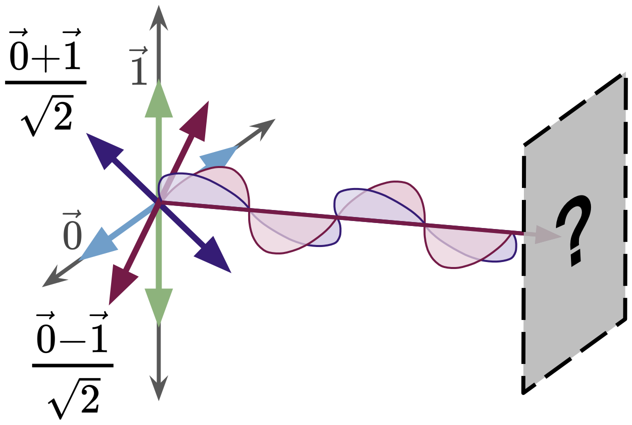


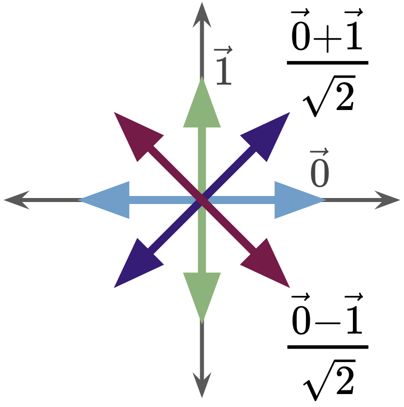




Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

**Can we distinguish** between the two diagonal polarizations?

# Quantum Measurement



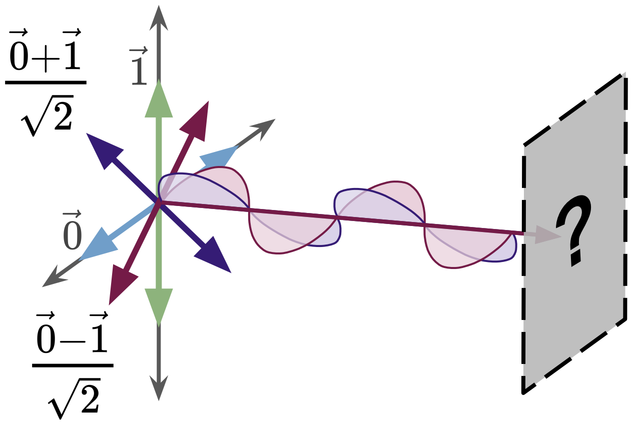

Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

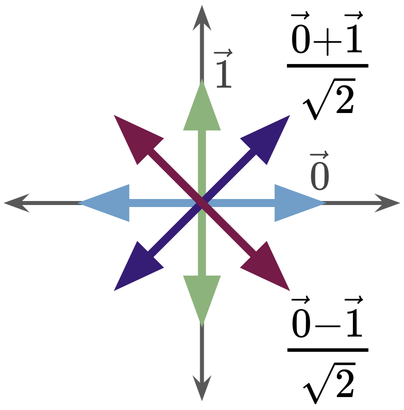
**Can we distinguish** between the two diagonal polarizations?

(a) **No.** The two diagonals are indistinguishable.

(b) **Yes!** There is a polarizer measurement that can tell them apart!

# Quantum Measurement



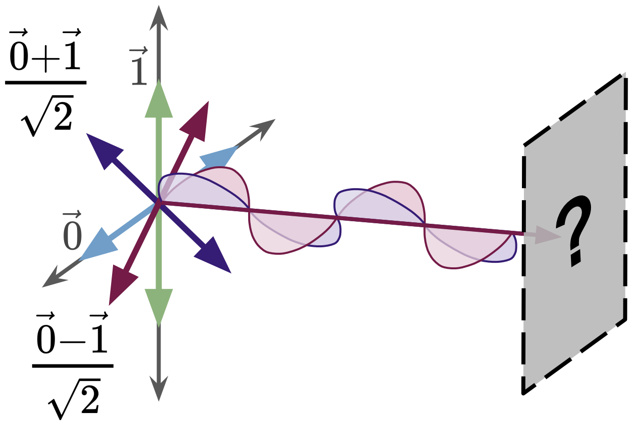

Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

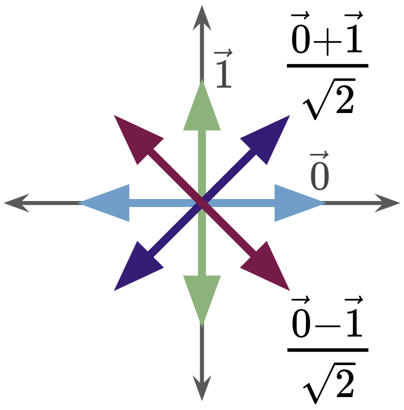
**Can we distinguish** between the two diagonal polarizations?

(a) **No.** The two diagonals are indistinguishable.

(b) **Yes!** There is a polarizer measurement that can tell them apart!

# Quantum Measurement




Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

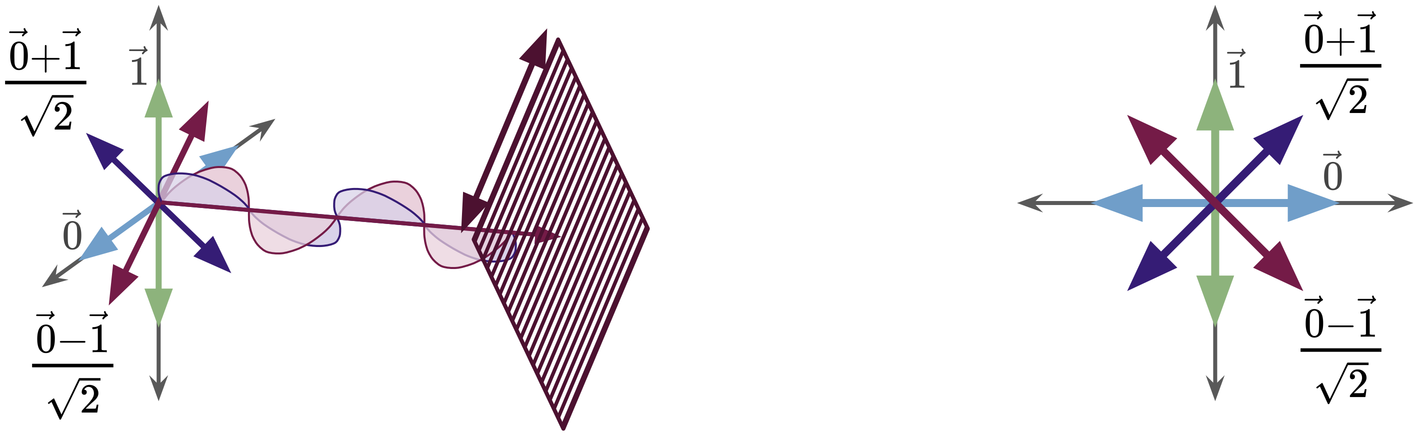
**Can we distinguish** between the two diagonal polarizations?

(a) **No.** The two diagonals are indistinguishable.

(b) **Yes!** There is a polarizer measurement that can tell them apart!

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Measurement




Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

**Can we distinguish** between the two diagonal polarizations?

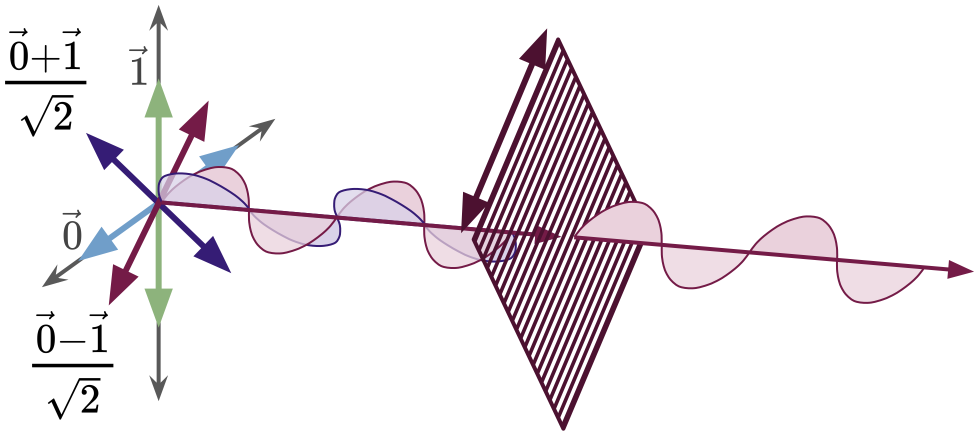
(a) **No.** The two diagonals are indistinguishable.

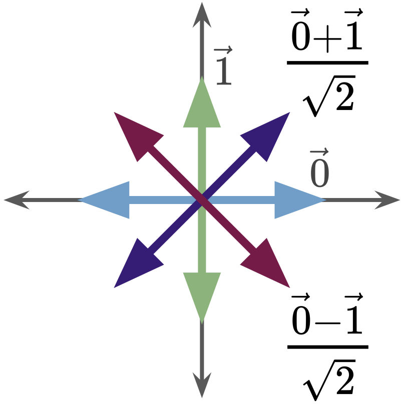
(b) **Yes!** There is a polarizer measurement that can tell them apart!

**Just tilt the polarizer!** This is also a valid measurement

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement




Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

**Can we distinguish** between the two diagonal polarizations?

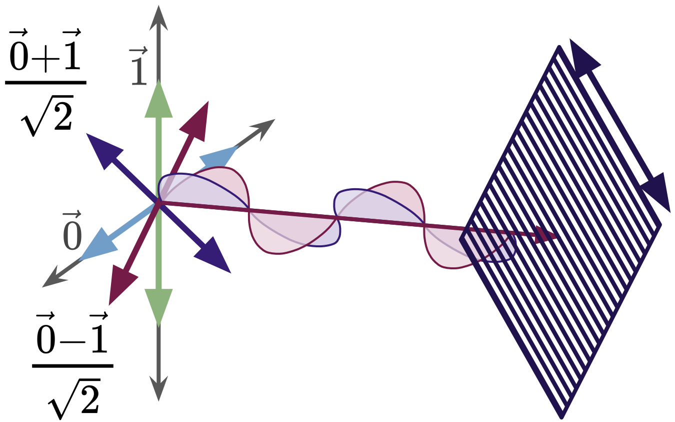
(a) **No.** The two diagonals are indistinguishable.

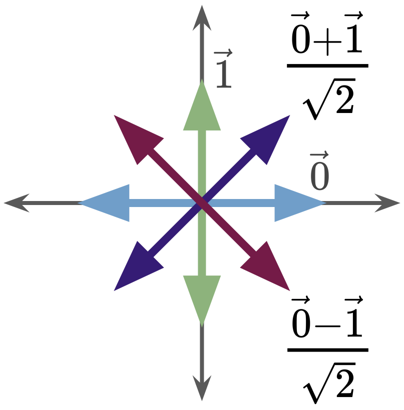
(b) **Yes!** There is a polarizer measurement that can tell them apart!

**Just tilt the polarizer!** This is also a valid measurement

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement




Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

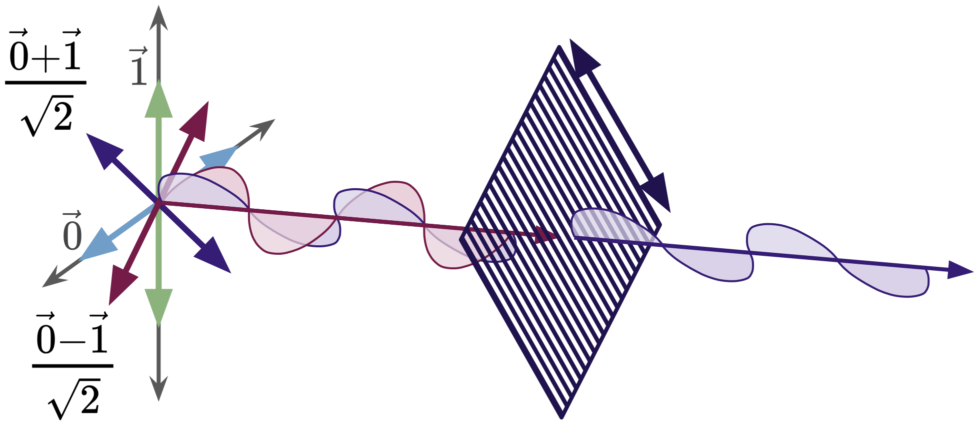
**Can we distinguish** between the two diagonal polarizations?

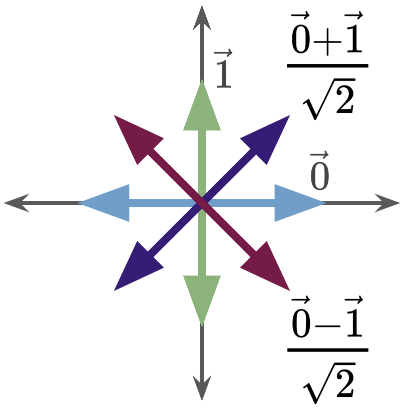
(a) **No.** The two diagonals are indistinguishable.

(b) **Yes!** There is a polarizer measurement that can tell them apart!

**Just tilt the polarizer!** This is also a valid measurement

# Quantum Measurement




Suppose we have a **single photon** in *either* the **+ state** or the **– state**, and we don't know which.

**Can we distinguish** between the two diagonal polarizations?

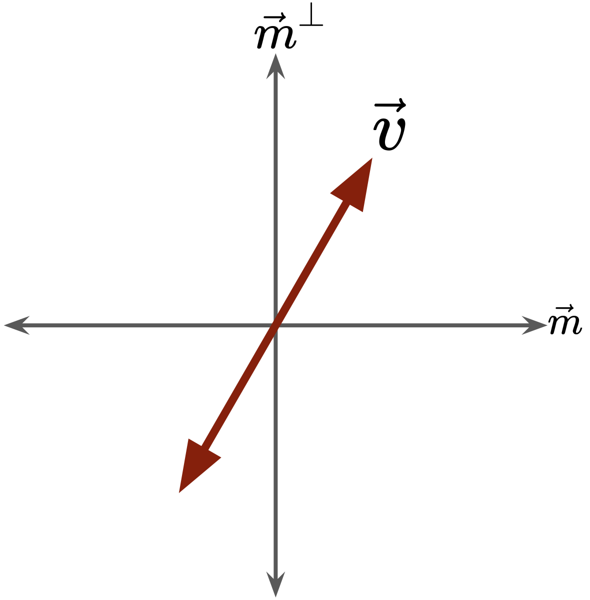
(a) **No.** The two diagonals are indistinguishable.

(b) **Yes!** There is a polarizer measurement that can tell them apart!

**Just tilt the polarizer!** This is also a valid measurement

# Quantum Measurement

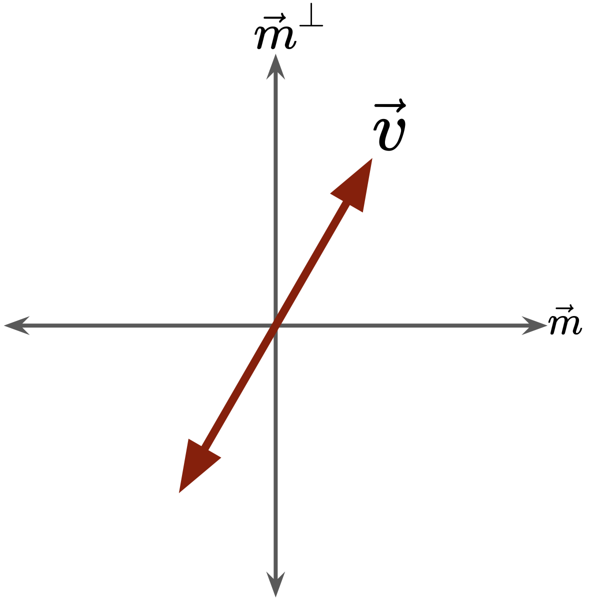
**Rule**:




(this view is rotated to depict m along the horizontal)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:



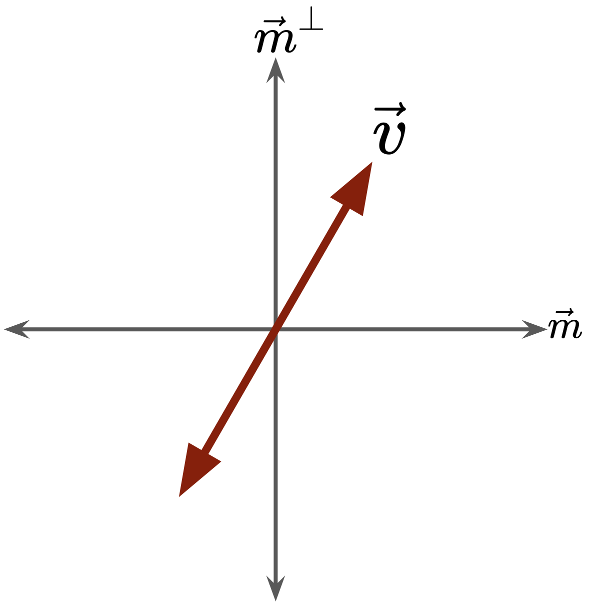

(this view is rotated to depict m along the horizontal)

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$



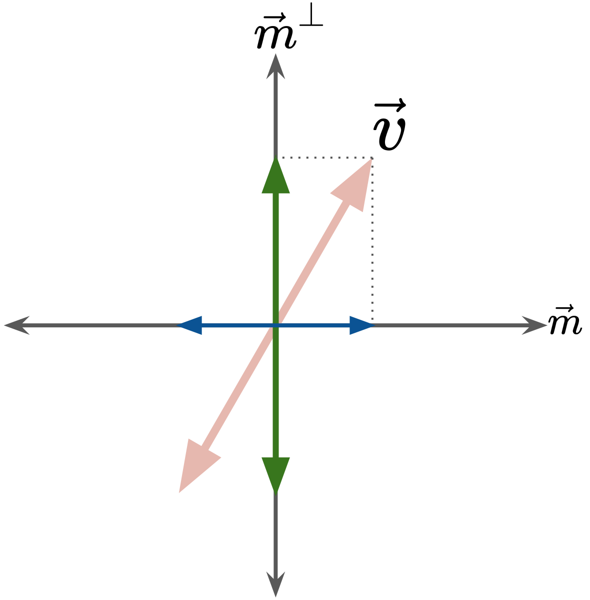

(this view is rotated to depict m along the horizontal)

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$




(this view is rotated to depict m along the horizontal)

Barak Nehoran (Postdoc, CS Department, Columbia University)

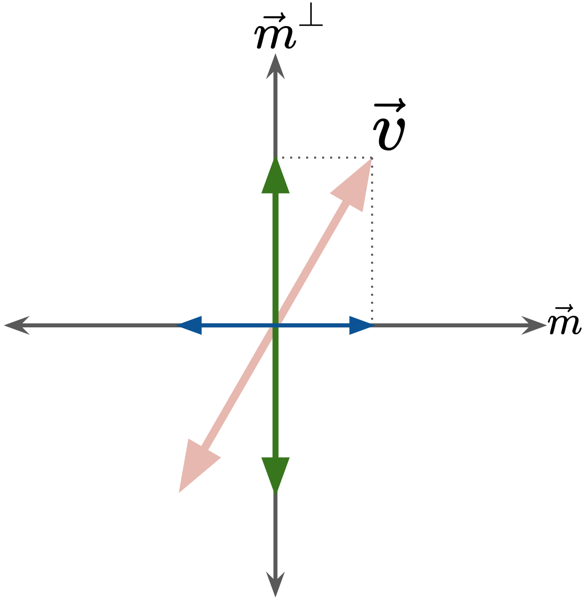
# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

$$|\langle \vec{m}, \vec{v} \rangle|^2$$



(this view is rotated to depict m along the horizontal)

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

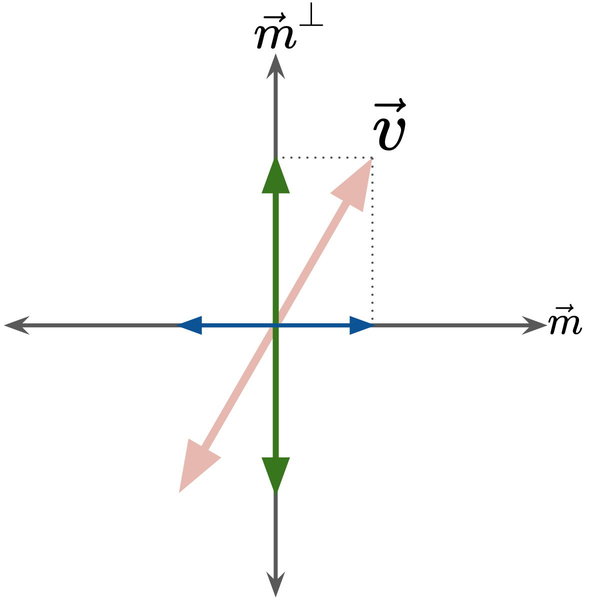
**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

$$|\langle \vec{m}, \vec{v} \rangle|^2$$

(This is the squared component in the direction of $\vec{m}$)




(this view is rotated to depict m along the horizontal)

# Quantum Measurement

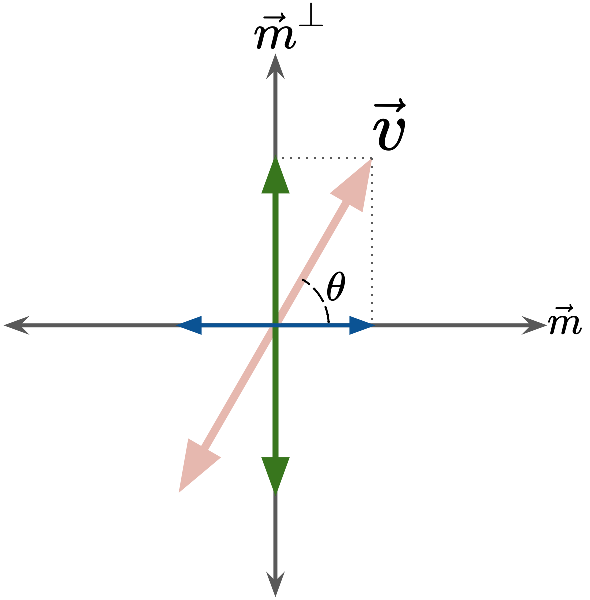
**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^\perp$

The probability of measuring $\vec{m}$ is

$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)




(this view is rotated to depict m along the horizontal)

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

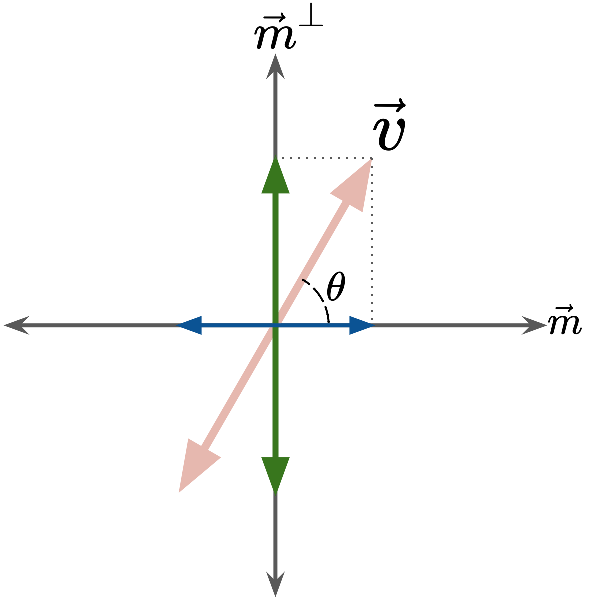
Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

In that case, the state *is* now $\vec{m}$ !



(this view is rotated to depict m along the horizontal)

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

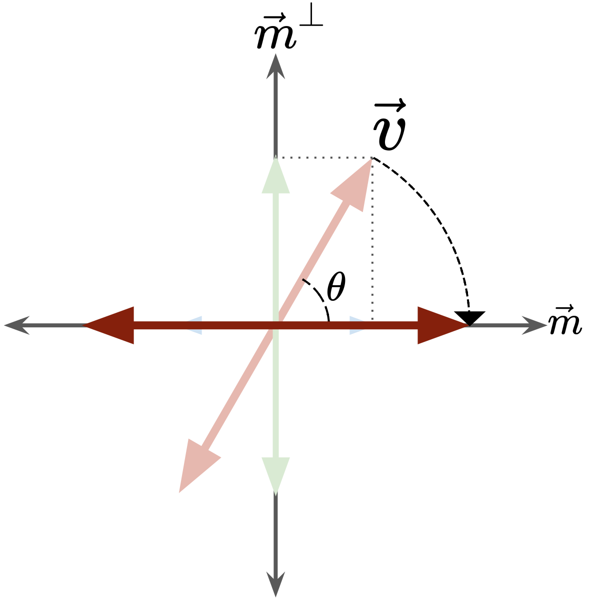
Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

$$|\langle\vec{m},\vec{v}\rangle|^2 = \cos^2\theta$$

(This is the squared component in the direction of $\vec{m}$)

In that case, the state *is* now $\vec{m}$ !



(this view is rotated to depict m along the horizontal)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

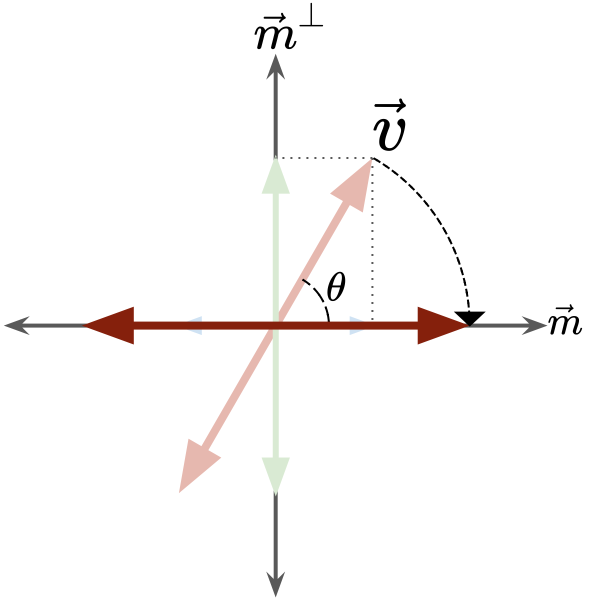
The probability of measuring $\vec{m}$ is

$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

In that case, the state ***is*** now $\vec{m}$ !

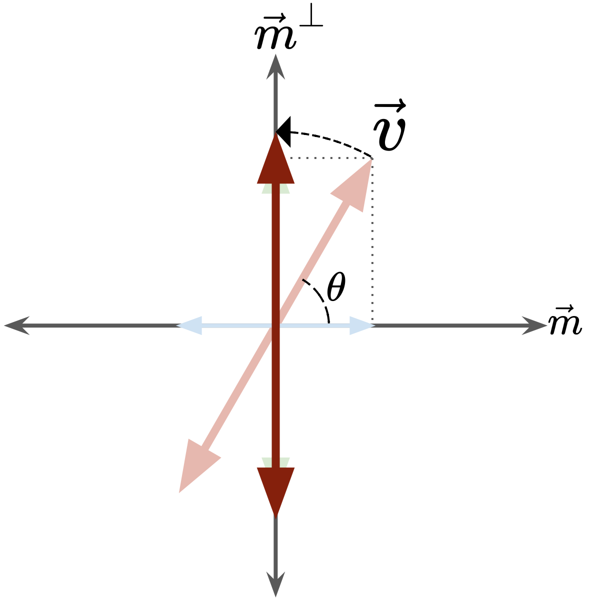
Otherwise, the state becomes the normalized projection onto $\vec{m}^{\perp}$ (with probability $|\langle \vec{m}^{\perp}, \vec{v} \rangle|^2 = \sin^2 \theta$ )



(this view is rotated to depict m along the horizontal)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:




(this view is rotated to depict m along the horizontal)

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

In that case, the state ***is*** now $\vec{m}$ !

Otherwise, the state becomes the normalized projection onto $\vec{m}^{\perp}$ (with probability $|\langle \vec{m}^{\perp}, \vec{v} \rangle|^2 = \sin^2 \theta$ )

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

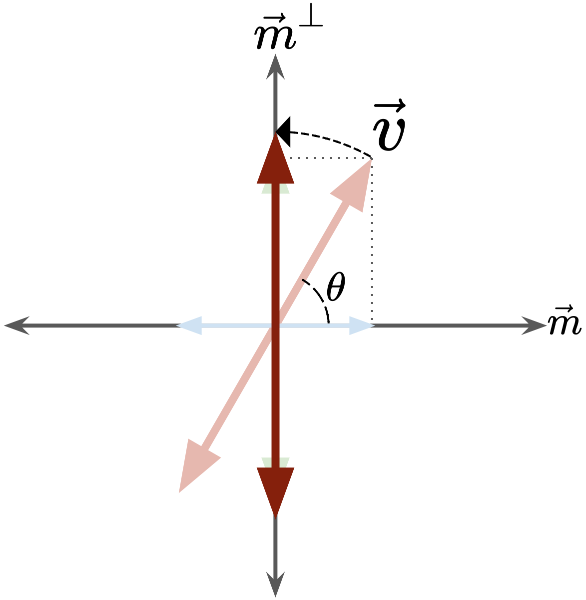
$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

In that case, the state ***is*** now $\vec{m}$ !

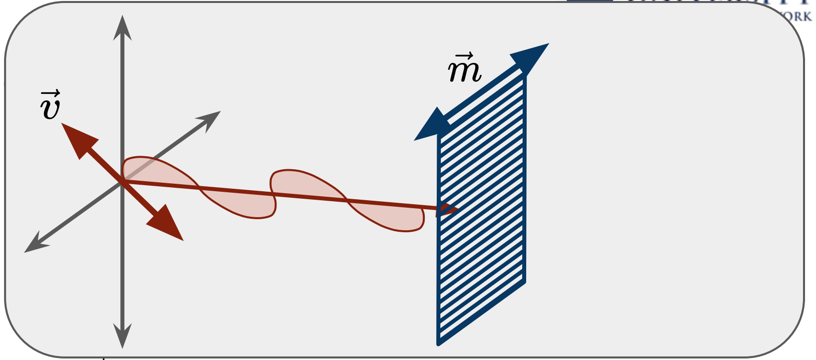
Either way, ***always*** ends up with norm 1.

Otherwise, the state becomes the normalized projection onto $\vec{m}^{\perp}$ (with probability $|\langle \vec{m}^{\perp}, \vec{v} \rangle|^2 = \sin^2 \theta$ )



(this view is rotated to depict m along the horizontal)

# Quantum Measurement




**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

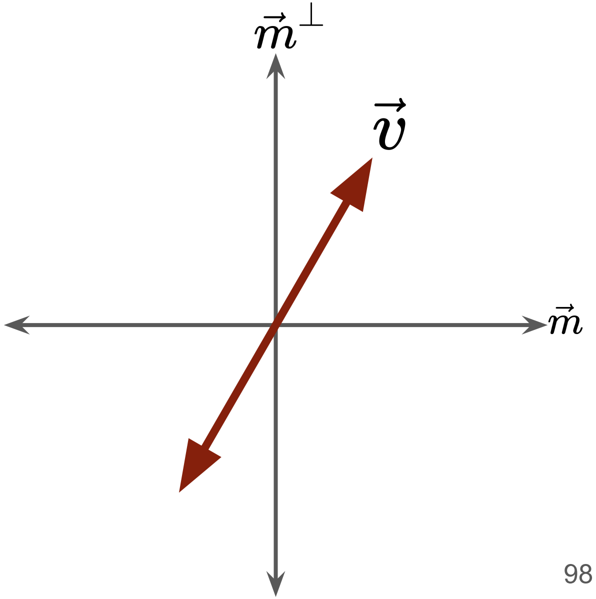
$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

In that case, the state ***is*** now $\vec{m}$ !

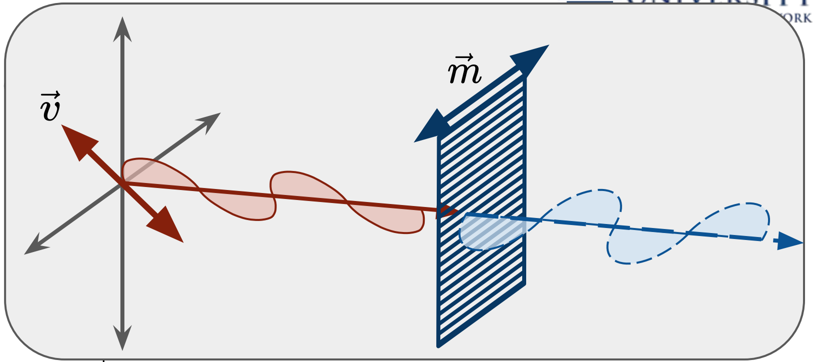
Either way, ***always*** ends up with norm 1.

Otherwise, the state becomes the normalized projection onto $\vec{m}^{\perp}$ (with probability $|\langle \vec{m}^{\perp}, \vec{v} \rangle|^2 = \sin^2 \theta$ )



Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement




**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

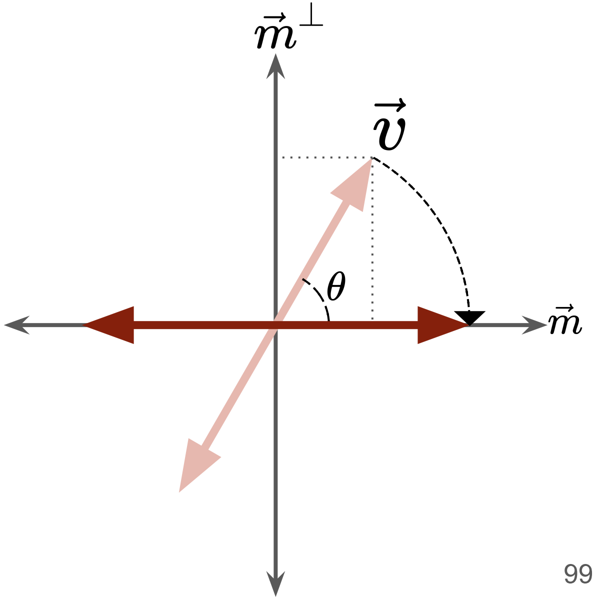
$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

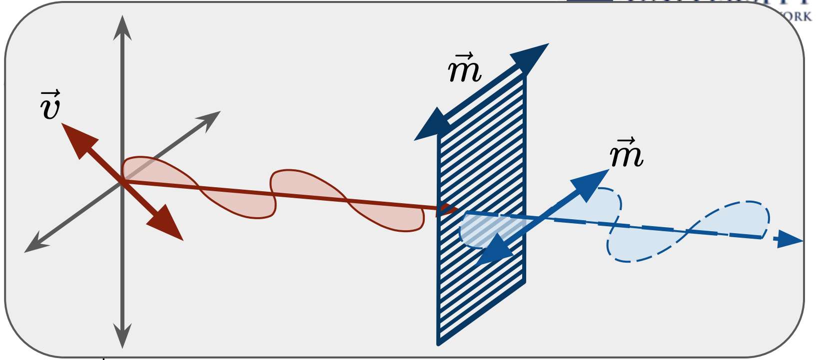
In that case, the state ***is*** now $\vec{m}$ !

Either way, ***always*** ends up with norm 1.

Otherwise, the state becomes the normalized projection onto $\vec{m}^{\perp}$ (with probability $|\langle \vec{m}^{\perp}, \vec{v} \rangle|^2 = \sin^2 \theta$ )



# Quantum Measurement




**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

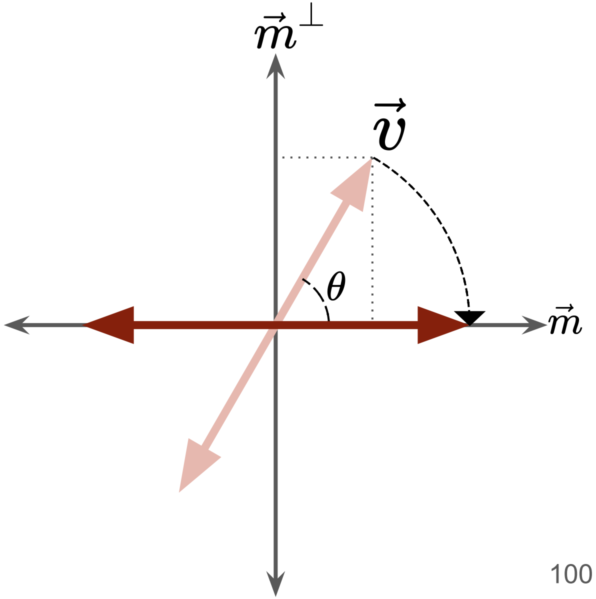
$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

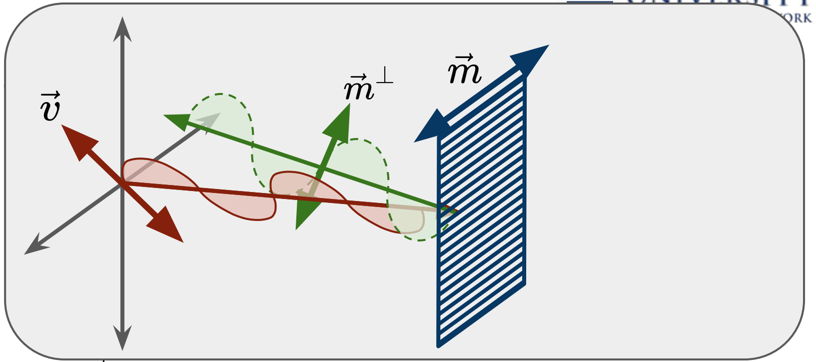
In that case, the state ***is*** now $\vec{m}$ !

Either way, ***always*** ends up with norm 1.

Otherwise, the state becomes the normalized projection onto $\vec{m}^{\perp}$ (with probability $|\langle \vec{m}^{\perp}, \vec{v} \rangle|^2 = \sin^2 \theta$ )



# Quantum Measurement




**Rule**: Given a state vector $\vec{v}$ , if you measure in direction $\vec{m}$:

Project $\vec{v}$ onto $\vec{m}$ and its perpendicular subspace $\vec{m}^{\perp}$

The probability of measuring $\vec{m}$ is

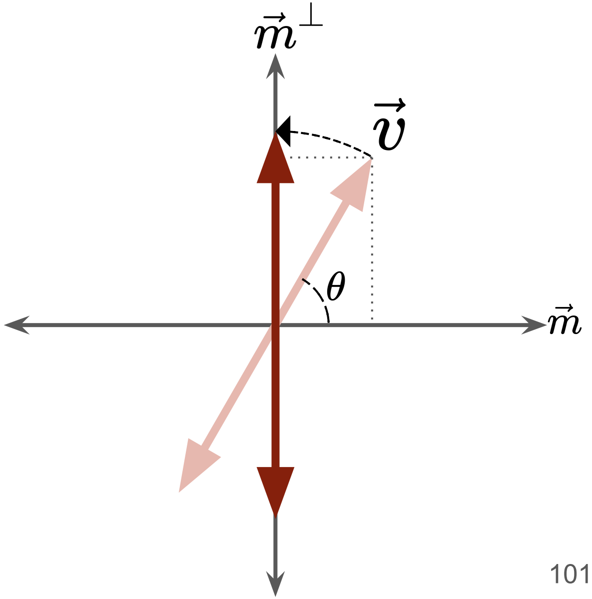
$$|\langle \vec{m}, \vec{v} \rangle|^2 = \cos^2 \theta$$

(This is the squared component in the direction of $\vec{m}$)

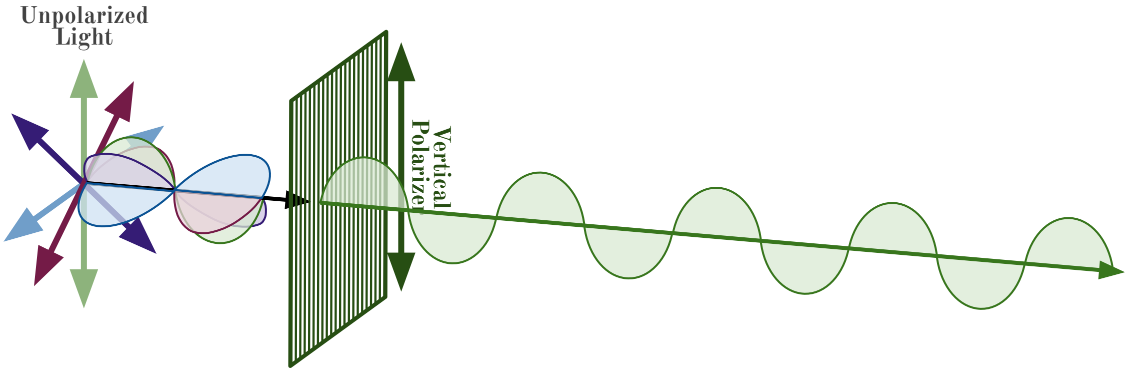
In that case, the state *is* now $\vec{m}$ !

Either way, ***always*** ends up with norm 1.

Otherwise, the state becomes the normalized projection onto $\vec{m}^{\perp}$ (with probability $|\langle \vec{m}^{\perp}, \vec{v} \rangle|^2 = \sin^2 \theta$ )

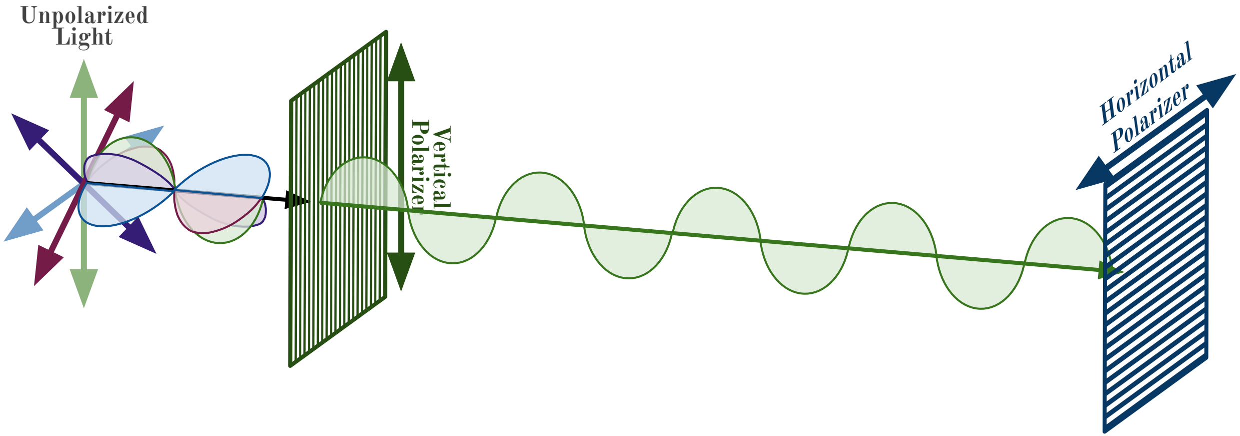


# Quantum Measurement



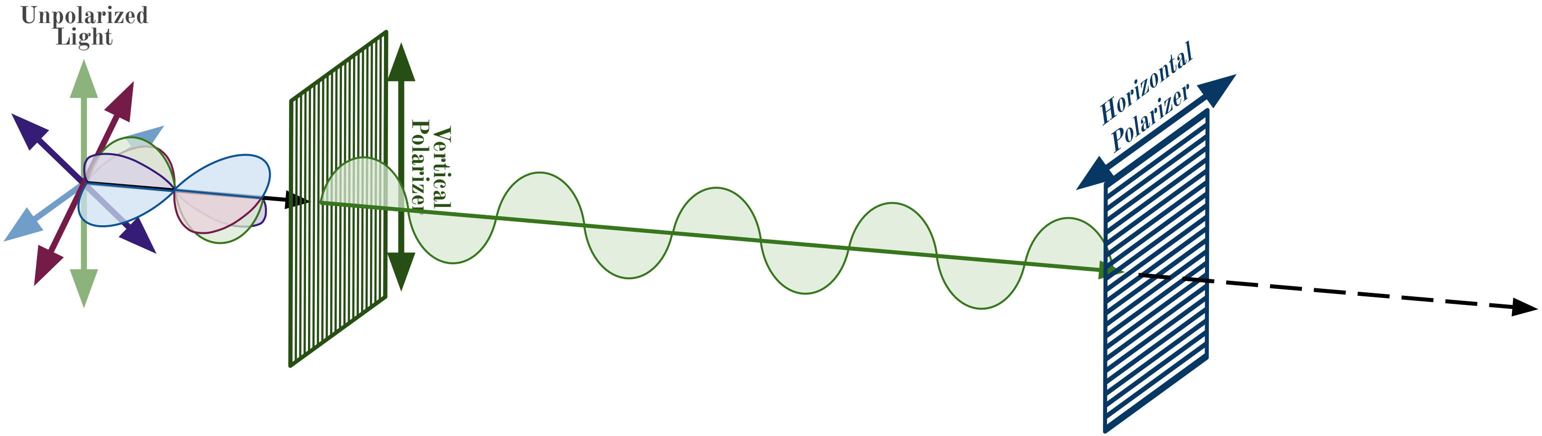
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

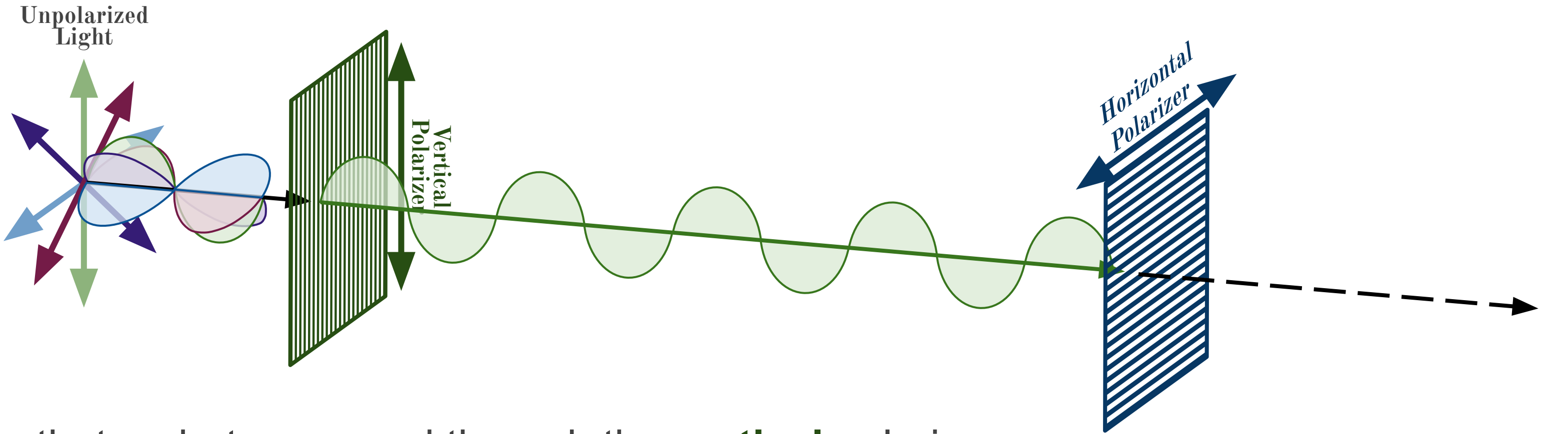


Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement



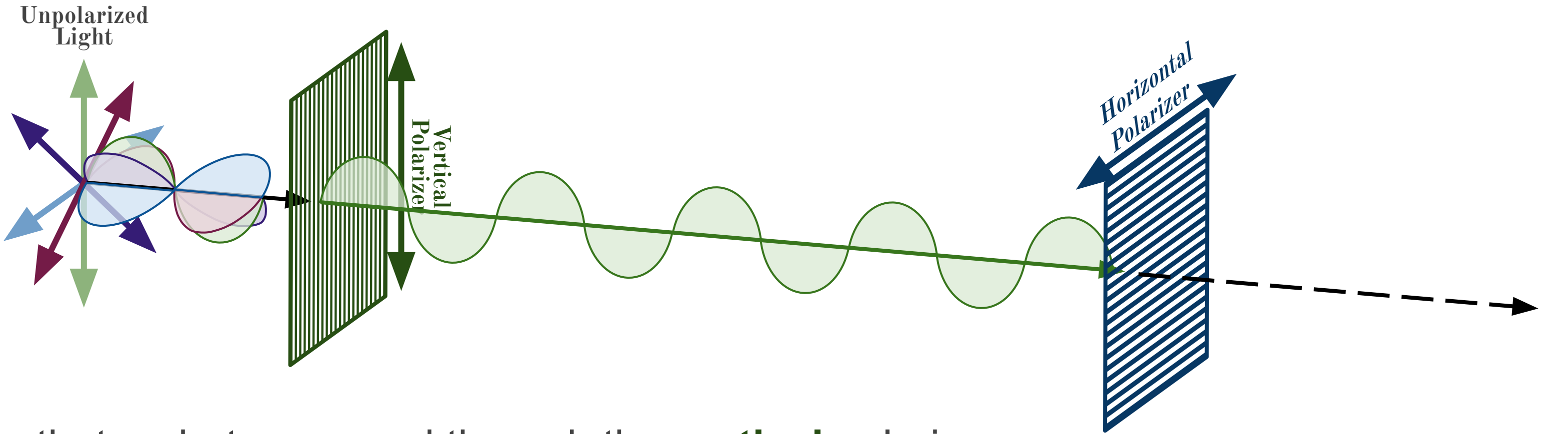
# Quantum Measurement




Given that a photon passed through the **vertical** polarizer, what is the probability that it then passes through the **horizontal** one?

(a) 0%
(b) 50%
(c) 100%

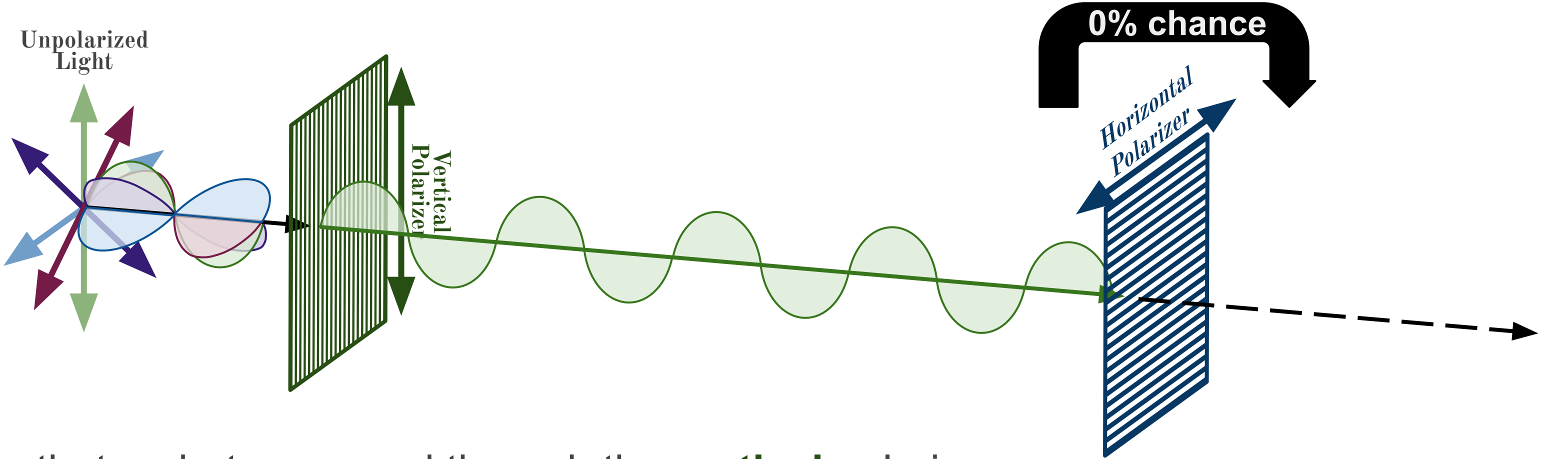
# Quantum Measurement




Given that a photon passed through the **vertical** polarizer,
what is the probability that it then passes through the **horizontal** one?

(a) 0%
(b) 50%
(c) 100%

# Quantum Measurement



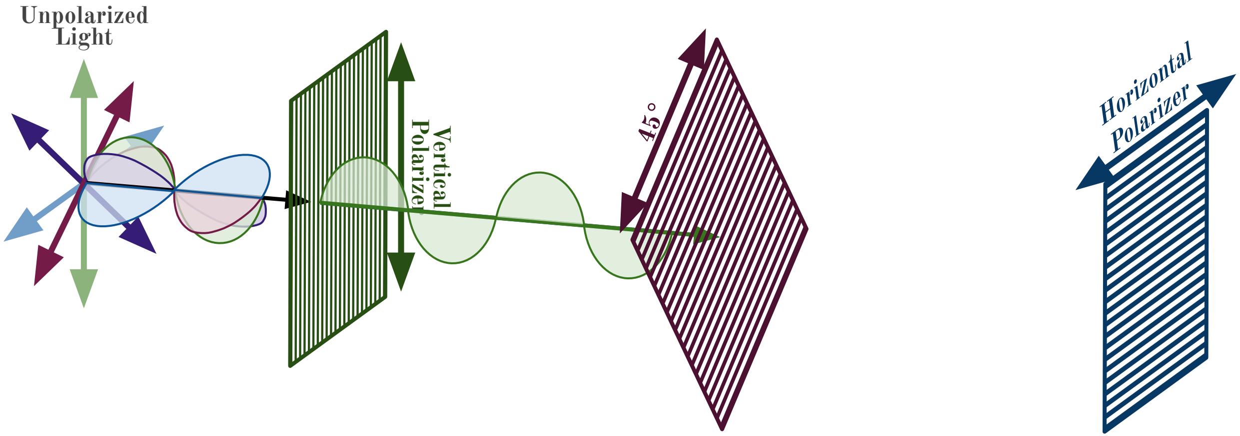

Given that a photon passed through the **vertical** polarizer,
what is the probability that it then passes through the **horizontal** one?

(a) 0%
(b) 50%
(c) 100%

?

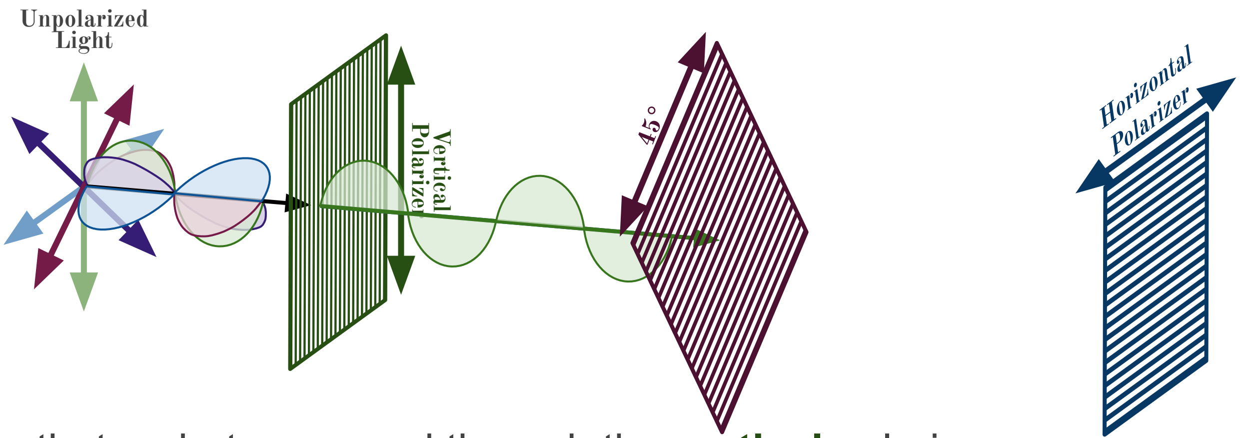
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement



Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

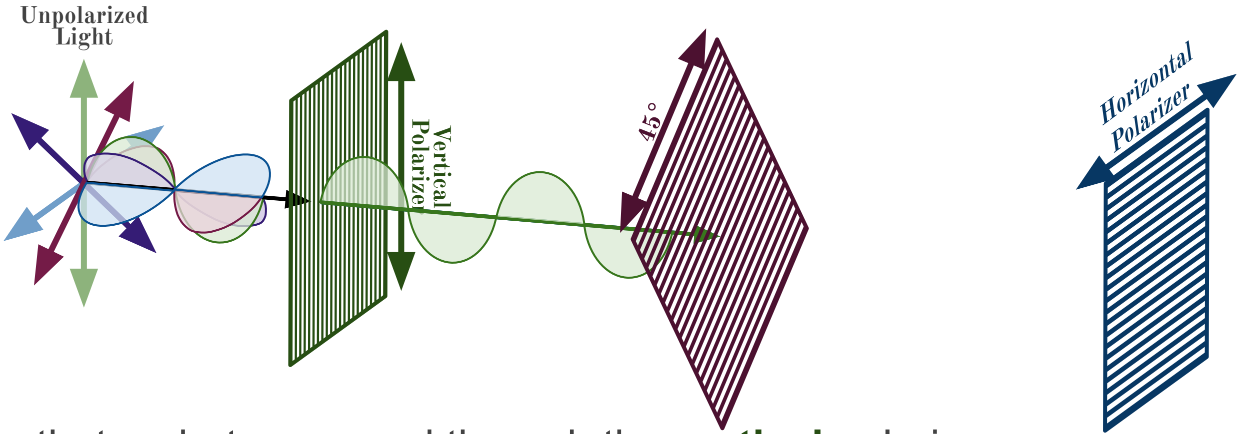



Given that a photon passed through the **vertical** polarizer, what is the probability that it then passes through the **diagonal** one?

(a) 0%
(b) 50%
(c) 100%

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Measurement

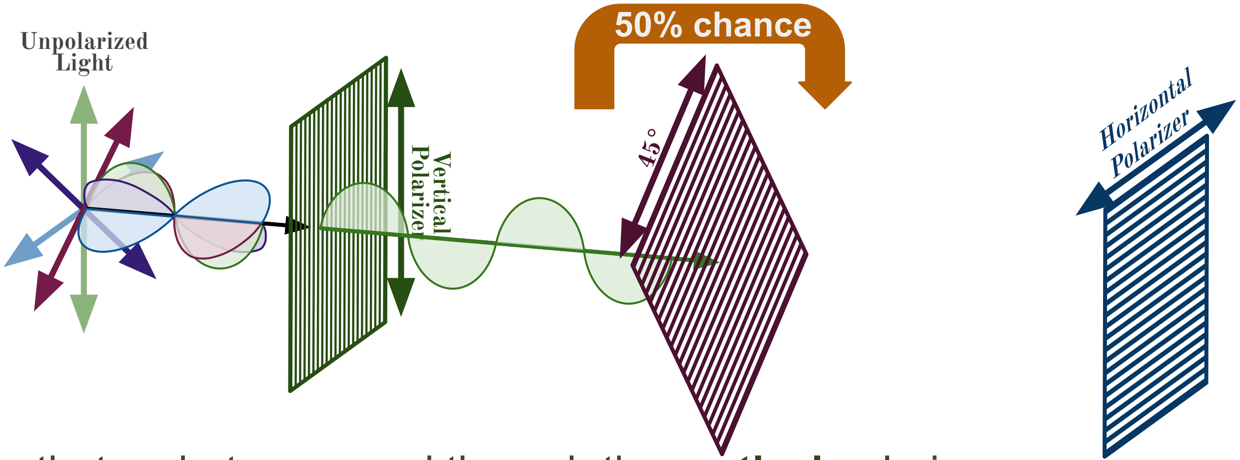



Given that a photon passed through the **vertical** polarizer,
what is the probability that it then passes through the **diagonal** one?

(a) 0%
(b) 50%
(c) 100%

?

# Quantum Measurement




Given that a photon passed through the **vertical** polarizer,
what is the probability that it then passes through the **diagonal** one?

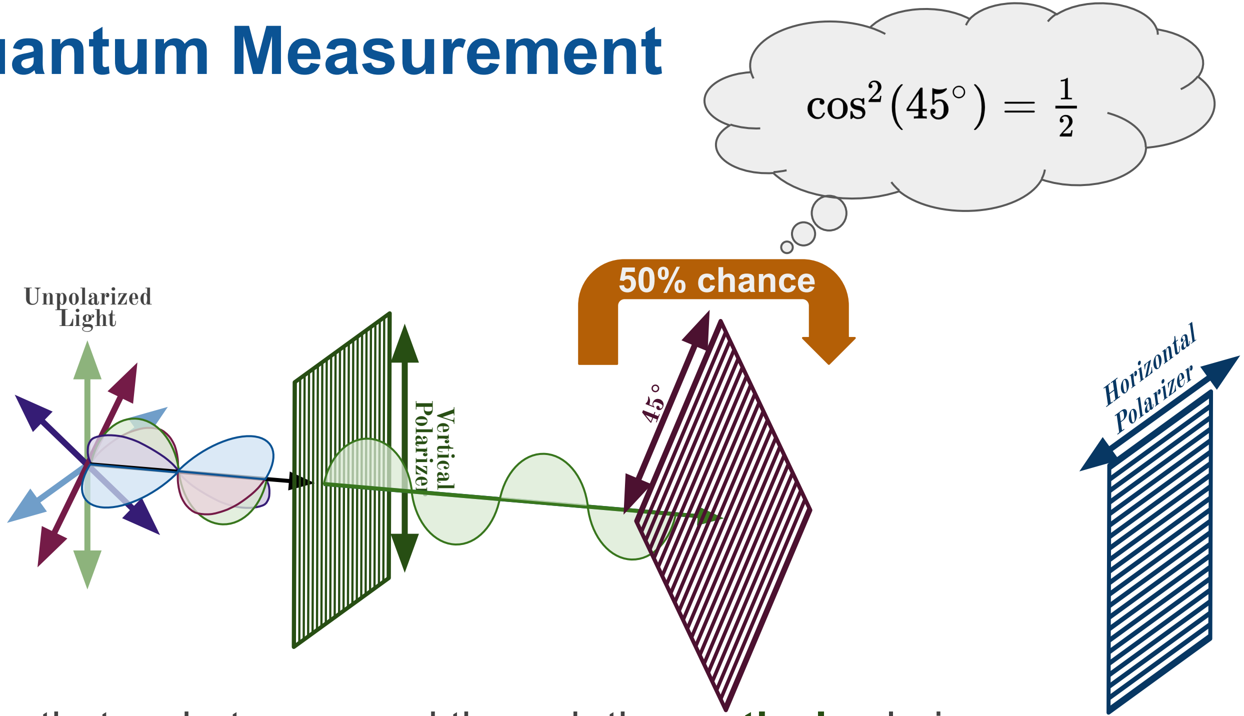
(a) 0%
(b) 50%
(c) 100%

?

Barak Nehoran (Postdoc, CS Department, Columbia University)

Columbia University in the City of New York

# Quantum Measurement

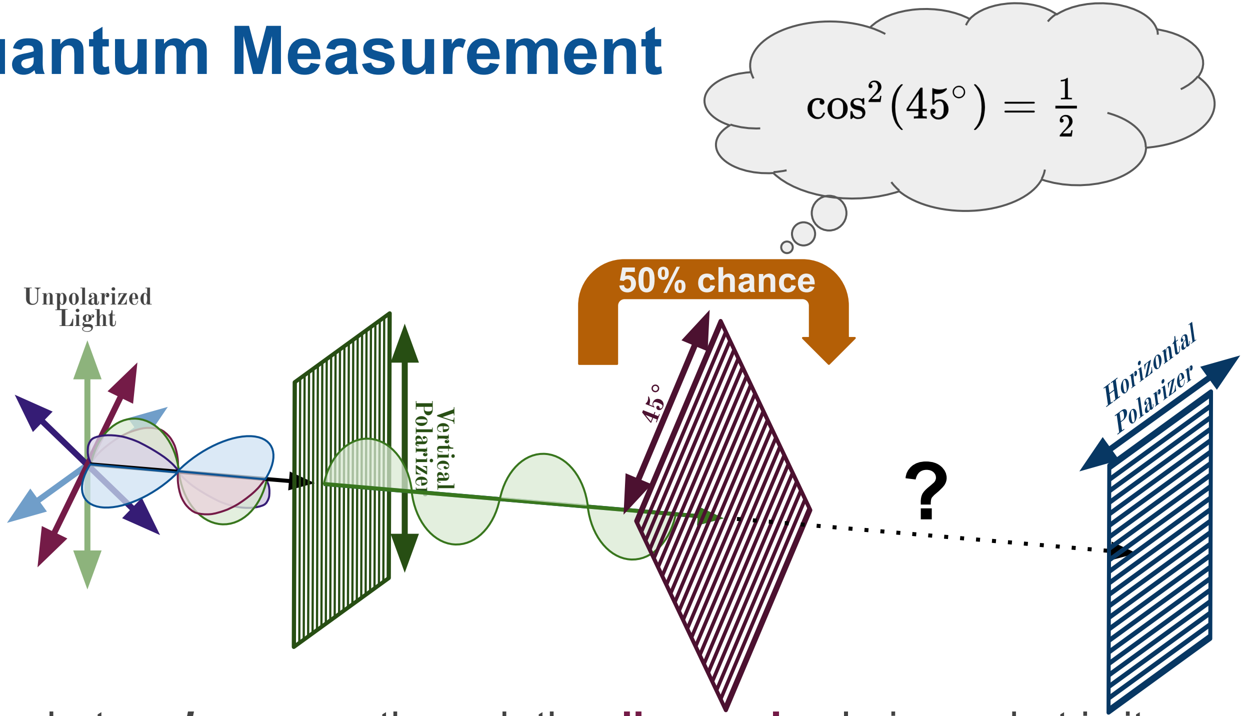



Given that a photon passed through the **vertical** polarizer, what is the probability that it then passes through the **diagonal** one?

(a) 0%
(b) 50%
(c) 100%

?

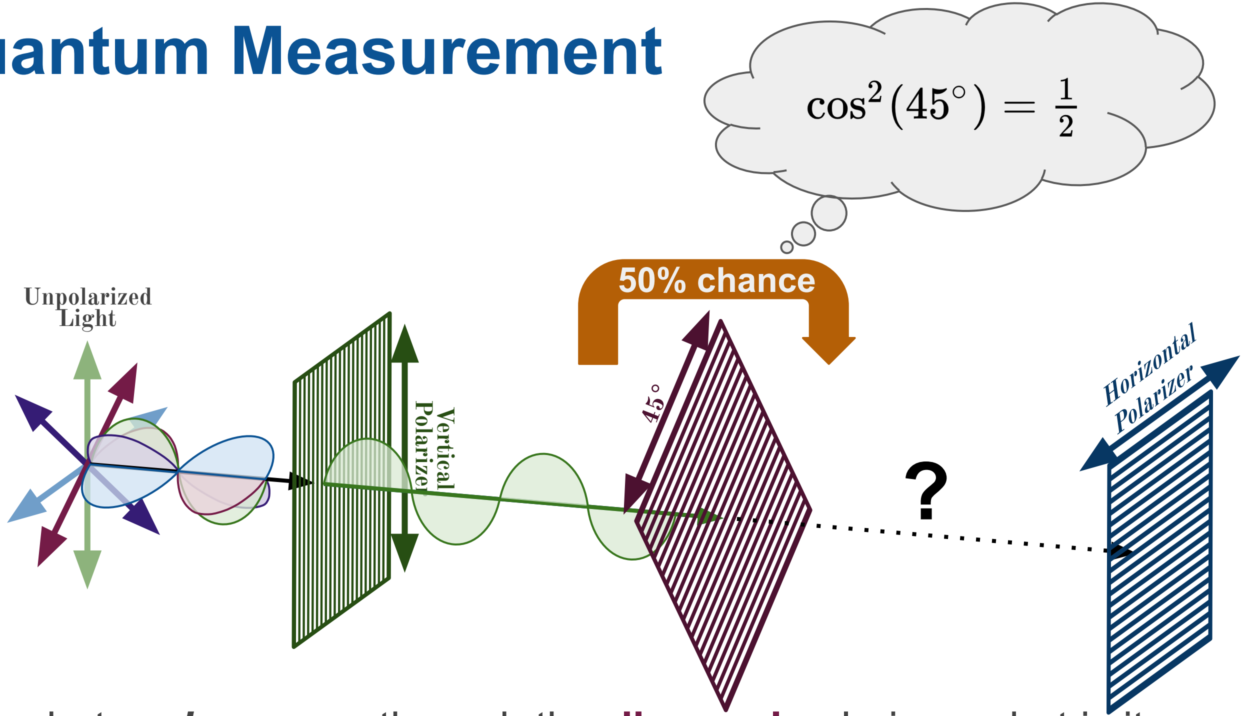
# Quantum Measurement




If the photon ***does*** pass through the **diagonal** polarizer, what is its resulting polarization?

(a) **vertical**
(b) **horizontal**
(c) **45°**
(d) **–45°**

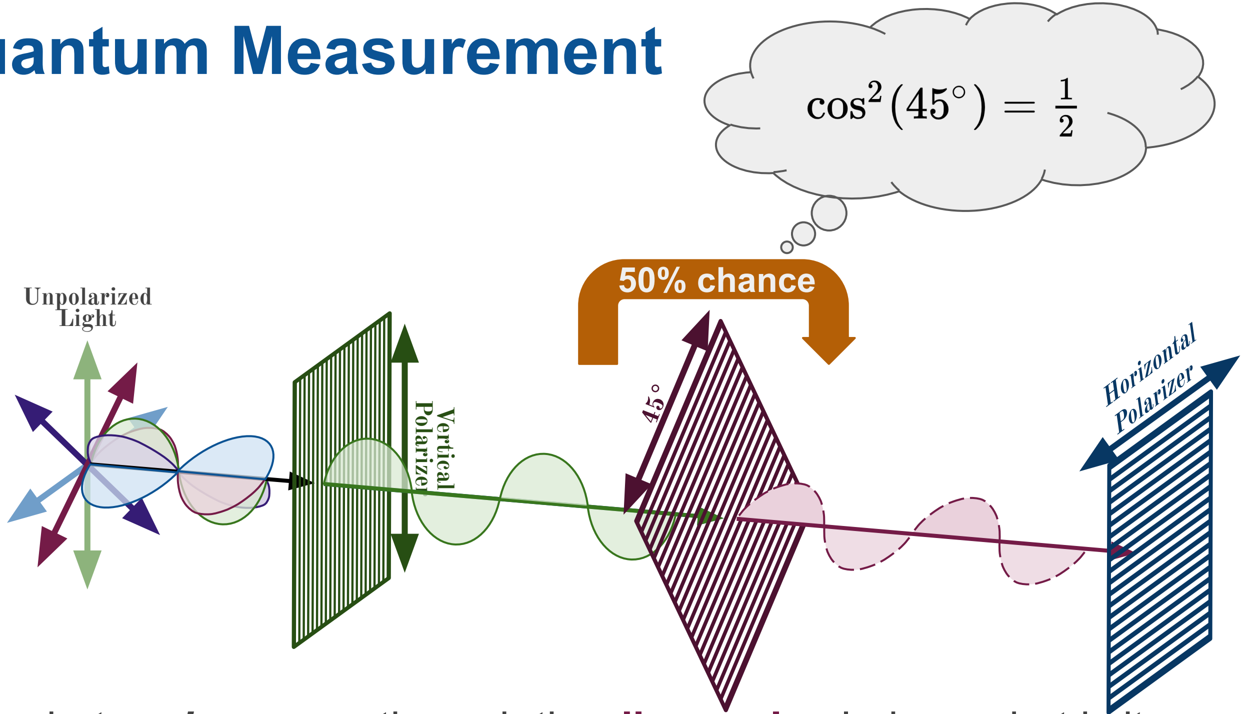
# Quantum Measurement




If the photon ***does*** pass through the **diagonal** polarizer, what is its resulting polarization?

(a) **vertical**
(b) **horizontal**
(c) **45°**
(d) **–45°**

# Quantum Measurement

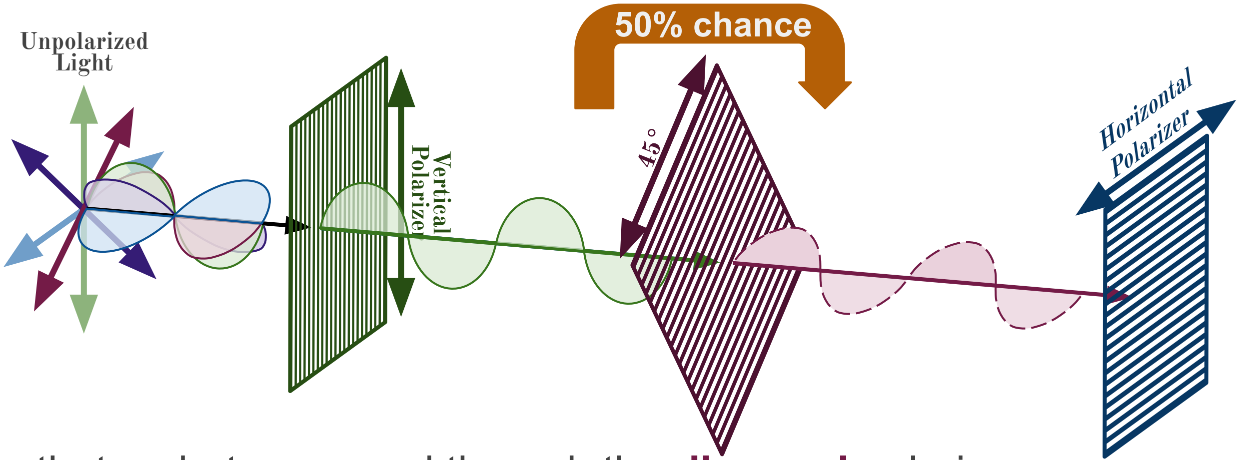



If the photon ***does*** pass through the **diagonal** polarizer, what is its resulting polarization?

(a) **vertical**
(b) **horizontal**
(c) **45°**
(d) **–45°**

?

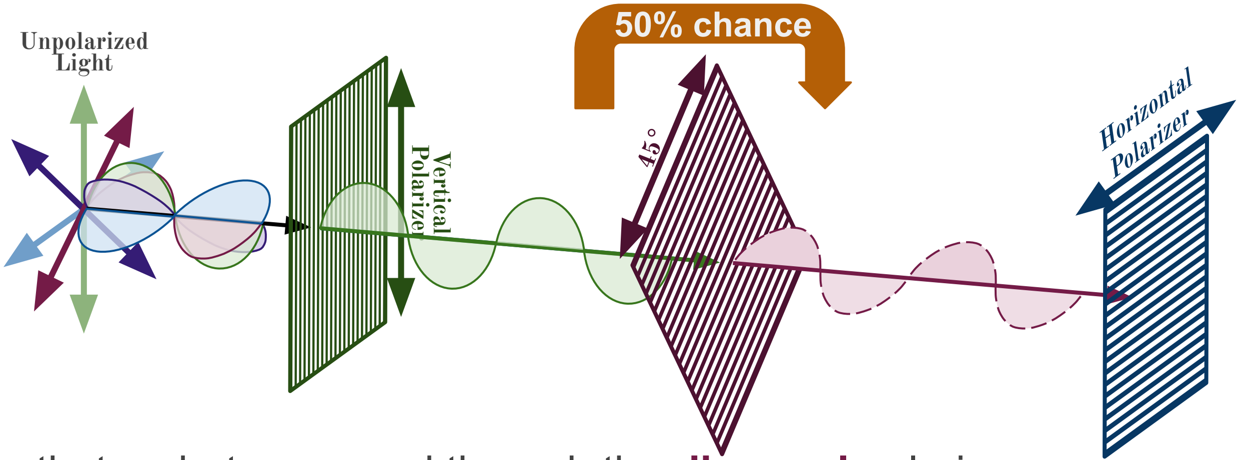
# Quantum Measurement




Given that a photon passed through the **diagonal** polarizer, what is the probability that it then passes through the **horizontal** one?

(a) 0%
(b) 50%
(c) 100%

# Quantum Measurement

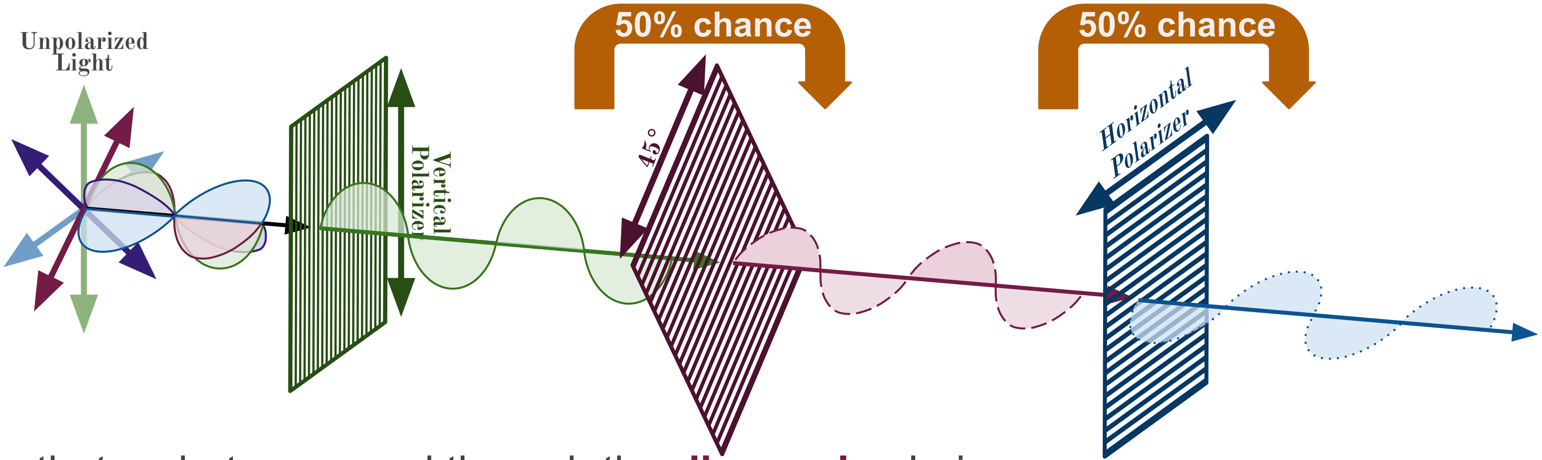



Given that a photon passed through the **diagonal** polarizer, what is the probability that it then passes through the **horizontal** one?

(a) 0%
(b) 50%
(c) 100%

?

# Quantum Measurement

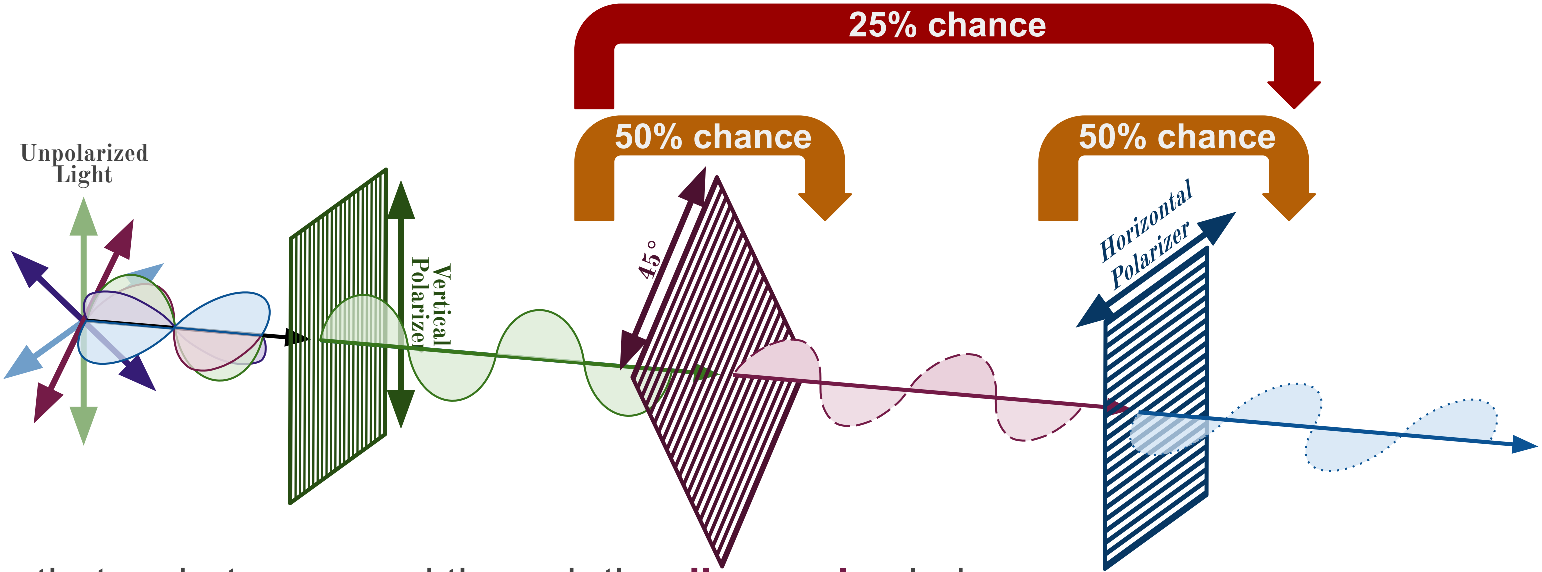



Given that a photon passed through the **diagonal** polarizer, what is the probability that it then passes through the **horizontal** one?

(a) 0%
(b) 50%
(c) 100%

?

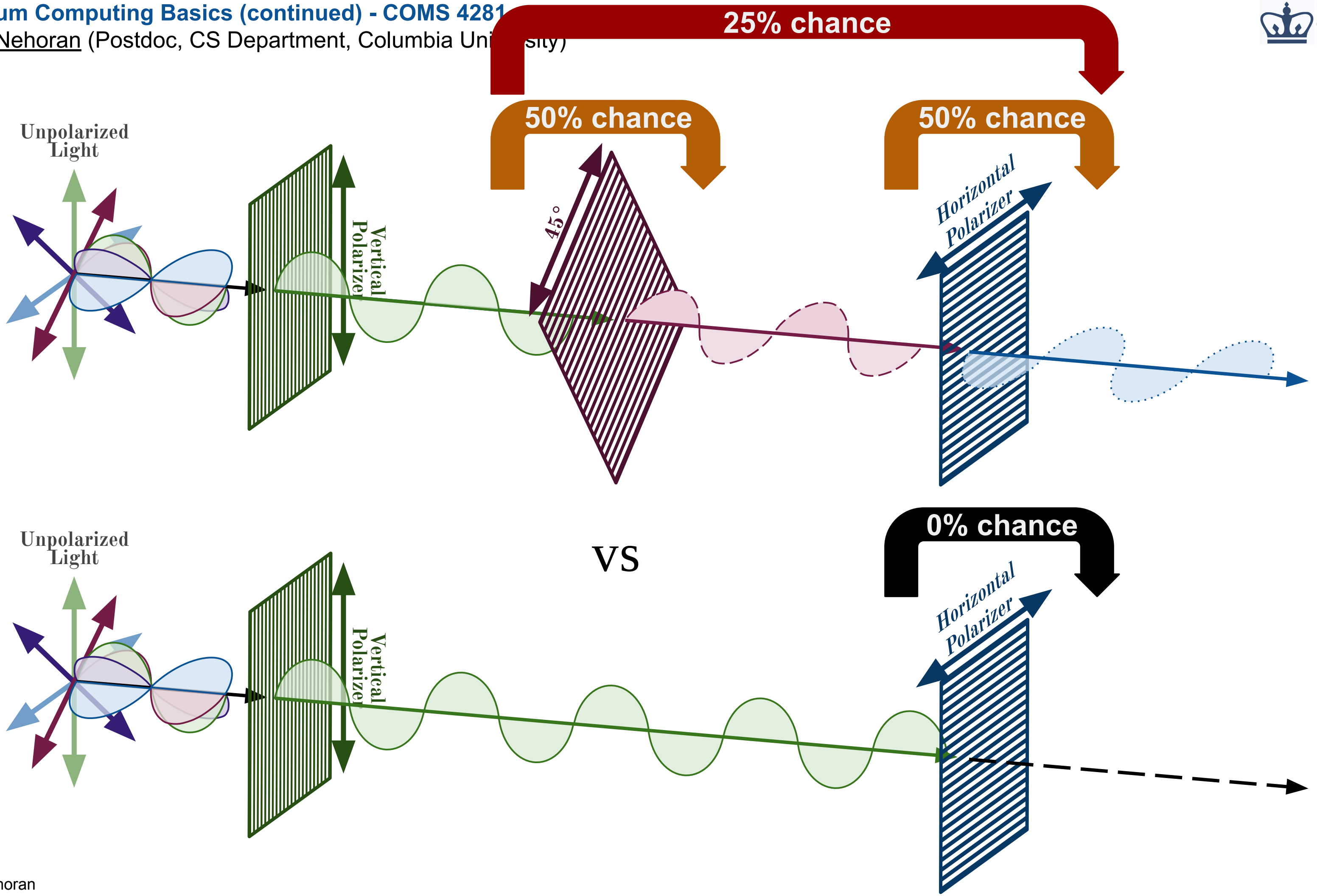
# Quantum Measurement



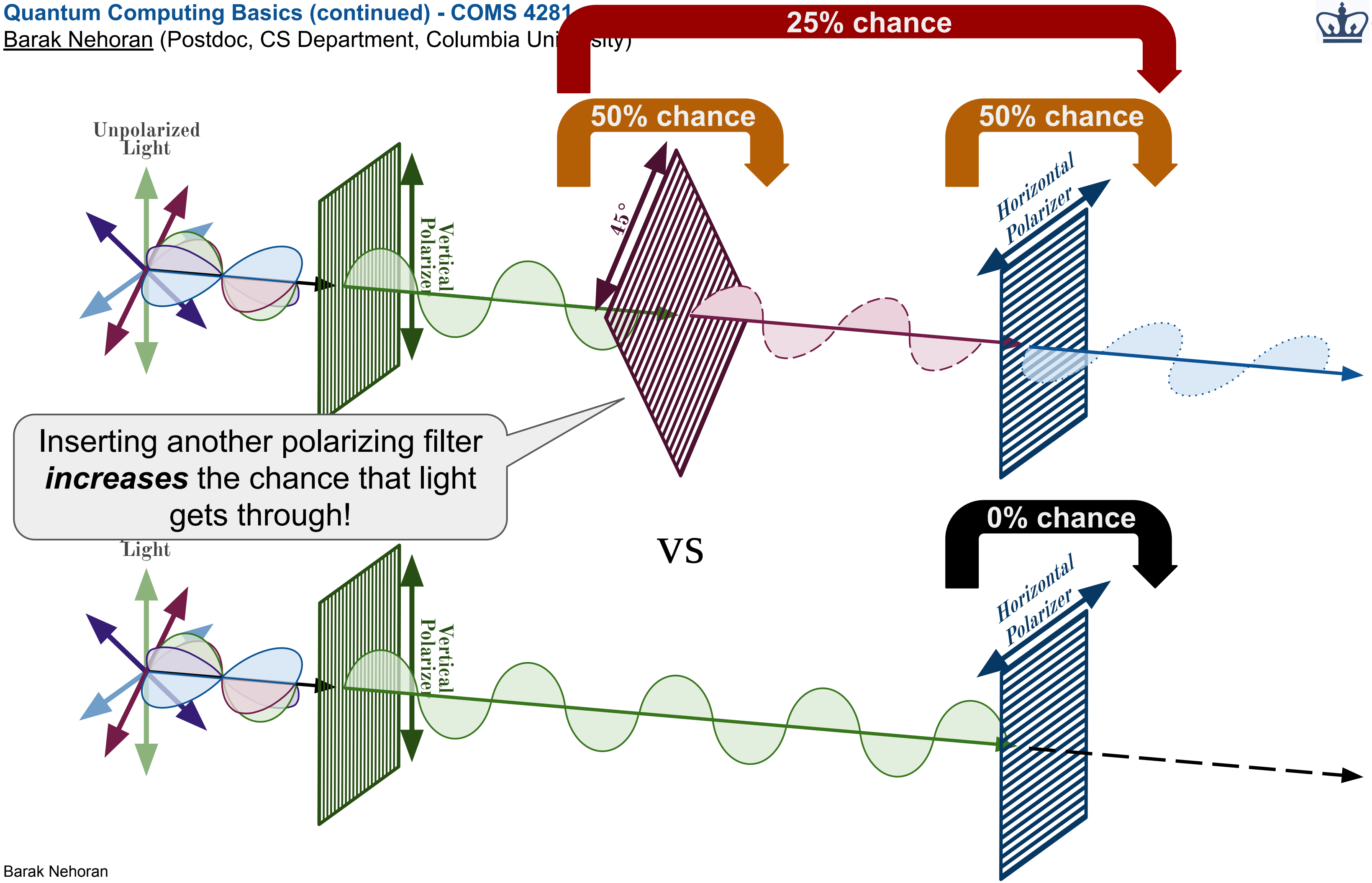

Given that a photon passed through the **diagonal** polarizer, what is the probability that it then passes through the **horizontal** one?

(a) 0%
(b) 50%
(c) 100%

?


25% chance
50% chance
50% chance
Unpolarized Light
Vertical Polarizer
45°
Horizontal Polarizer
VS
0% chance
Unpolarized Light
Vertical Polarizer
Horizontal Polarizer

Barak Nehoran (Postdoc, CS Department, Columbia University)



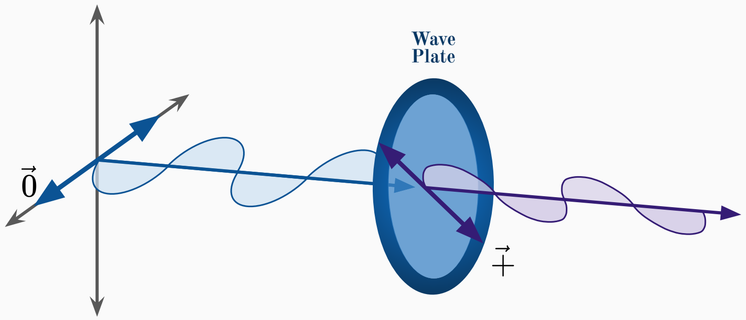
# Unitaries: Operations that don't measure

A polarizer **measures**: the photon passes or is absorbed, and the superposition is destroyed.

# Unitaries: Operations that don't measure

A polarizer **measures**: the photon passes or is absorbed, and the superposition is destroyed.

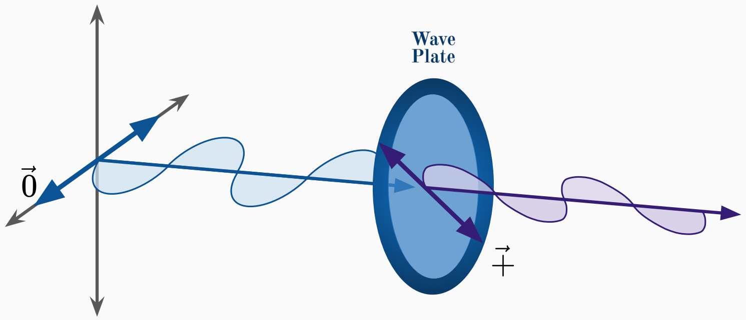
A **wave plate** does something different: a crystal that delays one polarization component relative to the other. It changes the polarization with no outcome and no collapse.



# Unitaries: Operations that don't measure

A polarizer **measures**: the photon passes or is absorbed, and the superposition is destroyed.

A **wave plate** does something different: a crystal that delays one polarization component relative to the other. It changes the polarization with no outcome and no collapse.




This is **unitary evolution**:

$$|\psi\rangle \longmapsto U|\psi\rangle$$

where $U$ is **unitary**: it preserves lengths, so unit vectors stay unit vectors. Every operation on an isolated system is of this form.

## The Hadamard gate

The single most important single-qubit unitary:

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

# The Hadamard gate

The single most important single-qubit unitary:

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

It takes the standard basis to the diagonal basis:

$$H|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle ,$$
$$H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle .$$

# The Hadamard gate

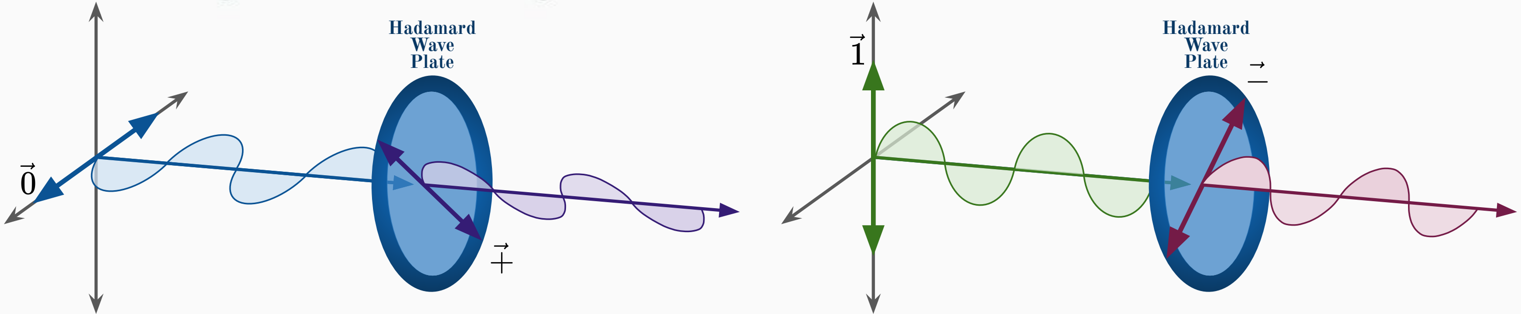
The single most important single-qubit unitary:

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

It takes the standard basis to the diagonal basis:

$$H|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle,$$
$$H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle.$$

**Physically**: a wave plate that **mirrors the polarization about an axis at** $22.5°$ does exactly this — vertical light comes out diagonal.



# Hadamard undoes itself

Since $H^2 = I$:

$$H|+\rangle = |0\rangle \qquad \text{and} \qquad H|-\rangle = |1\rangle .$$

# Hadamard undoes itself

Since $H^2 = I$:

$$H\,|+\rangle = |0\rangle \qquad \text{and} \qquad H\,|-\rangle = |1\rangle\,.$$

So here is a second way to tell $|+\rangle$ from $|-\rangle$: **apply $H$, then measure in the standard basis.**

# Hadamard undoes itself

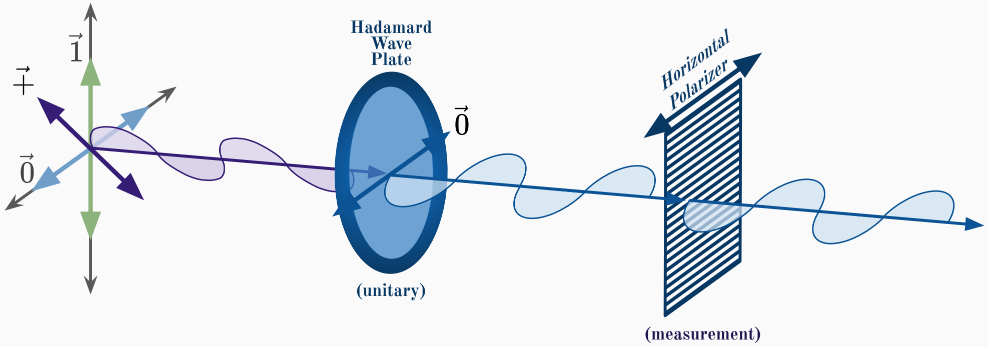
Since $H^2 = I$:

$$H|+\rangle = |0\rangle \qquad \text{and} \qquad H|-\rangle = |1\rangle\,.$$

So here is a second way to tell $|+\rangle$ from $|-\rangle$: **apply $H$, then measure in the standard basis.**

Earlier we tilted the polarizer by 45°. Here we rotate the state instead and leave the measurement alone.

Same experiment, viewed two ways.



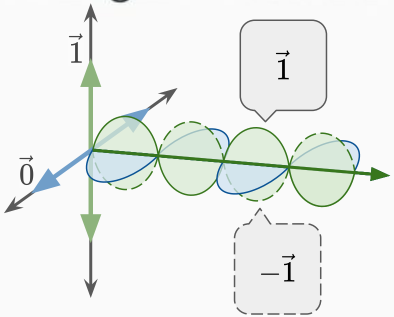
# Relative phase versus global phase

$|+\rangle$ and $|-\rangle$ differ by a **relative phase**, and we just saw that this is observable — $H$ followed by a measurement tells them apart perfectly.

# Relative phase versus global phase

$|+\rangle$ and $|-\rangle$ differ by a **relative phase**, and we just saw that this is observable — $H$ followed by a measurement tells them apart perfectly.

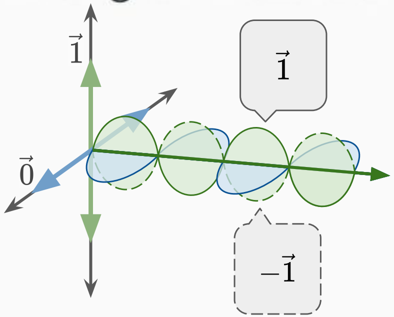
We also saw that negating a state vector leaves the polarization unchanged. That is a **global phase**.



# Relative phase versus global phase

$|+\rangle$ and $|-\rangle$ differ by a **relative phase**, and we just saw that this is observable — $H$ followed by a measurement tells them apart perfectly.

We also saw that negating a state vector leaves the polarization unchanged. That is a **global phase**.




For any real $\theta$, the states

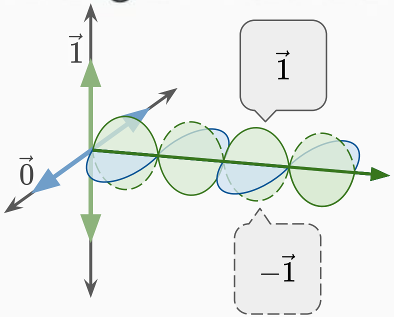
$$|\psi\rangle \qquad \text{and} \qquad e^{i\theta}\,|\psi\rangle$$

give the **same measurement statistics** after any unitary and any measurement.

# Relative phase versus global phase

$|+\rangle$ and $|-\rangle$ differ by a **relative phase**, and we just saw that this is observable — $H$ followed by a measurement tells them apart perfectly.

We also saw that negating a state vector leaves the polarization unchanged. That is a **global phase**.



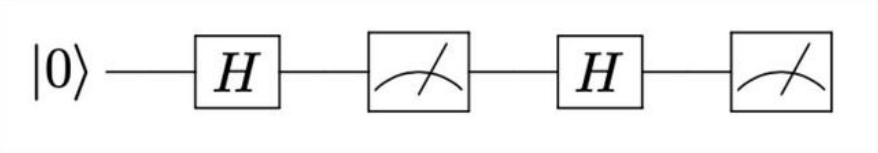

For any real $\theta$, the states

$$|\psi\rangle \qquad \text{and} \qquad e^{i\theta}\,|\psi\rangle$$

give the **same measurement statistics** after any unitary and any measurement.

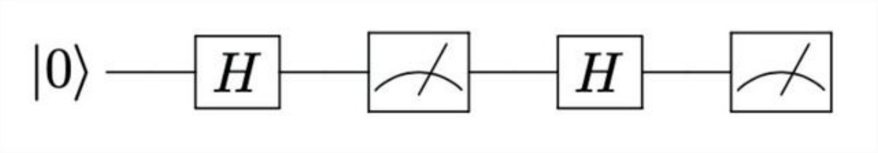
No quantum process can detect a global phase.

# Experiment A




A wire carries one qubit; a box is a gate; the meter is a standard-basis measurement.

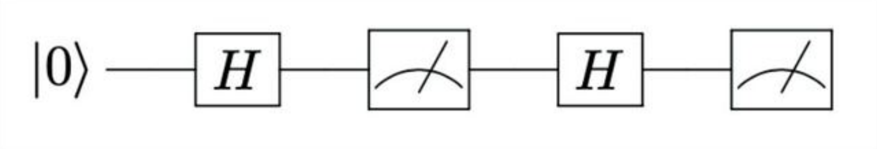
# Experiment A




A wire carries one qubit; a box is a gate; the meter is a standard-basis measurement.

**Outcome**: $|0\rangle$ and $|1\rangle$ with equal probability.

# Experiment A

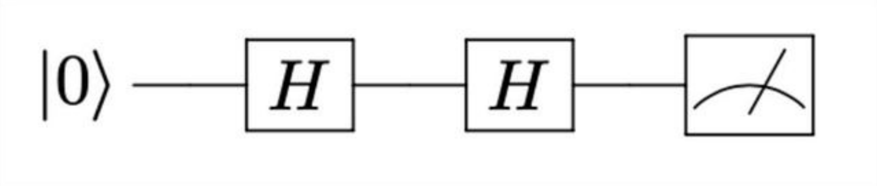



A wire carries one qubit; a box is a gate; the meter is a standard-basis measurement.

**Outcome**: $|0\rangle$ and $|1\rangle$ with equal probability.

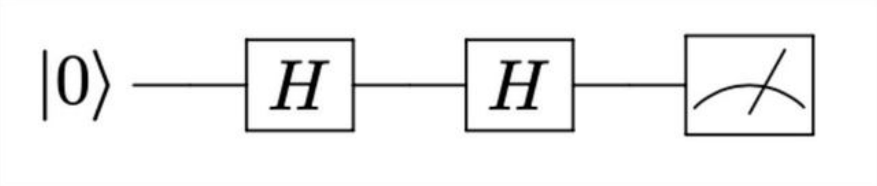
One might conclude that $H$ simply produces a random classical bit.

# Experiment B




The same circuit, but we measure **only at the end**.

# Experiment B




The same circuit, but we measure **only at the end**.

**Outcome**: $|0\rangle$, always.

# Experiment B

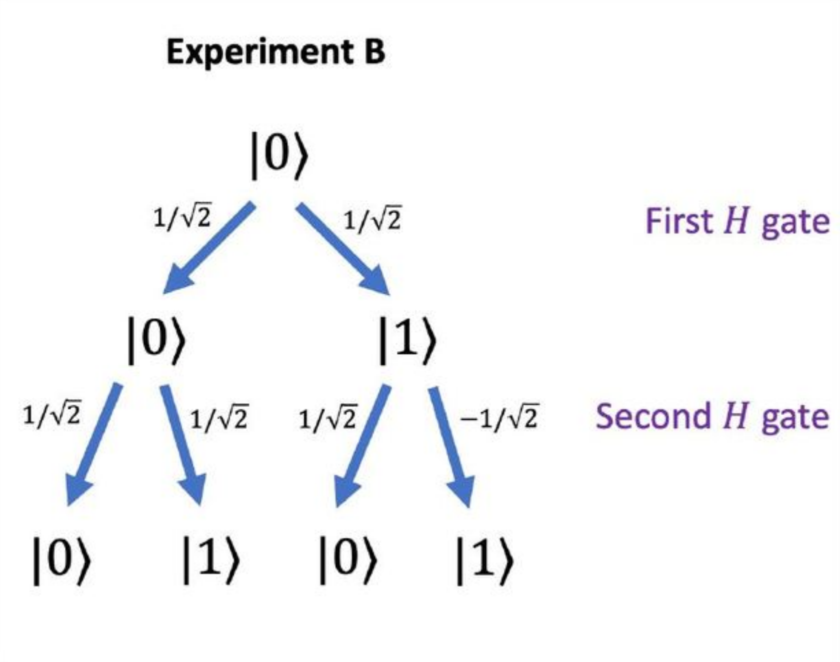
$$|0\rangle \;—\; \boxed{H} \;—\; \boxed{H} \;—\; \text{measure}$$

The same circuit, but we measure **only at the end**.

**Outcome**: $|0\rangle$, always.

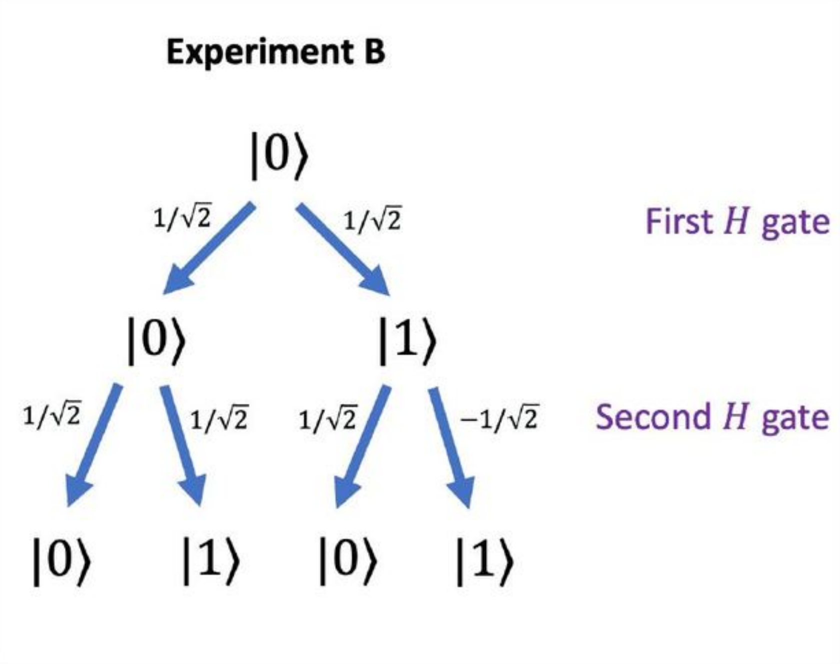
**Removing the intermediate measurement changes the result completely** — the circuit version of the three-polarizer surprise.

# Quantum interference




Applying several unitaries to a qubit gives a tree of "paths" between states.

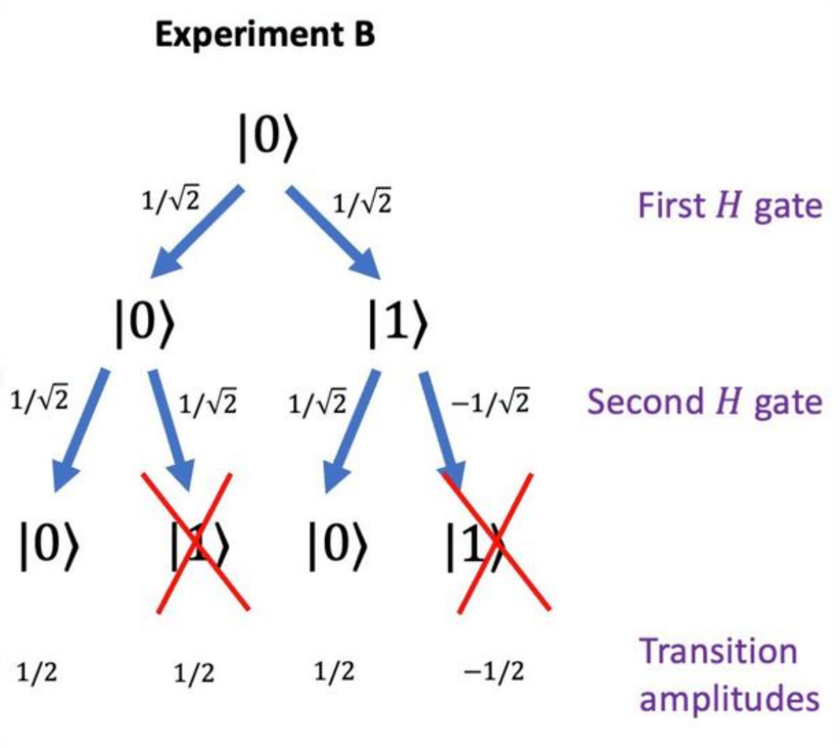
# Quantum interference




Applying several unitaries to a qubit gives a tree of "paths" between states.

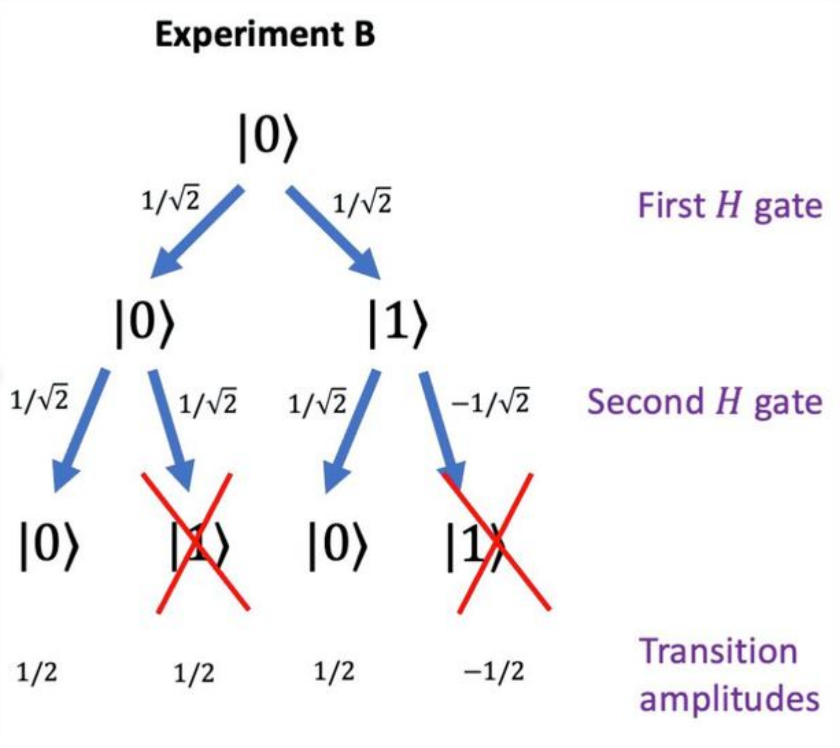
Each edge from $|a\rangle$ to $|b\rangle$ carries a **transition amplitude**, read off from the unitary.

# Quantum interference




A path's amplitude is the product of the amplitudes along it.

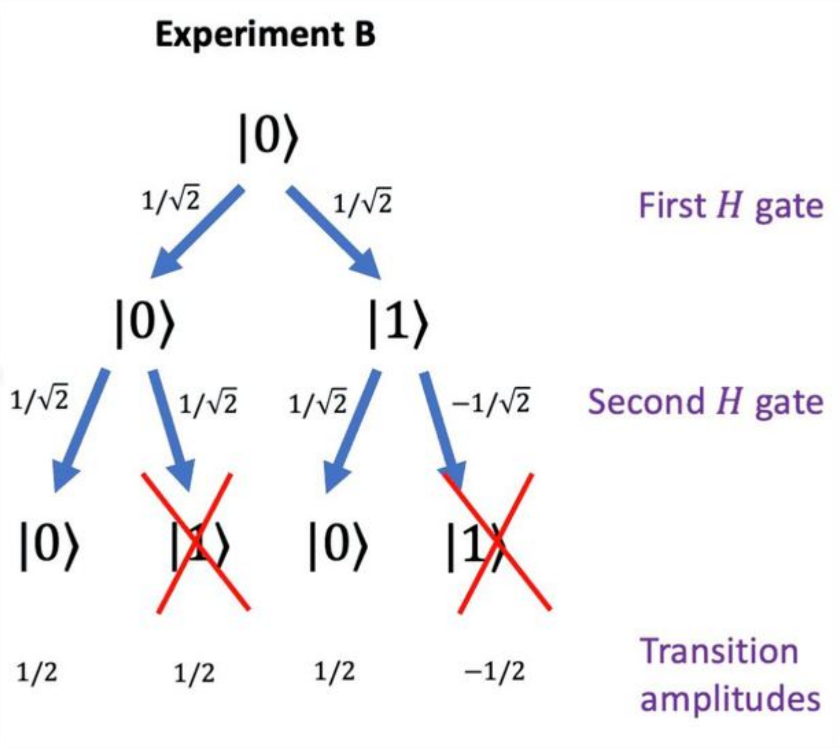
# Quantum interference




A path's amplitude is the product of the amplitudes along it.

Before measurement, the amplitude of ending at $|b\rangle$ is the **sum** over all paths ending at $|b\rangle$.

# Quantum interference

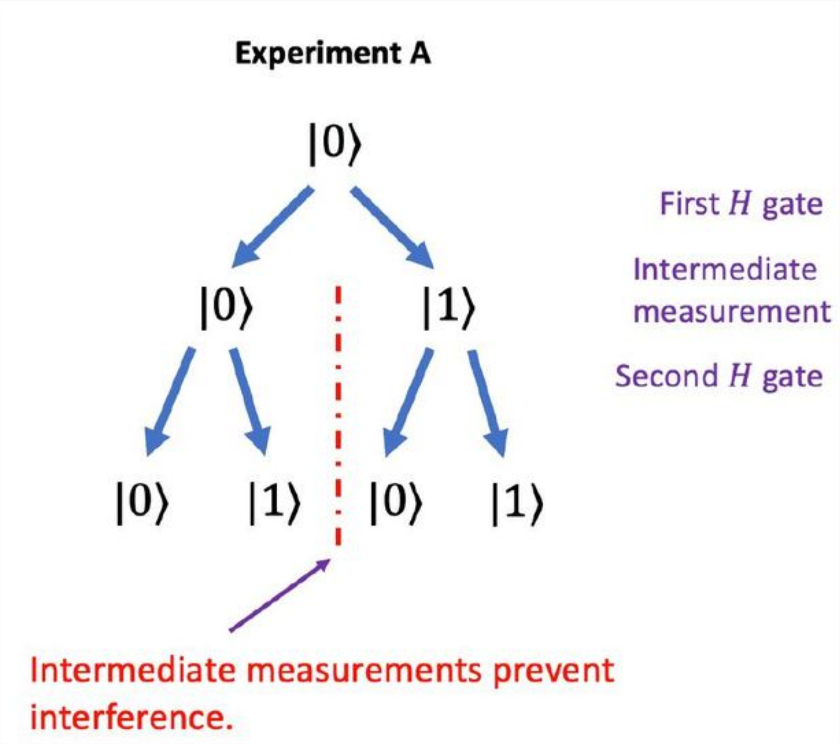



A path's amplitude is the product of the amplitudes along it.

Before measurement, the amplitude of ending at $|b\rangle$ is the **sum** over all paths ending at $|b\rangle$.

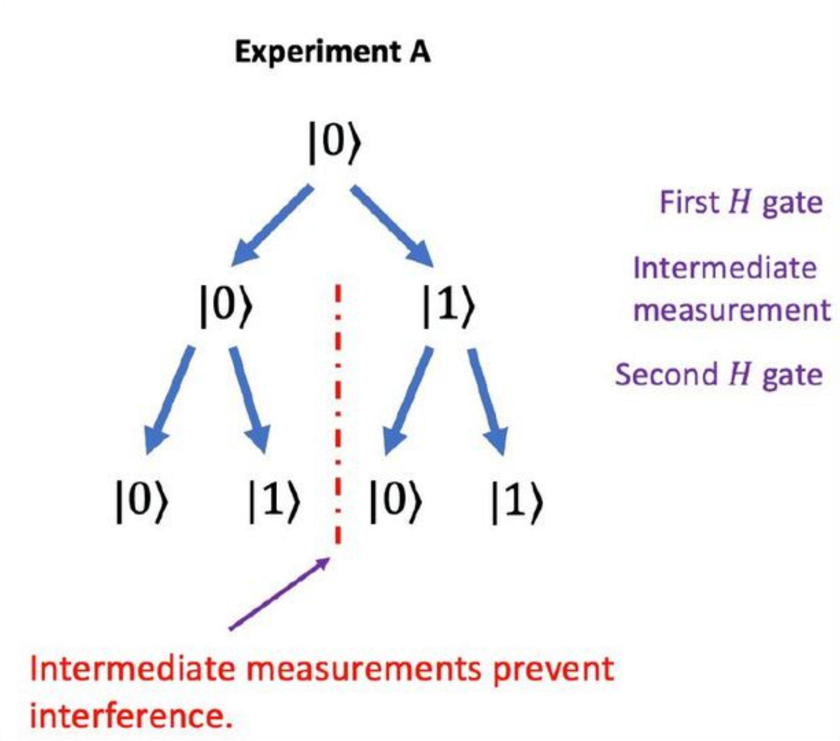
Amplitudes can be negative or complex, so paths can **constructively or destructively interfere**. In Experiment B, the two paths to $|1\rangle$ cancel.

# Quantum interference




With an intermediate measurement, only the paths consistent with the observed outcome are added up.

# Quantum interference




With an intermediate measurement, only the paths consistent with the observed outcome are added up.

**Takeaway**: measurement destroys superposition and prevents interference.

Barak Nehoran (Postdoc, CS Department, Columbia University)

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

$$\rho = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|$$

# Quantum Notation

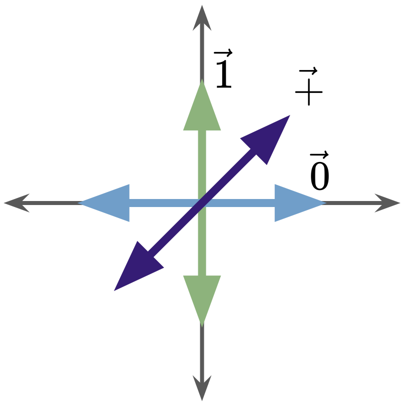
*It's all just fancy vectors!*

$$|\Psi_{\text{EPR}}\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

$$\rho_{\text{mixed}} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Notation: *It's all just fancy vectors!*

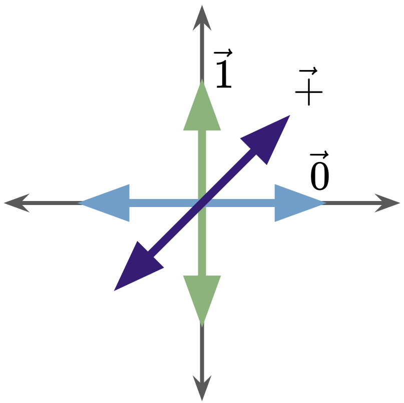



$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

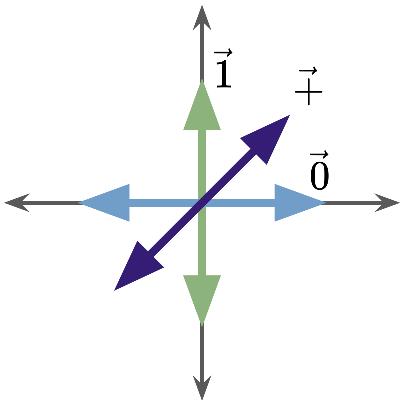
# Quantum Notation: *It's all just fancy vectors!*




$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^{\dagger} := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^{\dagger} := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

# Quantum Notation: *It's all just fancy vectors!*



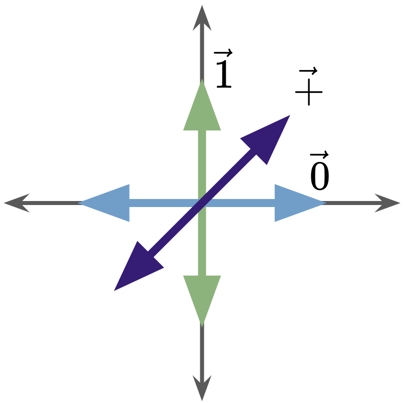

$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^{\dagger} := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^{\dagger} := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Notation: *It's all just fancy vectors!*



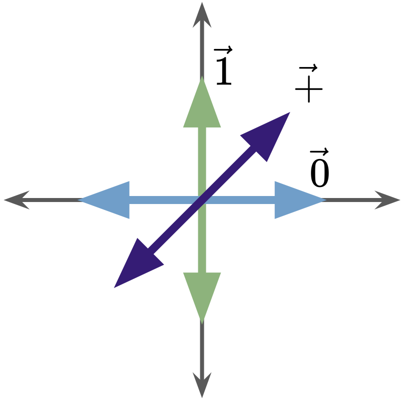

$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1}$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Notation: *It's all just fancy vectors!*

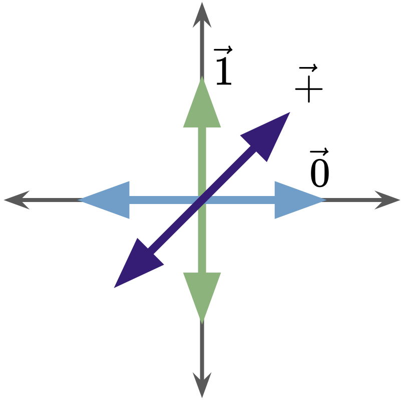



$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

# Quantum Notation: *It's all just fancy vectors!*



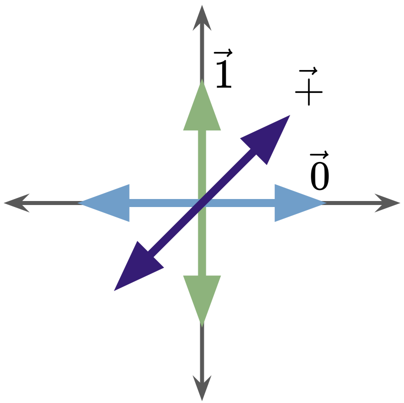

$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^{\dagger} := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^{\dagger} := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^{\dagger} \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle$$

# Quantum Notation: *It's all just fancy vectors!*




$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

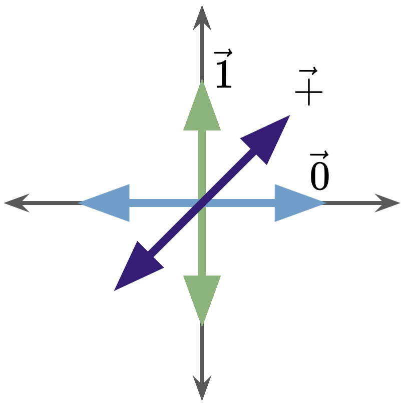
$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Notation: *It's all just fancy vectors!*




$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

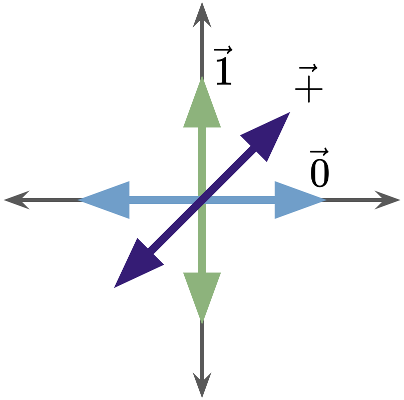
$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1 | 1 \rangle$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Notation: *It's all just fancy vectors!*



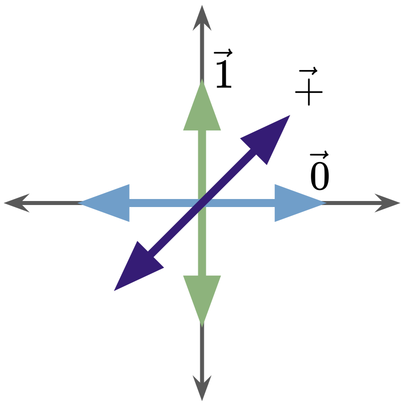

$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1 | 1 \rangle \longrightarrow \langle 1 | \cdot | 1 \rangle$$

# Quantum Notation: *It's all just fancy vectors!*




$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

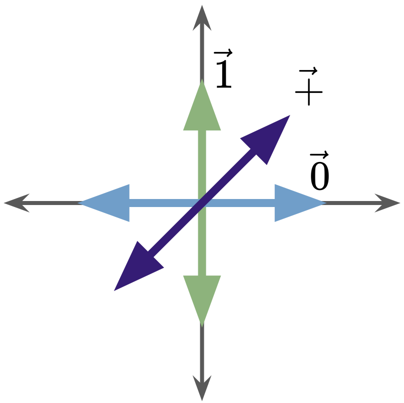
$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

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

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1 | 1 \rangle \longrightarrow \underset{\overset{\shortparallel}{\ }}{} \langle 1 | \cdot | 1 \rangle$$

# Quantum Notation: *It's all just fancy vectors!*



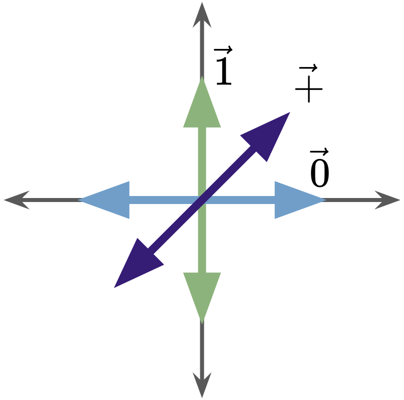

$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^{\dagger} := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^{\dagger} := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^{\dagger} \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1 | 1 \rangle \longrightarrow \underbrace{\langle 1 |}_{\begin{pmatrix} 0 & 1 \end{pmatrix}} \cdot \underbrace{| 1 \rangle}_{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}$$

# Quantum Notation: *It's all just fancy vectors!*




$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

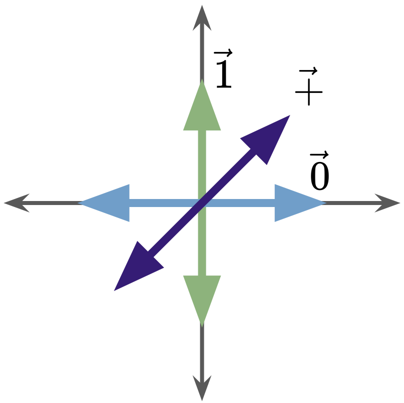
$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1 | 1 \rangle \longrightarrow \underset{\begin{pmatrix} 0 & 1 \end{pmatrix}}{\underset{\shortparallel}{\boxed{\langle 1 |}}} \cdot \underset{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}{\underset{\shortparallel}{\boxed{| 1 \rangle}}}$$

"bracket"

# Quantum Notation: *It's all just fancy vectors!*




$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^\dagger := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^\dagger := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^\dagger \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1 | 1 \rangle \longrightarrow \underset{\text{“bra”}}{\underset{\parallel}{\overset{\begin{pmatrix} 0 & 1 \end{pmatrix}}{\overset{\shortparallel}{\langle 1|}}}} \cdot \overset{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}{\overset{\shortparallel}{|1\rangle}}$$

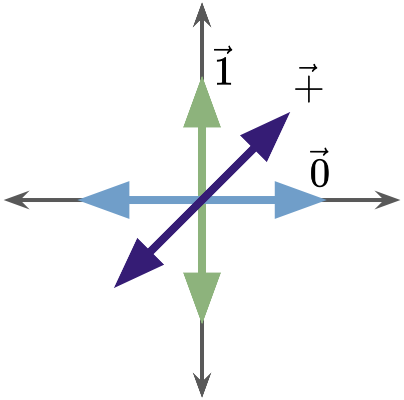
“bracket”

“bra”

Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Notation: *It's all just fancy vectors!*




$$\vec{0} := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \vec{0}^{\dagger} := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\vec{1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \vec{1}^{\dagger} := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

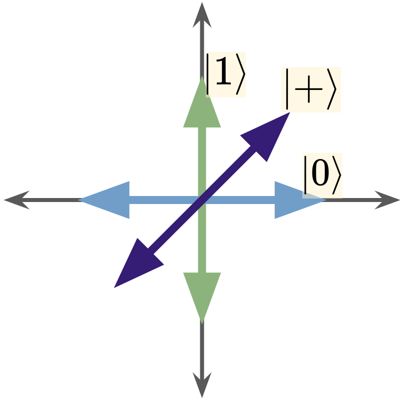
$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^{\dagger} \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1 | 1 \rangle \longrightarrow \underbrace{\langle 1 |}_{=\begin{pmatrix} 0 & 1 \end{pmatrix}} \cdot \underbrace{| 1 \rangle}_{=\begin{pmatrix} 0 \\ 1 \end{pmatrix}}$$

"bracket" "bra" "ket"

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Notation: *It's all just fancy vectors!*




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

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

$$\langle \vec{1}, \vec{1} \rangle := \vec{1}^{\dagger} \cdot \vec{1} = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle \vec{1}, \vec{1} \rangle \longrightarrow \langle \vec{1} | \vec{1} \rangle \longrightarrow \langle 1|1 \rangle \longrightarrow \underset{\text{“bra”}}{\langle 1|} \cdot \underset{\text{“ket”}}{|1\rangle}$$

“bracket”

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

# Bras are conjugated rows

A ket is a column vector; its **dual** (Hermitian conjugate) is a row vector, the bra:

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

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \langle \psi| = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix}$$

# Bras are conjugated rows

A ket is a column vector; its **dual** (Hermitian conjugate) is a row vector, the bra:

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

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad \langle \psi| = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix}$$

$\overline{\alpha}, \overline{\beta}$ are the **complex conjugates** of $\alpha, \beta$ — which matters as soon as we allow complex amplitudes, as in circular polarization.

# Inner products

For $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\theta\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$:

$$\langle\psi \mid \theta\rangle = \begin{pmatrix}\overline{\alpha}, & \overline{\beta}\end{pmatrix}\begin{pmatrix}\gamma \\ \delta\end{pmatrix} = \overline{\alpha}\gamma + \overline{\beta}\delta.$$

# Inner products

For $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\theta\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$:

$$\langle \psi \mid \theta \rangle = \begin{pmatrix} \overline{\alpha}, & \overline{\beta} \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \overline{\alpha}\gamma + \overline{\beta}\delta.$$

Two familiar facts in this language: $\langle \psi \mid \psi \rangle = 1$ is normalization, and the probability of outcome $|m\rangle$ is $|\langle m \mid \psi \rangle|^2$.

# Inner products

For $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\theta\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$:

$$\langle \psi \mid \theta \rangle = \begin{pmatrix} \overline{\alpha}, & \overline{\beta} \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \overline{\alpha}\gamma + \overline{\beta}\delta.$$

Two familiar facts in this language: $\langle \psi \mid \psi \rangle = 1$ is normalization, and the probability of outcome $|m\rangle$ is $|\langle m \mid \psi \rangle|^2$.

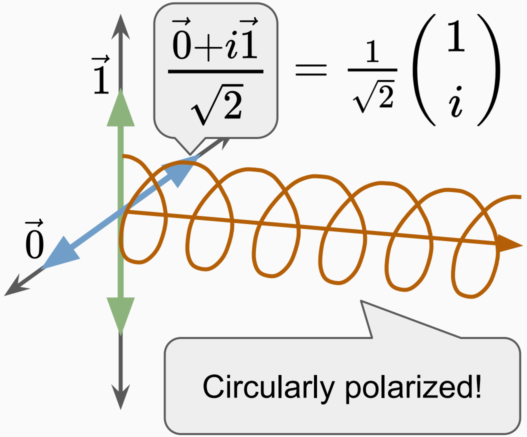
The order matters:

$$\langle \theta \mid \psi \rangle = \overline{\gamma}\alpha + \overline{\delta}\beta = \overline{\langle \psi \mid \theta \rangle}.$$

# A numerical example

Circularly polarized light:

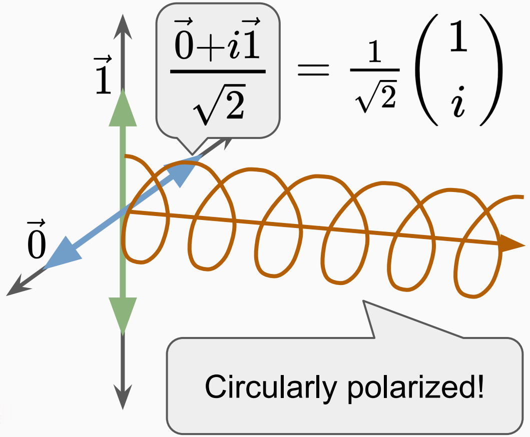
$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}.$$



# A numerical example

Circularly polarized light:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}.$$




Its bra is

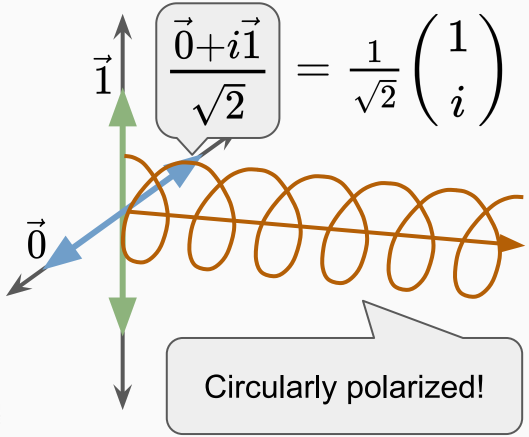
$$\langle\psi| = \frac{1}{\sqrt{2}}\langle 0| - \frac{i}{\sqrt{2}}\langle 1| = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\end{pmatrix}.$$

**Note the conjugate:** $\bar{i} = -i$.

# A numerical example

Circularly polarized light:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}.$$




Its bra is

$$\langle\psi| = \frac{1}{\sqrt{2}}\langle 0| - \frac{i}{\sqrt{2}}\langle 1| = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\end{pmatrix}.$$

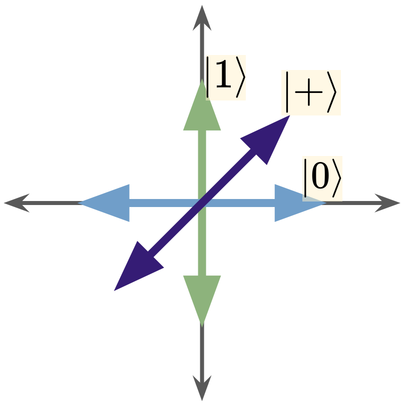
**Note the conjugate:** $\bar{i} = -i$.

Check normalization:

$$\langle\psi \mid \psi\rangle = \frac{1}{2}\begin{pmatrix}1 & -i\end{pmatrix}\begin{pmatrix}1\\ i\end{pmatrix} = \frac{1+(-i)i}{2} = 1.$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Notation: *It's all just fancy vectors!*

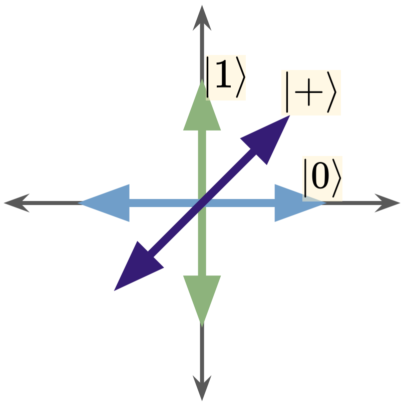



$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

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

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

# Quantum Notation: *It's all just fancy vectors!*



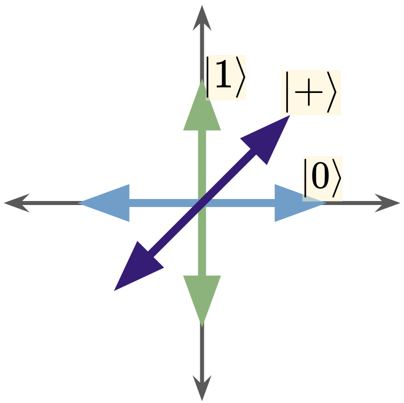

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

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

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |+\rangle\end{array}\right]$$

# Quantum Notation: *It's all just fancy vectors!*



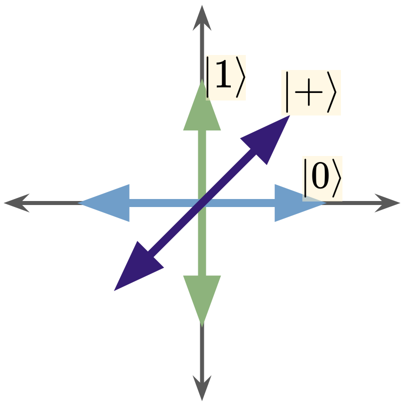

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

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

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |+\rangle\end{array}\right] = \left|\langle 1|+\rangle\right|^2$$

# Quantum Notation: *It's all just fancy vectors!*



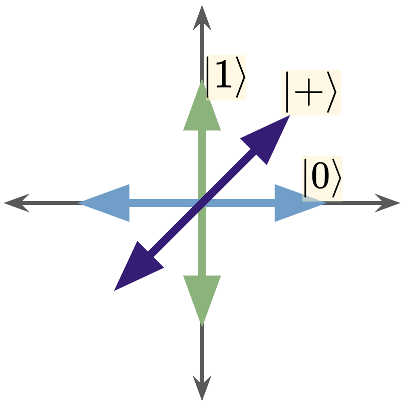

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

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

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |+\rangle\end{array}\right] = \left|\langle 1|+\rangle\right|^2 = \left|\langle 1|\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)\right|^2$$

# Quantum Notation: *It's all just fancy vectors!*




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

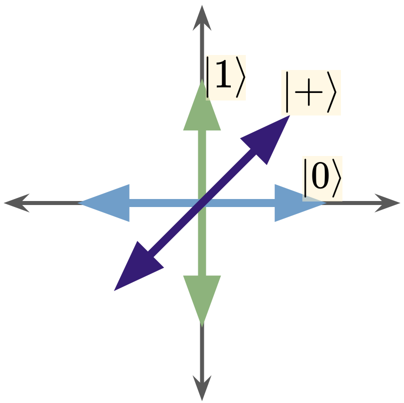
$$|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \langle 1| := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

distribute

$$\Pr\left[\begin{array}{l}\text{we get a } |1\rangle \text{ if we} \\ \text{measure the state } |+\rangle\end{array}\right] = \left|\langle 1|+\rangle\right|^2 = \left|\langle 1|\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\right|^2$$

# Quantum Notation: *It's all just fancy vectors!*



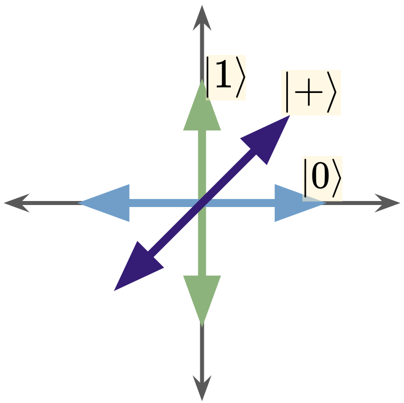

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

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

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |+\rangle\end{array}\right] = \left|\langle 1|+\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}\langle 1|0\rangle + \frac{1}{\sqrt{2}}\langle 1|1\rangle\right|^2$$

# Quantum Notation: *It's all just fancy vectors!*




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

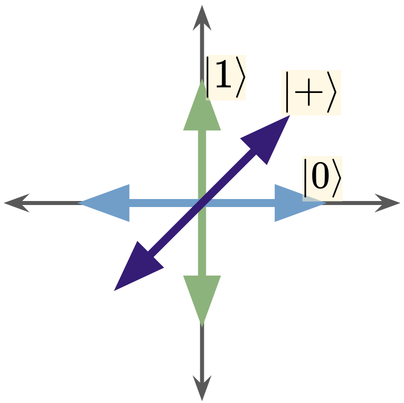
$$|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \langle 1| := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\text{we get a } |1\rangle \text{ if we} \\ \text{measure the state } |+\rangle\end{array}\right] = \left|\langle 1|+\rangle\right|^2 = \left|\tfrac{1}{\sqrt{2}}\langle 1|0\rangle + \tfrac{1}{\sqrt{2}}\langle 1|1\rangle\right|^2 = \left|0 + \tfrac{1}{\sqrt{2}}\right|^2$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Notation: *It's all just fancy vectors!*




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

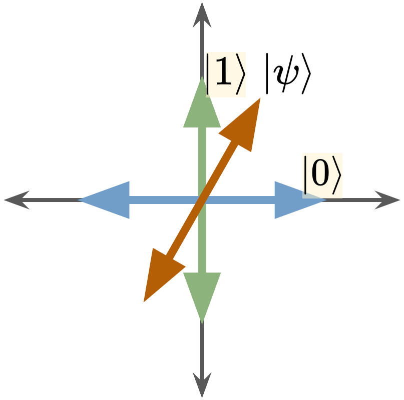
$$|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \langle 1| := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |+\rangle\end{array}\right] = \left|\langle 1|+\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}\langle 1|0\rangle + \frac{1}{\sqrt{2}}\langle 1|1\rangle\right|^2 = \left|0 + \frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Barak Nehoran (Postdoc, CS Department, Columbia University)


# Quantum Notation: *It's all just fancy vectors!*




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

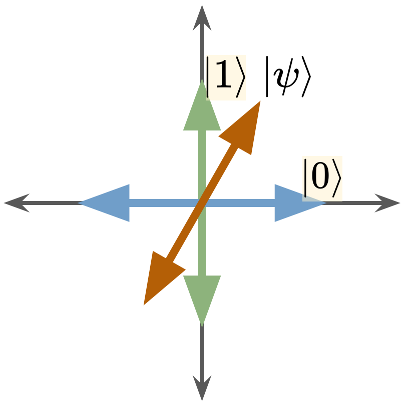
$$|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \langle 1| := \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\text{we get a } |1\rangle \text{ if we} \\ \text{measure the state } |\psi\rangle\end{array}\right]$$

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Notation: *It's all just fancy vectors!*




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

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

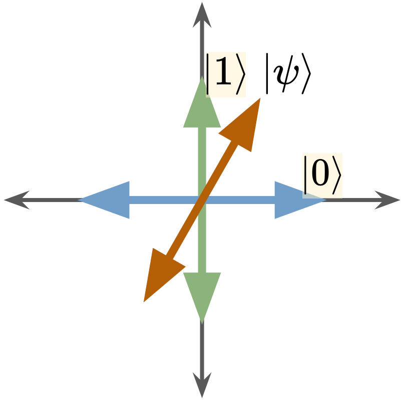
$$|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |\psi\rangle\end{array}\right] = \left|\langle 1|\psi\rangle\right|^2$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Notation: *It's all just fancy vectors!*



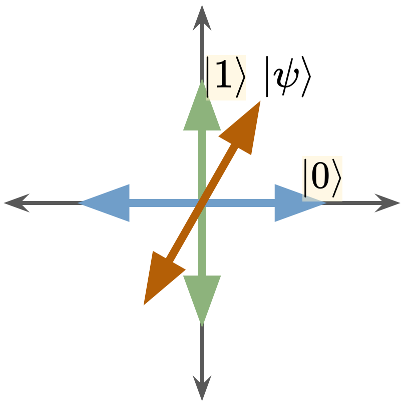

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

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

$$|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |\psi\rangle\end{array}\right] = \left|\langle 1|\psi\rangle\right|^2 =$$

# Quantum Notation: *It's all just fancy vectors!*



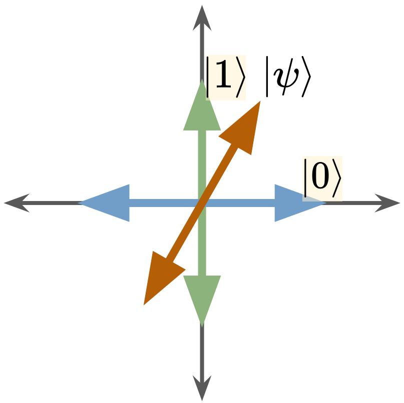

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \langle 0| := \begin{pmatrix} 1 & 0 \end{pmatrix}$$

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

$$|\psi\rangle = \frac{1}{2}|0\rangle + \boxed{\frac{\sqrt{3}}{2}}|1\rangle$$

$$\Pr\left[\begin{array}{l}\text{we get a } |1\rangle \text{ if we} \\ \text{measure the state } |\psi\rangle\end{array}\right] = \left|\langle 1|\psi\rangle\right|^2 = \left|\frac{\sqrt{3}}{2}\right|^2$$

# Quantum Notation: *It's all just fancy vectors!*




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

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

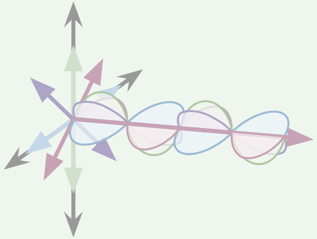
$$|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

$$\mathbf{Pr}\left[\begin{array}{l}\textbf{we get a } |1\rangle \textbf{ if we} \\ \textbf{measure the state } |\psi\rangle\end{array}\right] = \left|\langle 1|\psi\rangle\right|^2 = \left|\frac{\sqrt{3}}{2}\right|^2 = \frac{3}{4}$$

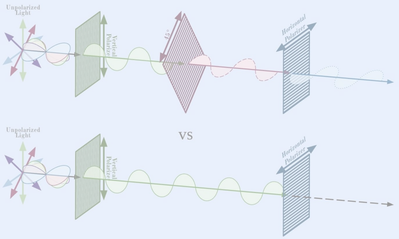
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Outline

1 The Qubit



2 Quantum Measurement

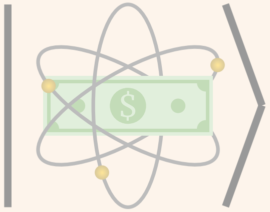


3 Quantum Entanglement & Many Qubits

First qubit Second qubit

$$\frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

4 No Cloning and Quantum Money



# Two photons instead of one

If the first photon is in state $|\psi_1\rangle$ and the second in state $|\psi_2\rangle$, the joint state is written

$$|\psi_1\rangle \otimes |\psi_2\rangle\,, \qquad \text{or just} \qquad |\psi_1\rangle\,|\psi_2\rangle\,.$$

# Two photons instead of one

If the first photon is in state $|\psi_1\rangle$ and the second in state $|\psi_2\rangle$, the joint state is written

$$|\psi_1\rangle \otimes |\psi_2\rangle\,, \qquad \text{or just} \qquad |\psi_1\rangle\,|\psi_2\rangle\,.$$

Two qubits have **four** basis states:

$$|0\rangle\,|0\rangle \qquad |0\rangle\,|1\rangle \qquad |1\rangle\,|0\rangle \qquad |1\rangle\,|1\rangle\,,$$

often abbreviated $|0,0\rangle\,, |0,1\rangle\,, |1,0\rangle\,, |1,1\rangle$ or $|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle$.

# Two photons instead of one

If the first photon is in state $|\psi_1\rangle$ and the second in state $|\psi_2\rangle$, the joint state is written

$$|\psi_1\rangle \otimes |\psi_2\rangle\,, \qquad \text{or just} \qquad |\psi_1\rangle\,|\psi_2\rangle\,.$$

Two qubits have **four** basis states:

$$|0\rangle\,|0\rangle \qquad |0\rangle\,|1\rangle \qquad |1\rangle\,|0\rangle \qquad |1\rangle\,|1\rangle\,,$$

often abbreviated $|0,0\rangle\,, |0,1\rangle\,, |1,0\rangle\,, |1,1\rangle$ or $|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle$.

So a two-qubit state is a unit vector in the four-dimensional space $\mathbb{C}^2 \otimes \mathbb{C}^2$, and $n$ qubits live in $2^n$ dimensions.

# Multiplying out the tensor product

If $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi_2\rangle = \gamma|0\rangle + \delta|1\rangle$, then

$$|\psi_1\rangle \otimes |\psi_2\rangle = \alpha\gamma|0,0\rangle + \alpha\delta|0,1\rangle + \beta\gamma|1,0\rangle + \beta\delta|1,1\rangle\,.$$

# Multiplying out the tensor product

If $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi_2\rangle = \gamma|0\rangle + \delta|1\rangle$, then

$$|\psi_1\rangle \otimes |\psi_2\rangle = \alpha\gamma|0,0\rangle + \alpha\delta|0,1\rangle + \beta\gamma|1,0\rangle + \beta\delta|1,1\rangle\,.$$

These four numbers are exactly the amplitudes $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}$ of a general two-qubit state:

$$|\psi\rangle = \sum_{i,j} \alpha_{ij}|i,j\rangle\,, \qquad \sum_{i,j} |\alpha_{ij}|^2 = 1.$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Multiple Qubits

General two-qubit state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Multiple Qubits

That is, this is any unit vector on these four basis vectors.

General two-qubit state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Multiple Qubits

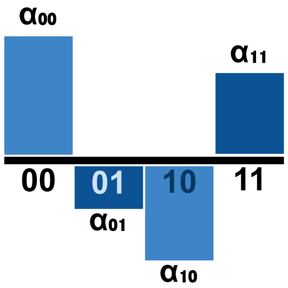
That is, this is any unit vector on these four basis vectors.

General two-qubit state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$|\psi\rangle =$



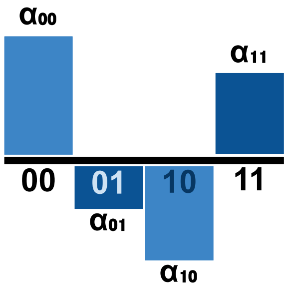
# Multiple Qubits

That is, this is any unit vector on these four basis vectors.

General two-qubit state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$|\psi\rangle =$ 


If we measure, the probability of getting outcome $x$ is $|\alpha_x|^2$

Barak Nehoran (Postdoc, CS Department, Columbia University)

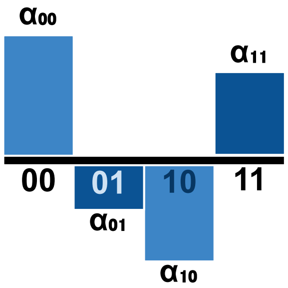
# Multiple Qubits

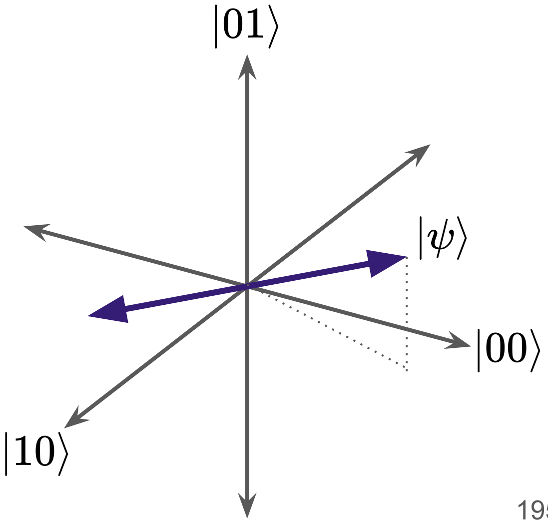
That is, this is any unit vector on these four basis vectors.

General two-qubit state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$|\psi\rangle =$ 


If we measure, the probability of getting outcome $x$ is $|\alpha_x|^2$

Barak Nehoran (Postdoc, CS Department, Columbia University)

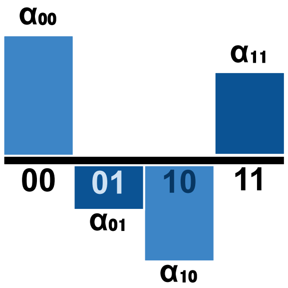
# Multiple Qubits

That is, this is any unit vector on these four basis vectors.

General two-qubit state:

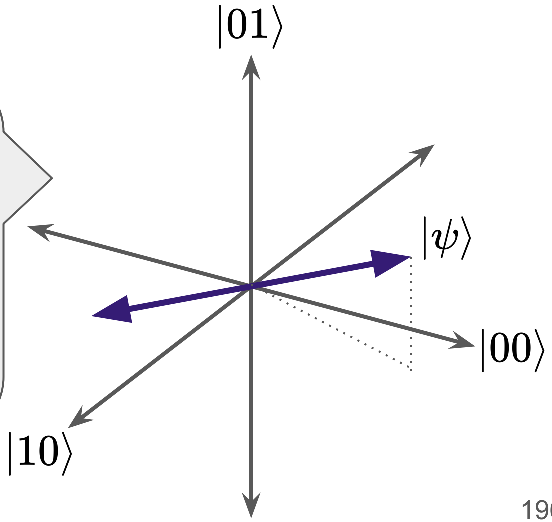
$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$|\psi\rangle =$ 


If we measure, the probability of getting outcome $x$ is $|\alpha_x|^2$

Unfortunately, we can't easily depict 4-dimensional vectors, so you'll have to imagine it! This is a 3D depiction.



Barak Nehoran (Postdoc, CS Department, Columbia University)

# Multiple Qubits

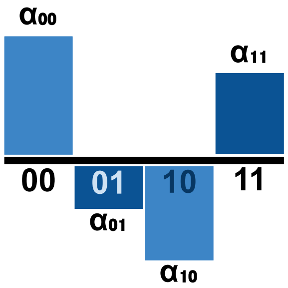
That is, this is any unit vector on these four basis vectors.

General two-qubit state:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

$$|\psi\rangle =$$




If we measure, the probability of getting outcome $x$ is $|\alpha_x|^2$

### Partial Measurement

If we measure **just the first qubit**,

We get outcome **0** with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$,

and the remaining quantum state is the state

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{|\alpha_{00}|^2 + |\alpha_{01}|^2}$$

the normalized projection onto the subspace spanned by $|00\rangle$ and $|01\rangle$.

# Examples of two-qubit states

$$|0\rangle \otimes |1\rangle = |0, 1\rangle$$

# Examples of two-qubit states

$$|0\rangle \otimes |1\rangle = |0,1\rangle$$

$$\begin{aligned}
|+\rangle \otimes |-\rangle &= \frac{1}{2}\Big( |0\rangle + |1\rangle \Big) \otimes \Big( |0\rangle - |1\rangle \Big) \\
&= \frac{1}{2}\Big( |0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle \Big)
\end{aligned}$$

# Examples of two-qubit states

$$|0\rangle \otimes |1\rangle = |0,1\rangle$$

$$\begin{aligned} |+\rangle \otimes |-\rangle &= \frac{1}{2}\Big( |0\rangle + |1\rangle \Big) \otimes \Big( |0\rangle - |1\rangle \Big) \\ &= \frac{1}{2}\Big( |0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle \Big) \end{aligned}$$

$$\frac{1}{\sqrt{2}}\Big( |0,0\rangle + |1,1\rangle \Big) \qquad \frac{1}{\sqrt{2}}\Big( |0,1\rangle - |1,0\rangle \Big)$$

# Examples of two-qubit states

$$|0\rangle \otimes |1\rangle = |0,1\rangle$$

$$\begin{aligned}|+\rangle \otimes |-\rangle &= \frac{1}{2}\Big(\,|0\rangle + |1\rangle\,\Big) \otimes \Big(\,|0\rangle - |1\rangle\,\Big)\\ &= \frac{1}{2}\Big(\,|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle\,\Big)\end{aligned}$$

$$\frac{1}{\sqrt{2}}\Big(\,|0,0\rangle + |1,1\rangle\,\Big) \qquad\qquad \frac{1}{\sqrt{2}}\Big(\,|0,1\rangle - |1,0\rangle\,\Big)$$

The first two were built from single-qubit states. **Can the last two be?**

# Product states and entangled states

A state that can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$ is called a **product state**.

# Product states and entangled states

A state that can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$ is called a **product state**.

Try it for $\frac{1}{\sqrt{2}}(|0,1\rangle - |1,0\rangle)$. We would need

$$\left(a\,|0\rangle + b\,|1\rangle\right) \otimes \left(c\,|0\rangle + d\,|1\rangle\right) = ac\,|0,0\rangle + ad\,|0,1\rangle + bc\,|1,0\rangle + bd\,|1,1\rangle\,,$$

so $ad = \frac{1}{\sqrt{2}}$ and $bc = -\frac{1}{\sqrt{2}}$, while $ac = bd = 0$.

# Product states and entangled states

A state that can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$ is called a **product state**.

Try it for $\frac{1}{\sqrt{2}}(|0,1\rangle - |1,0\rangle)$. We would need

$$\left(a\,|0\rangle + b\,|1\rangle\right) \otimes \left(c\,|0\rangle + d\,|1\rangle\right) = ac\,|0,0\rangle + ad\,|0,1\rangle + bc\,|1,0\rangle + bd\,|1,1\rangle\,,$$

so $ad = \frac{1}{\sqrt{2}}$ and $bc = -\frac{1}{\sqrt{2}}$, while $ac = bd = 0$.

But $ad \neq 0$ forces $a \neq 0$, so $ac = 0$ forces $c = 0$ — contradicting $bc \neq 0$. **No such factorization exists.**

# Product states and entangled states

A state that can be written as $|\psi_1\rangle \otimes |\psi_2\rangle$ is called a **product state**.

Try it for $\frac{1}{\sqrt{2}}(|0,1\rangle - |1,0\rangle)$. We would need

$$\left(a\,|0\rangle + b\,|1\rangle\right) \otimes \left(c\,|0\rangle + d\,|1\rangle\right) = ac\,|0,0\rangle + ad\,|0,1\rangle + bc\,|1,0\rangle + bd\,|1,1\rangle\,,$$

so $ad = \frac{1}{\sqrt{2}}$ and $bc = -\frac{1}{\sqrt{2}}$, while $ac = bd = 0$.

But $ad \neq 0$ forces $a \neq 0$, so $ac = 0$ forces $c = 0$ — contradicting $bc \neq 0$. **No such factorization exists.**

A state that is not a product state is **entangled**. This one and $\frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$ are both called **EPR pairs** or **Bell pairs**.

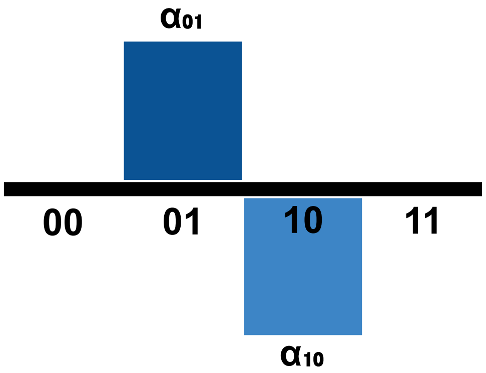
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Entanglement

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

# Quantum Entanglement

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

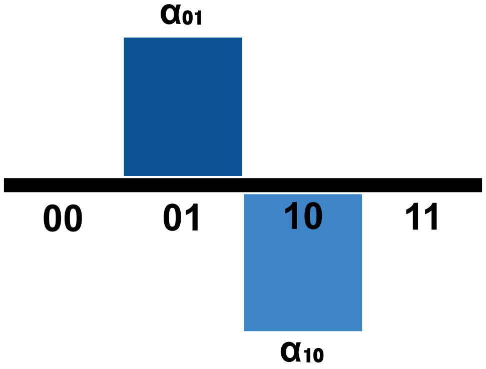


Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Entanglement

First qubit

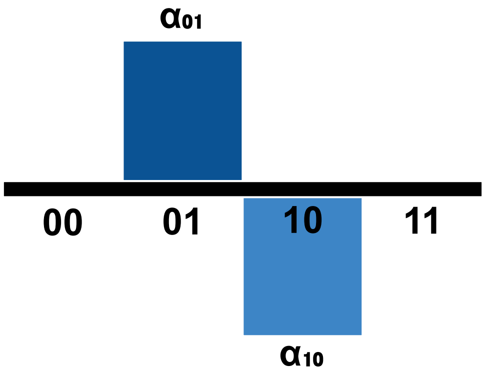
$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$



# Quantum Entanglement

First qubit     Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

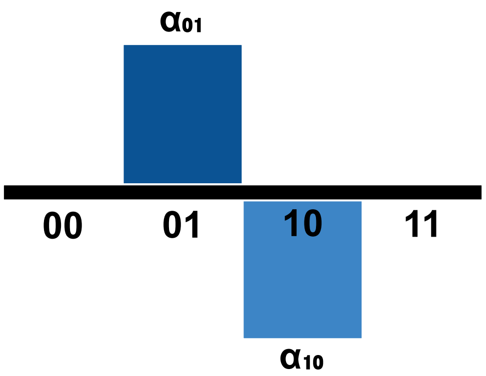


Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**).
What is the probability that we get **outcome 0**?

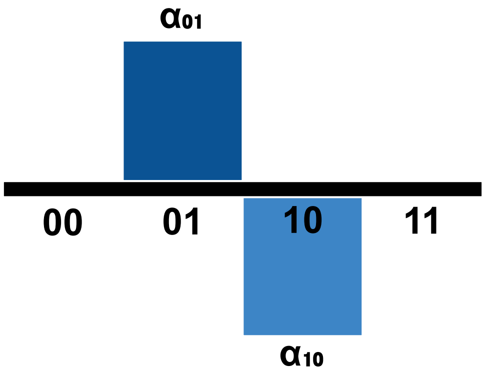
(a) 0
(b) 1/2
(c) 1/√2
(d) 1

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**). What is the probability that we get **outcome 0**?

(a) 0
(b) 1/2
(c) $1/\sqrt{2}$
(d) 1

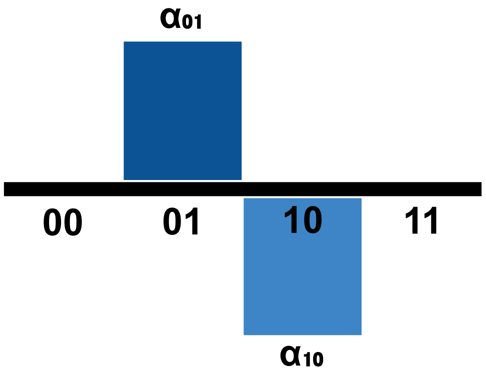
?

Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**). What is the probability that we get **outcome 0**?

(a) 0
(b) 1/2
(c) 1/√2
(d) 1

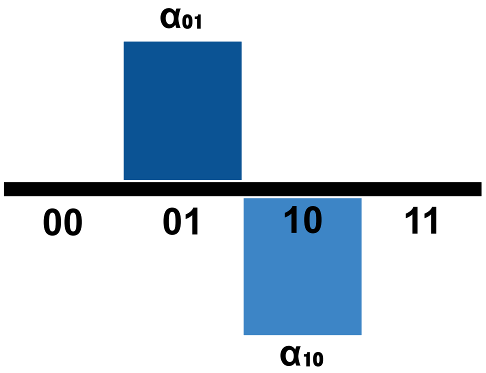
Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Entanglement

**First qubit** **Second qubit**

$$|\psi\rangle = \boxed{\frac{1}{\sqrt{2}}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**). What is the probability that we get **outcome 0**?

(a) 0
(b) 1/2
(c) 1/√2
(d) 1

$$\alpha_{00} = \frac{1}{\sqrt{2}}$$

?

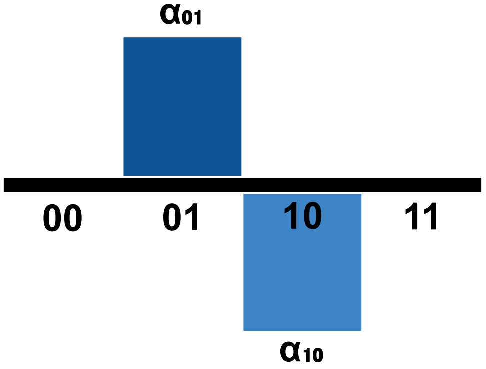
Barak Nehoran (Postdoc, CS Department, Columbia University)



# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \boxed{\frac{1}{\sqrt{2}}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**).
What is the probability that we get **outcome 0**?

(a) 0
(b) 1/2
(c) 1/√2
(d) 1

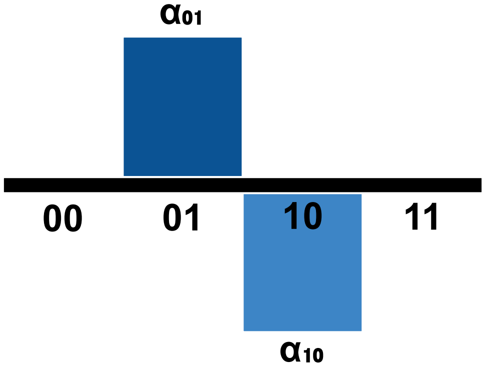
$$\alpha_{00} = \frac{1}{\sqrt{2}} \quad \Rightarrow \quad |\alpha_{00}|^2 = \frac{1}{2}$$

?

# Quantum Entanglement

**First qubit** **Second qubit**

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$



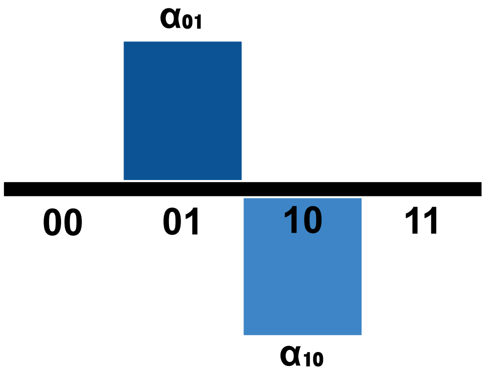

Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**).
Suppose we got **outcome 0**. What is the resulting quantum state?

(a) $|0\rangle|0\rangle$
(b) $|0\rangle|1\rangle$
(c) $(|0\rangle|0\rangle + |0\rangle|1\rangle)/\sqrt{2}$
(d) $|1\rangle|0\rangle$

# Quantum Entanglement

First qubit    Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**). Suppose we got **outcome 0**. What is the resulting quantum state?

(a) $|0\rangle|0\rangle$
(b) $|0\rangle|1\rangle$
(c) $(|0\rangle|0\rangle + |0\rangle|1\rangle)/\sqrt{2}$
(d) $|1\rangle|0\rangle$

?

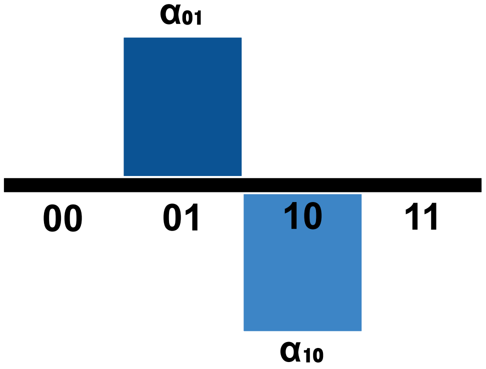
Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}\boxed{|0\rangle|1\rangle} - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**). Suppose we got **outcome 0**. What is the resulting quantum state?

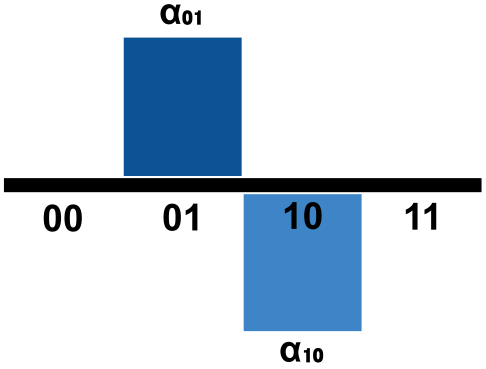
(a) $|0\rangle|0\rangle$
(b) $|0\rangle|1\rangle$
(c) $(|0\rangle|0\rangle + |0\rangle|1\rangle)/\sqrt{2}$
(d) $|1\rangle|0\rangle$

?

# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**).
Suppose we got **outcome 0**. What is the resulting quantum state?

(a) $|0\rangle|0\rangle$
(b) $|0\rangle|1\rangle$
(c) $(|0\rangle|0\rangle + |0\rangle|1\rangle)/\sqrt{2}$
(d) $|1\rangle|0\rangle$

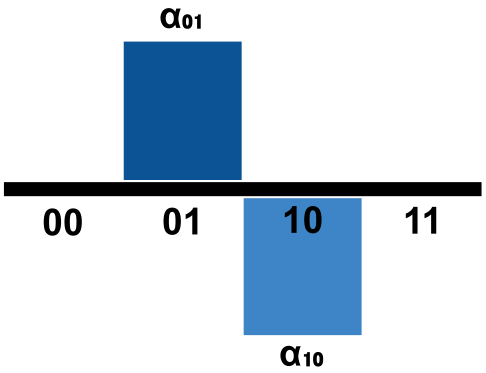
?

Notice that we now know **for certain** that the **second qubit** will measure to **outcome 1**, ***even before we've measured it!***

# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**).
Suppose we got **outcome 0**. What is the resulting quantum state?

(a) |0⟩|0⟩
(b) |0⟩|1⟩
(c) (|0⟩|0⟩ + |0⟩|1⟩)/√2
(d) |1⟩|0⟩

Notice that we now know **for certain** that the **second qubit** will measure to **outcome 1**, ***even before we've measured it!***
**Fact**: This is the case in any basis!

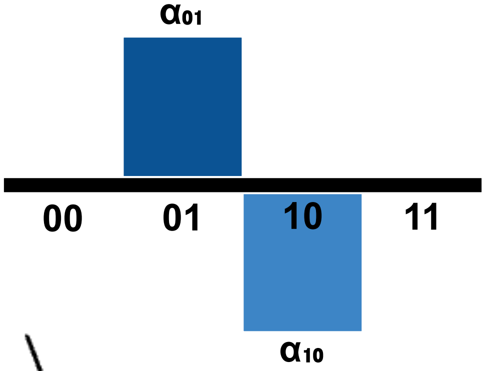
?

# Quantum Entanglement

First qubit     Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

$$= \frac{1}{\sqrt{2}}|+\rangle|-\rangle - \frac{1}{\sqrt{2}}|-\rangle|+\rangle$$




Suppose we **measure the first qubit** in the $|0\rangle$ vs $|1\rangle$ basis (a **partial measurement**).
Suppose we got **outcome 0**. What is the resulting quantum state?

(a) $|0\rangle|0\rangle$
(b) $|0\rangle|1\rangle$
(c) $(|0\rangle|0\rangle + |0\rangle|1\rangle)/\sqrt{2}$
(d) $|1\rangle|0\rangle$

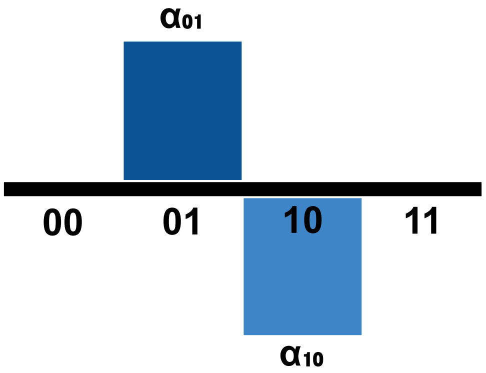
Notice that we now know **for certain** that the **second qubit** will measure to **outcome 1**, ***even before we've measured it!***
**Fact**: This is the case in any basis!

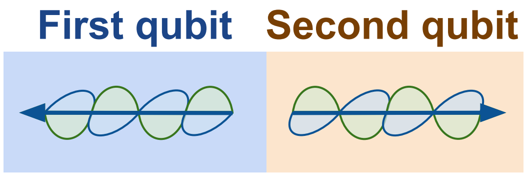
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$



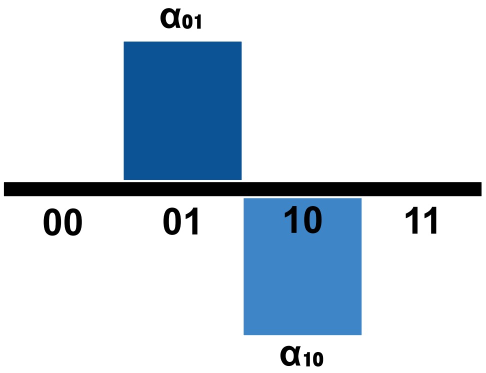



Barak Nehoran (Postdoc, CS Department, Columbia University)

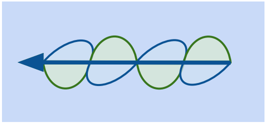
# Quantum Entanglement

First qubit Second qubit

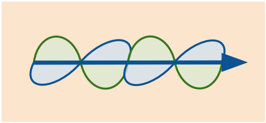
$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




First qubit



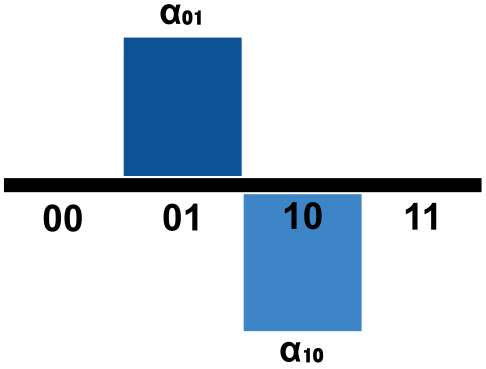
Second qubit



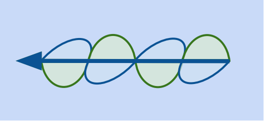
# Quantum Entanglement

First qubit Second qubit

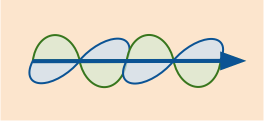
$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$




First qubit



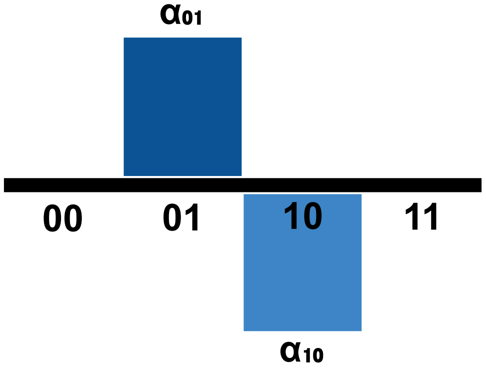
Second qubit

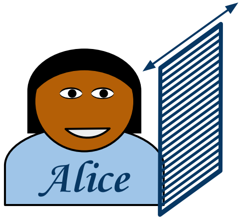


# Quantum Entanglement

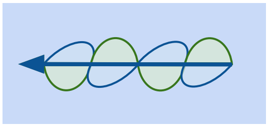
First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

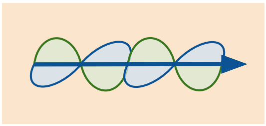


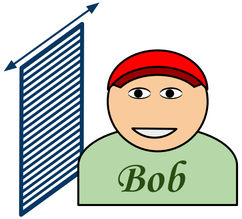




First qubit



Second qubit

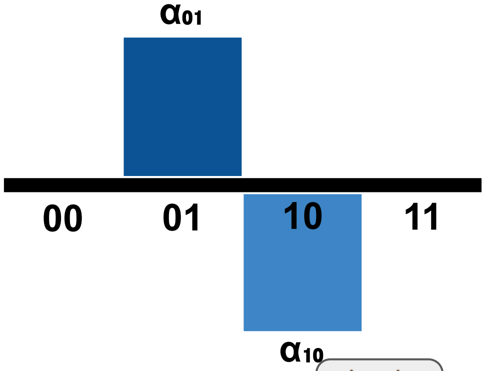


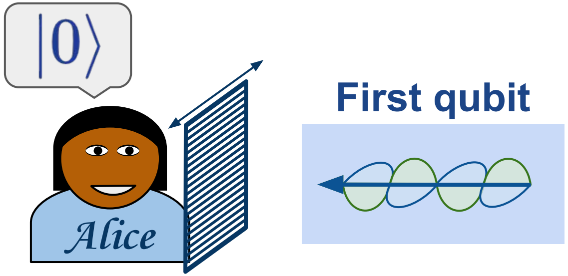


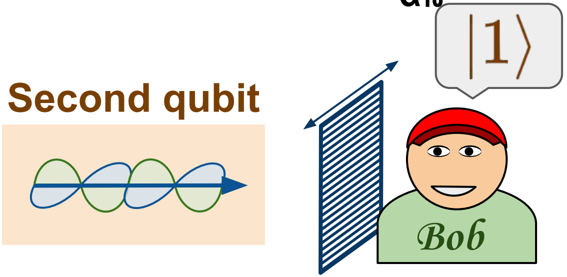
# Quantum Entanglement

First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$



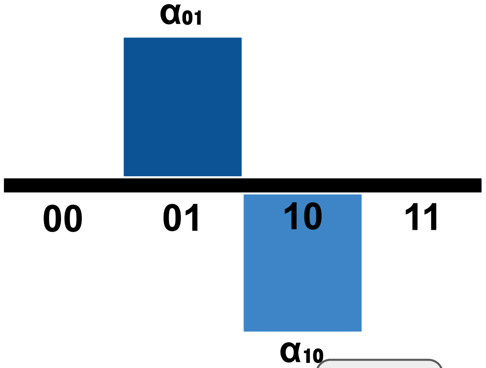



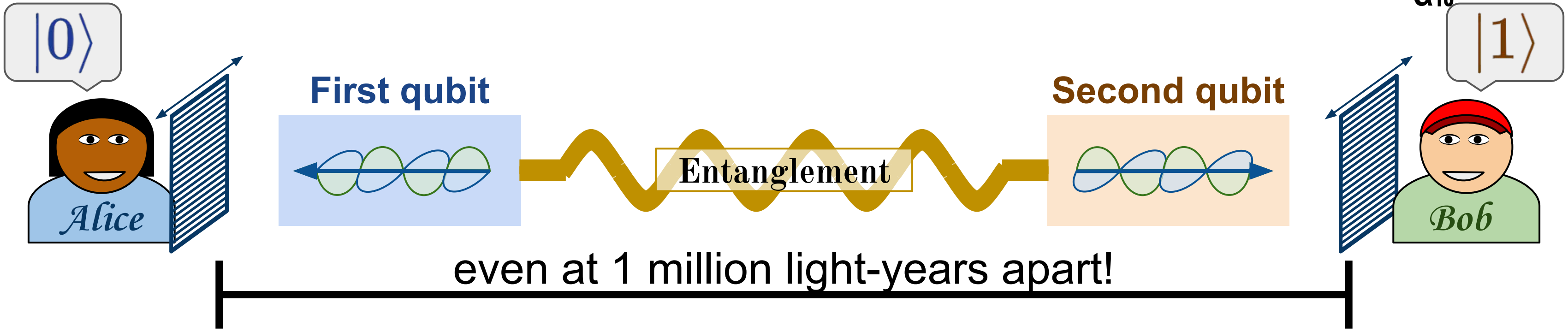



# Quantum Entanglement

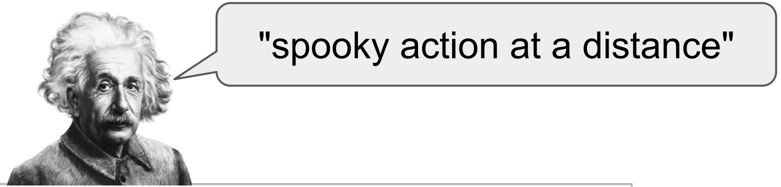
First qubit Second qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$



# Quantum Entanglement



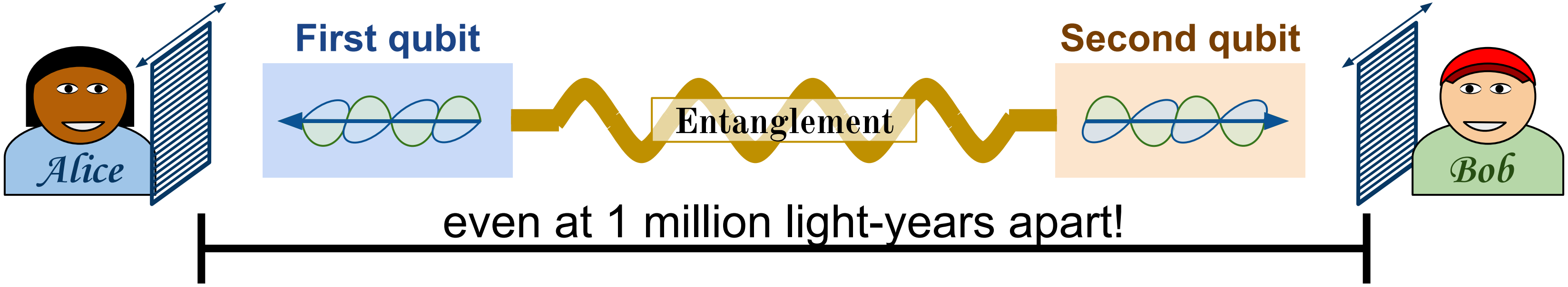

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

## Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. Einstein, B. Podolsky and N. Rosen, *Institute for Advanced Study, Princeton, New Jersey*

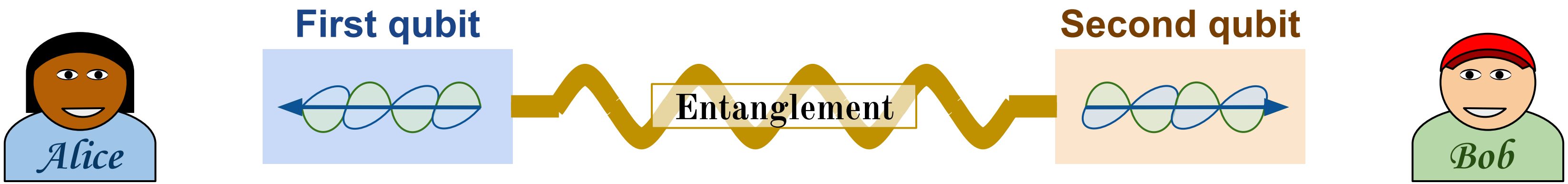
(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function



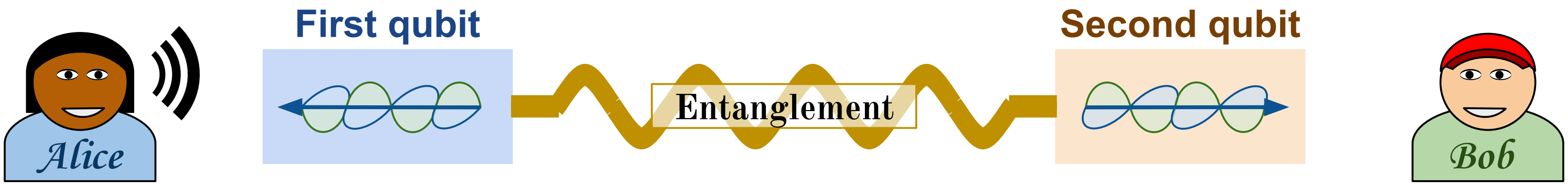
Barak Nehoran (Postdoc, CS Department, Columbia University)

# The No-Communication Theorem

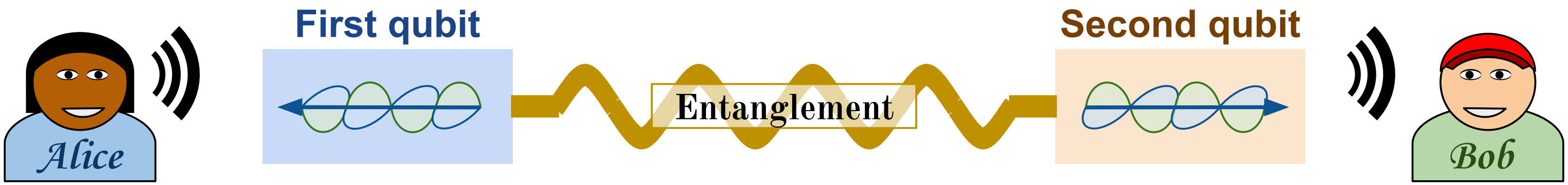


Barak Nehoran (Postdoc, CS Department, Columbia University)

# The No-Communication Theorem

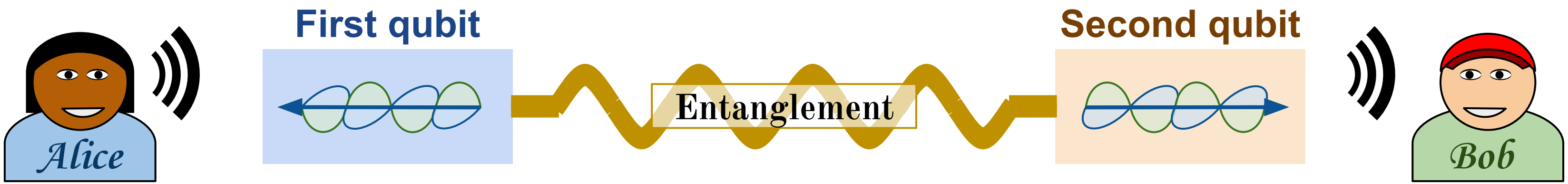


# The No-Communication Theorem



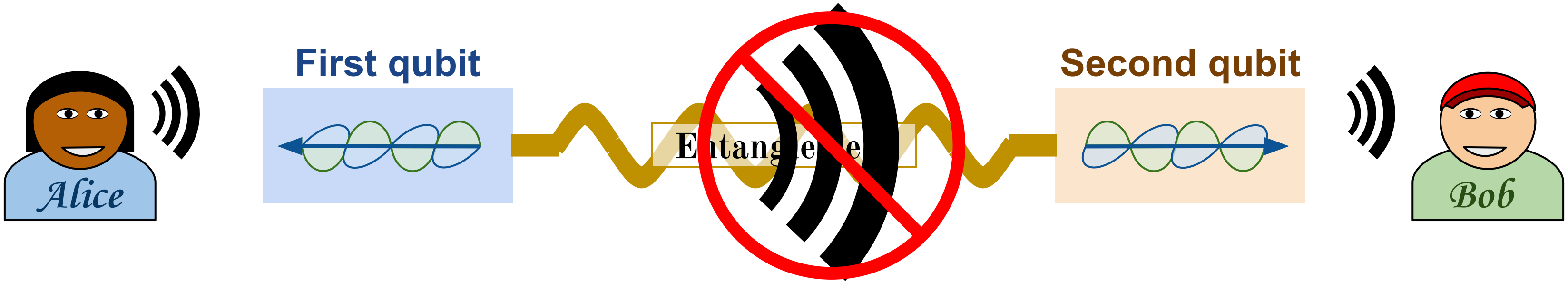
# The No-Communication Theorem

**Theorem**: Alice and Bob **cannot** use their entangled qubits to communicate information.



# The No-Communication Theorem

**Theorem**: Alice and Bob **cannot** use their entangled qubits to communicate information.

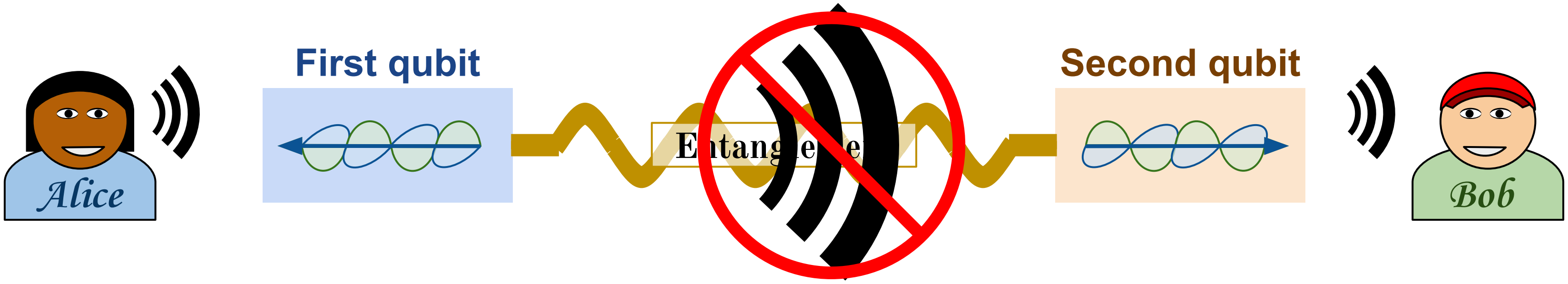


Barak Nehoran (Postdoc, CS Department, Columbia University)

# The No-Communication Theorem

**Theorem**: Alice and Bob **cannot** use their entangled qubits to communicate information.

That is, they can get **classically impossible correlations**, but **no communication**.



# Unitaries on two qubits

If $U, V$ are single-qubit unitaries, then $U \otimes V$ acts on each qubit separately:

$$(U \otimes V) |i\rangle |j\rangle = U|i\rangle \otimes V|j\rangle .$$

# Unitaries on two qubits

If $U, V$ are single-qubit unitaries, then $U \otimes V$ acts on each qubit separately:

$$(U \otimes V) |i\rangle |j\rangle = U|i\rangle \otimes V|j\rangle .$$

But just as not every state is a product state, **not every two-qubit unitary is a product unitary**.

# Unitaries on two qubits

If $U, V$ are single-qubit unitaries, then $U \otimes V$ acts on each qubit separately:

$$(U \otimes V) |i\rangle |j\rangle = U|i\rangle \otimes V|j\rangle .$$

But just as not every state is a product state, **not every two-qubit unitary is a product unitary**.

Those are the interesting ones: they can create entanglement out of unentangled inputs.

# CNOT makes a Bell pair

**CNOT** flips the second qubit exactly when the first is $|1\rangle$:

$$\begin{aligned} |0,0\rangle &\mapsto |0,0\rangle\,, & |0,1\rangle &\mapsto |0,1\rangle\,, \\ |1,0\rangle &\mapsto |1,1\rangle\,, & |1,1\rangle &\mapsto |1,0\rangle\,. \end{aligned}$$

# CNOT makes a Bell pair

**CNOT** flips the second qubit exactly when the first is $|1\rangle$:

$$\begin{aligned} |0,0\rangle &\mapsto |0,0\rangle\,, \qquad & |0,1\rangle &\mapsto |0,1\rangle\,, \\ |1,0\rangle &\mapsto |1,1\rangle\,, \qquad & |1,1\rangle &\mapsto |1,0\rangle\,. \end{aligned}$$

Starting from two photons, both vertical:

$$|0,0\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(\,|0,0\rangle + |1,0\rangle\,\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(\,|0,0\rangle + |1,1\rangle\,\Big).$$

# CNOT makes a Bell pair

**CNOT** flips the second qubit exactly when the first is $|1\rangle$:

$$|0,0\rangle \mapsto |0,0\rangle\,, \qquad |0,1\rangle \mapsto |0,1\rangle\,,$$
$$|1,0\rangle \mapsto |1,1\rangle\,, \qquad |1,1\rangle \mapsto |1,0\rangle\,.$$

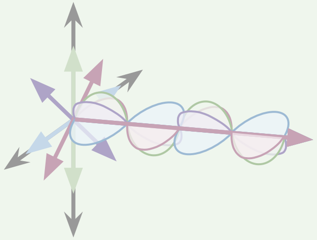
Starting from two photons, both vertical:

$$|0,0\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(\,|0,0\rangle + |1,0\rangle\,\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(\,|0,0\rangle + |1,1\rangle\,\Big).$$

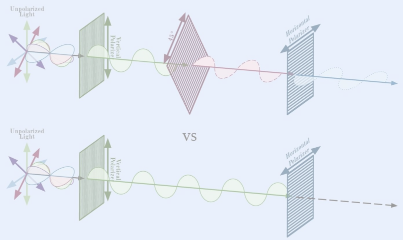
**A two-gate circuit produces the entangled pair Alice and Bob were sharing.**

# Outline

1 The Qubit



2 Quantum Measurement

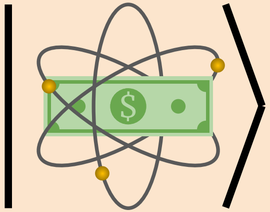


3 Quantum Entanglement & Many Qubits

First qubit Second qubit

$$\frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

4 No Cloning and Quantum Money



Barak Nehoran (Postdoc, CS Department, Columbia University)

# A Brief History of Quantum Cryptography

Public-key Cryptography

1968
**Quantum Money**
[Stephen Wiesner]



1976
Diffie Hellman Key Exchange
[Diffie, Hellman]

1977
RSA Cryptosystem
[Rivest, Shamir, Adelman]

1984
**Quantum Key Distribution**
[Bennett, Brassard]



1994
**Shor's Factoring Algorithm**
[Shor]

# A Brief History of Quantum Cryptography

Public-key Cryptography

1968
**Quantum Money**
[Stephen Wiesner]



1976
Diffie Hellman Key Exchange
[Diffie, Hellman]

1977
RSA Cryptosystem
[Rivest, Shamir, Adelman]

1984
**Quantum Key Distribution**
[Bennett, Brassard]



1994
**Shor's Factoring Algorithm**
[Shor]

Barak Nehoran (Postdoc, CS Department, Columbia University)

# A Brief History of Quantum Cryptography

Public-key Cryptography

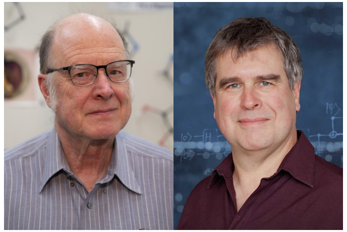
1968
Quantum Money
[Stephen Wiesner]



1976
Diffie Hellman Key Exchange
[Diffie, Hellman]

1977
RSA Cryptosystem
[Rivest, Shamir, Adelman]

1984
**Quantum Key Distribution**
[Bennett, Brassard]



1994
Shor's Factoring Algorithm
[Shor]

# A Brief History of Quantum Cryptography

Broken by quantum computers

Public-key Cryptography

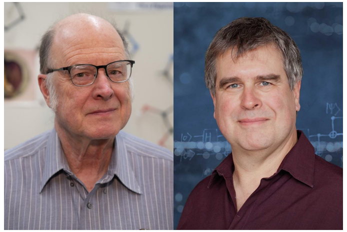
**1968**
Quantum Money
[Stephen Wiesner]



**1976**
~~Diffie Hellman Key Exchange~~
[Diffie, Hellman]

**1977**
~~RSA Cryptosystem~~
[Rivest, Shamir, Adelman]

**1984**
**Quantum Key Distribution**
[Bennett, Brassard]



**1994**
**Shor's Factoring Algorithm**
[Shor]

Barak Nehoran (Postdoc, CS Department, Columbia University)

# A Brief History of Quantum Cryptography

Broken by quantum computers

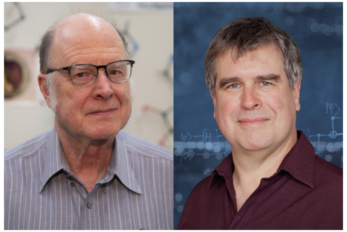
Public-key Cryptography

**1968** — **Quantum Money** [Stephen Wiesner]

**1976** — ~~Diffie Hellman Key Exchange~~ [Diffie, Hellman]

**1977** — ~~RSA Cryptosystem~~ [Rivest, Shamir, Adelman]

**1984** — **Quantum Key Distribution** [Bennett, Brassard]



**1994** — **Shor's Factoring Algorithm** [Shor]

# A Brief History of Quantum Cryptography

Broken by quantum computers

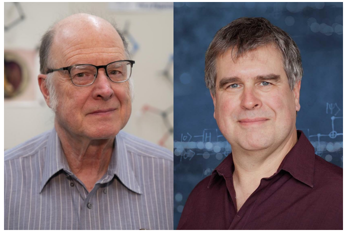
Public-key Cryptography

**1968** — **Quantum Money**
[Stephen Wiesner]

**1976** — ~~Diffie Hellman Key Exchange~~
[Diffie, Hellman]

**1977** — ~~RSA Cryptosystem~~
[Rivest, Shamir, Adelman]

**1984** — **Quantum Key Distribution**
[Bennett, Brassard]



**1994** — **Shor's Factoring Algorithm**
[Shor]

# A Brief History of Quantum Cryptography

Broken by quantum computers

Public-key Cryptography

**1968** — **Quantum Money** [Stephen Wiesner]

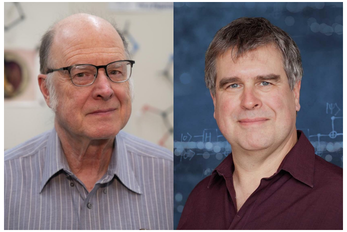
**1976** — ~~Diffie Hellman Key Exchange~~ [Diffie, Hellman]

**1977** — ~~RSA Cryptosystem~~ [Rivest, Shamir, Adelman]

**1984** — **Quantum Key Distribution** [Bennett, Brassard]

**1994** — **Shor's Factoring Algorithm** [Shor]

**While he was a PhD student at Columbia University**



# Cloning and the No-cloning Theorem

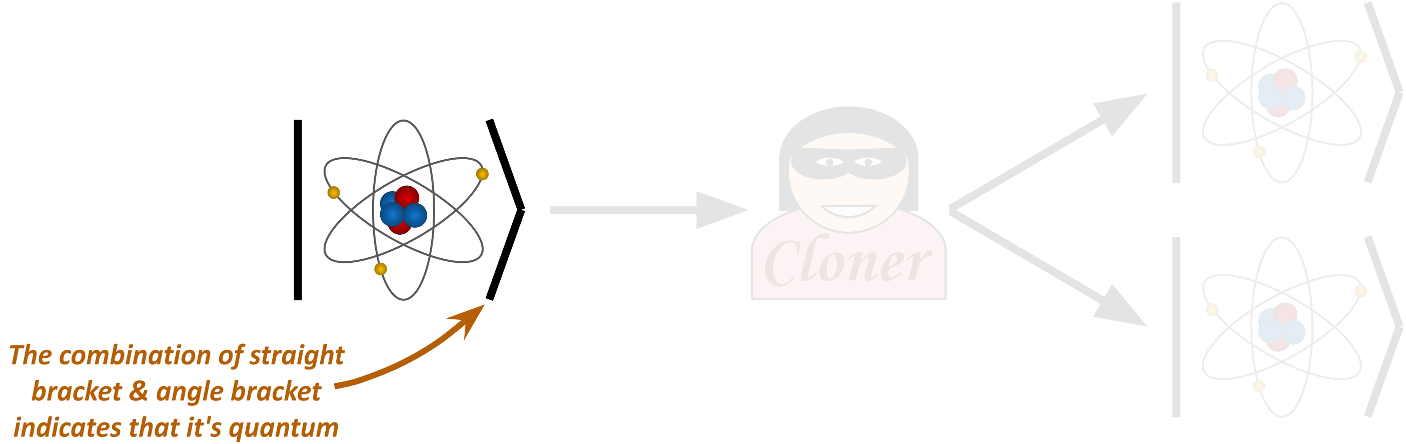



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Cloning and the No-cloning Theorem

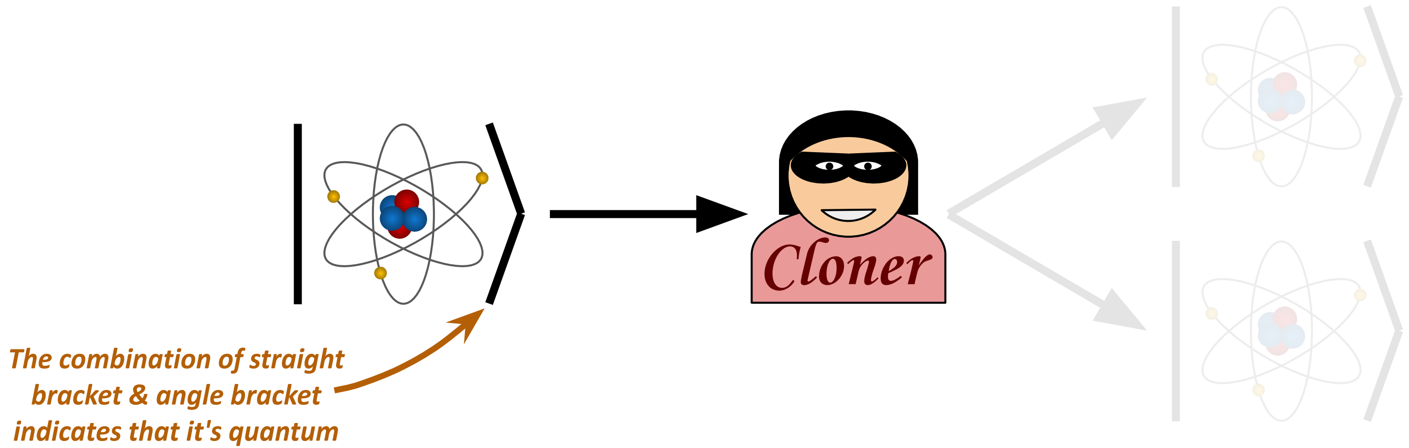



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Cloning and the No-cloning Theorem

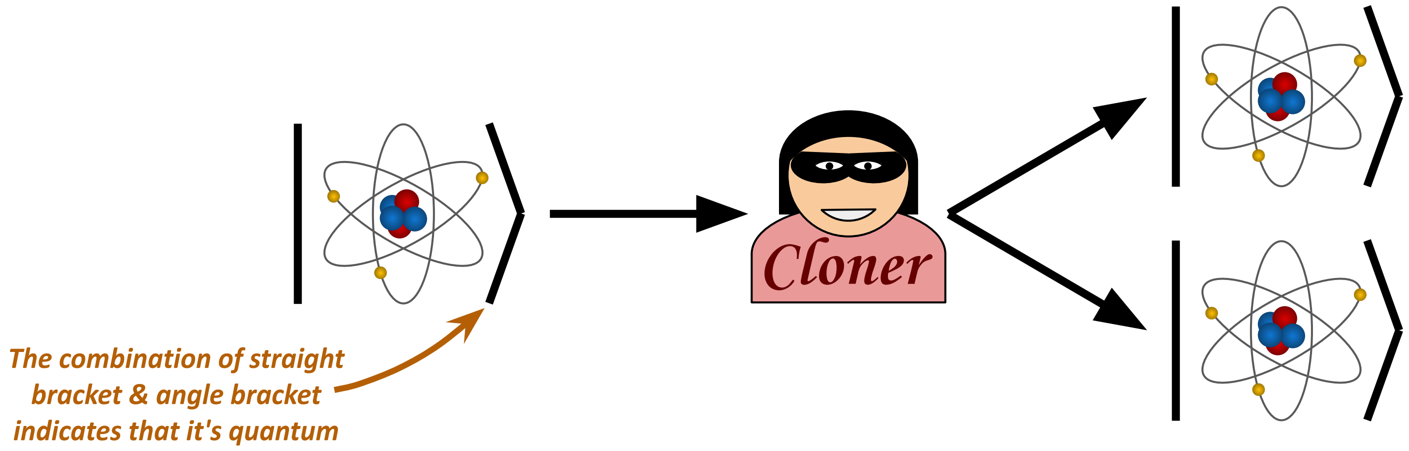



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Cloning and the No-cloning Theorem

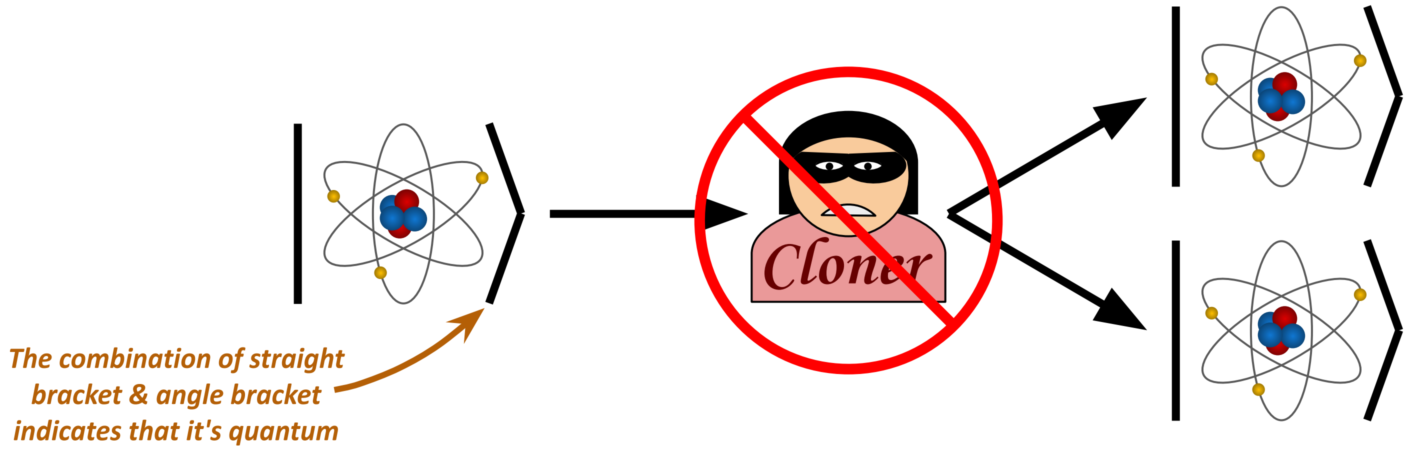



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Cloning and the No-cloning Theorem

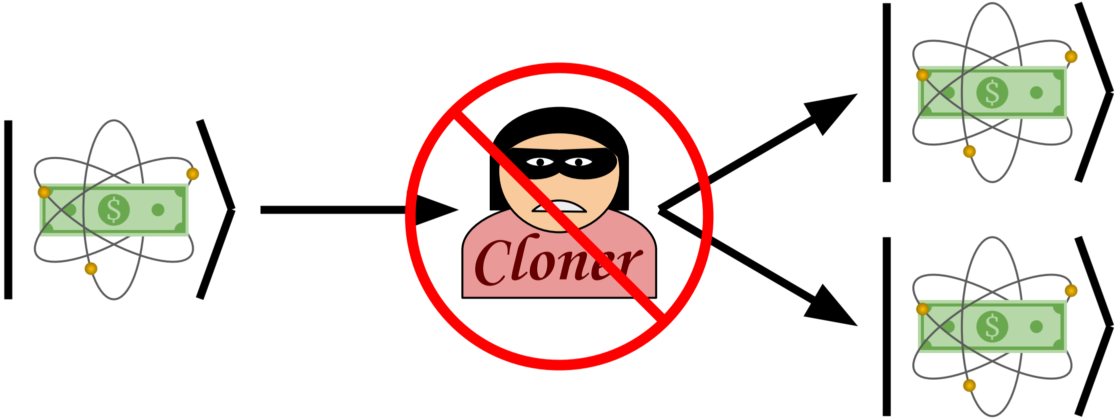



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Quantum Money [Wiesner '68]

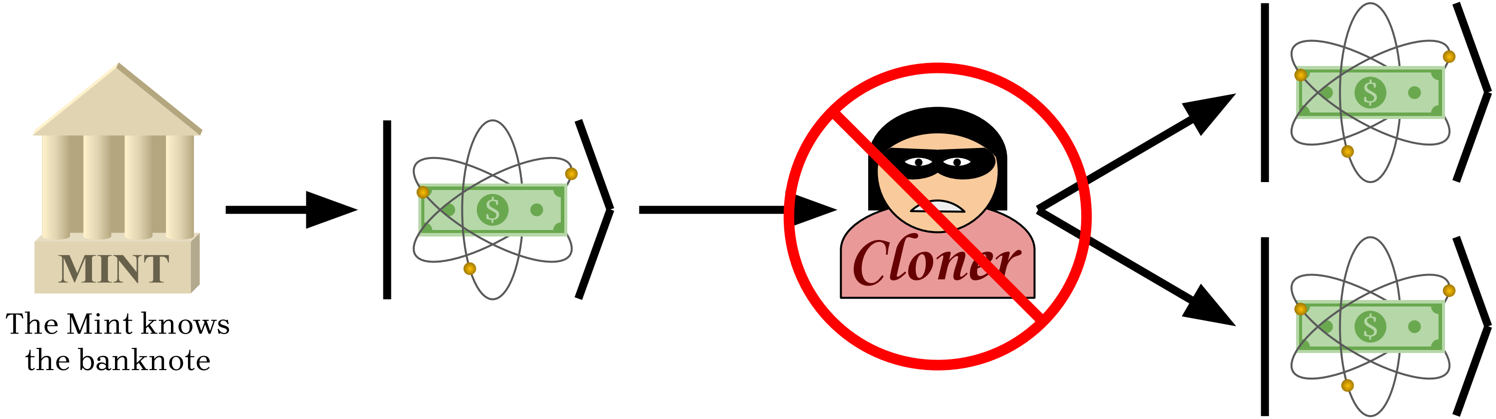



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Quantum Money [Wiesner '68]

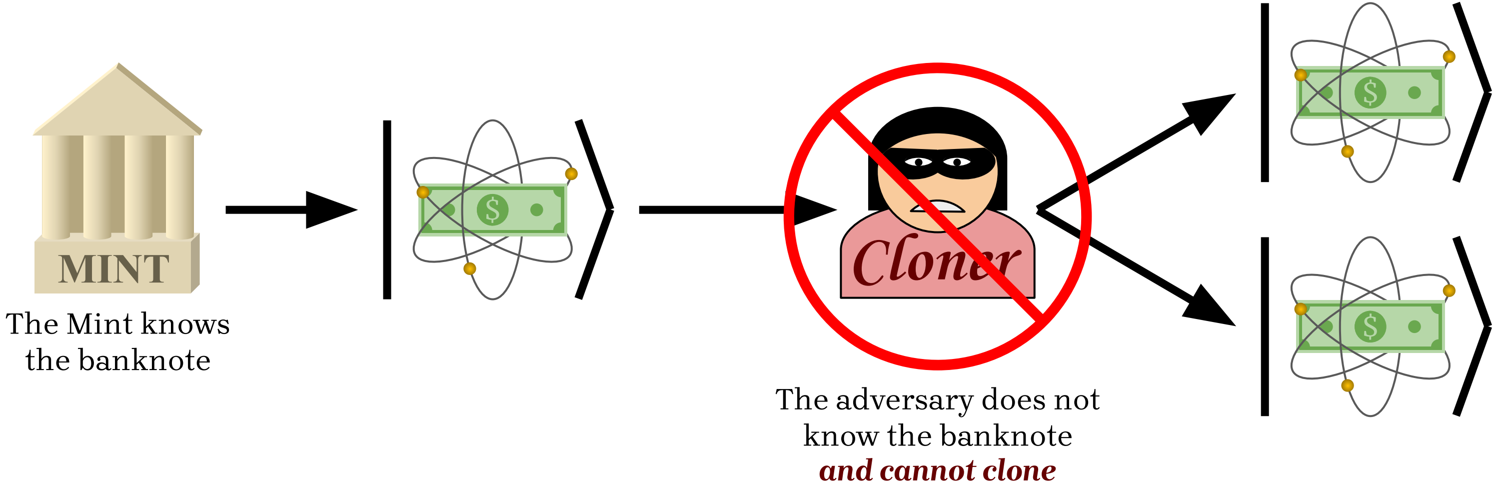



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Quantum Money [Wiesner '68]

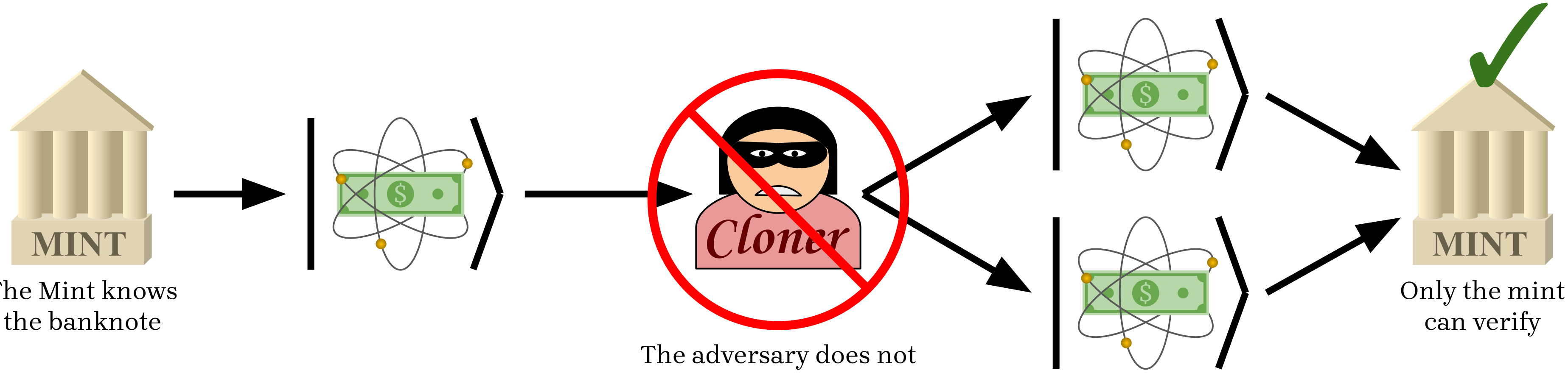



**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Quantum Money [Wiesner '68]




The Mint knows the banknote

The adversary does not know the banknote *and cannot clone*

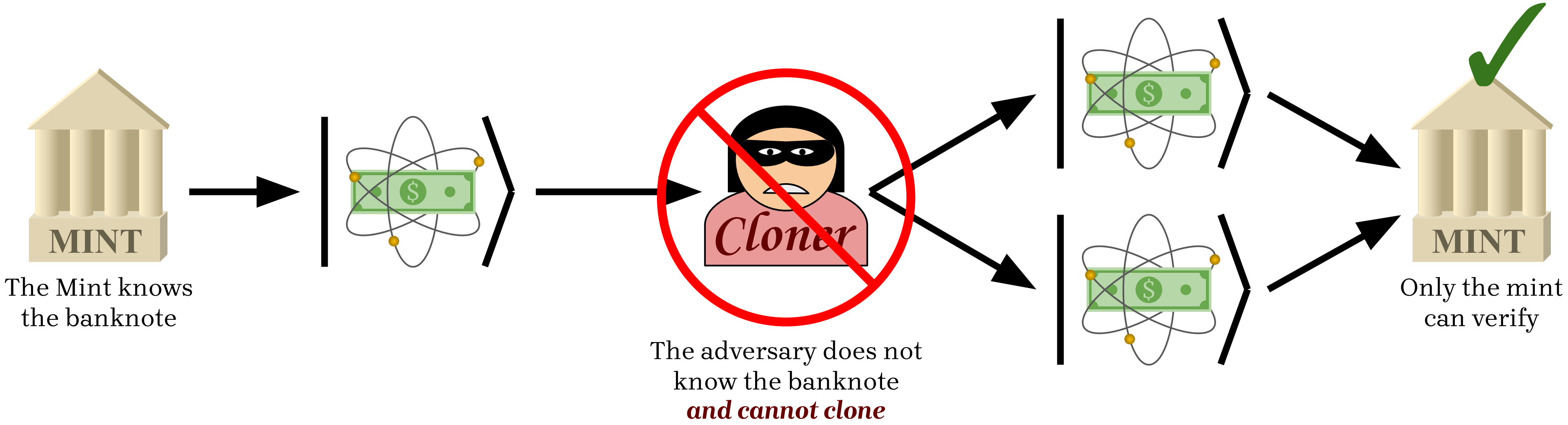
Only the mint can verify

**Cloning** = Making a faithful copy of a quantum state

The **No-Cloning Theorem** [Park 1970, Dieks 1982, Wootters & Zurek 1982]:

An *unknown* quantum state **cannot be cloned**.

# Quantum Money [Wiesner '68]




**Quantum money was the *first* quantum cryptographic protocol**
**(and was the inspiration for Quantum Key Distribution [BB84])**

| Physical Currency | Digital Currency |
|---|---|
|  |  |
| Coins, cash, gold, shells, valuable goods | Credit cards, checks, cryptocurrency |
| Person to person transactions | Can be transmitted, encrypted, etc. |
| Physical limitations (transmission, storage, etc.) | Third-party record of every transaction |
| No cryptographic security | |

## Physical Currency

Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

## Digital Currency



Credit cards, checks, cryptocurrency

Can be transmitted, encrypted, etc.

Third-party record of every transaction

## Physical Currency

Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

## Digital Currency



Credit cards, checks, cryptocurrency

Can be transmitted, encrypted, etc.

Third-party record of every transaction

## Physical Currency

## Digital Currency



Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

Credit cards, checks, cryptocurrency

Can be transmitted, encrypted, etc.

Third-party record of every transaction

## Physical Currency

Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

## Digital Currency



Credit cards, checks, cryptocurrency

Can be transmitted, encrypted, etc.

Third-party record of every transaction

Barak Nehoran (Postdoc, CS Department, Columbia University)

Columbia University in the City of New York

## Physical Currency

Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

## Digital Currency

Credit cards, checks, cryptocurrency

Can be transmitted, encrypted, etc.

Third-party record of every transaction

## Physical Currency

Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

## Digital Currency

Credit cards, checks, cryptocurrency

Can be transmitted, encrypted, etc.

Third-party record of every transaction

Barak Nehoran (Postdoc, CS Department, Columbia University)

## Physical Currency

Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

## Digital Currency

Credit cards, checks, cryptocurrency

Can be transmitted, encrypted, etc.

Third-party record of every transaction

## Physical Currency

<u>Coins, cash, gold, shells, valuable goods</u>

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

## Digital Currency

<u>Credit cards, checks, cryptocurrency</u>

Can be transmitted, encrypted, etc.

Third-party record of every transaction

Barak Nehoran (Postdoc, CS Department, Columbia University)

## Physical Currency

Coins, cash, gold, shells, valuable goods

Person to person transactions

Physical limitations (transmission, storage, etc.)

No cryptographic security

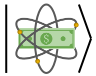
## Digital Currency

Credit cards, checks, cryptocurrency

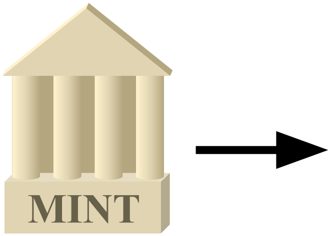
Can be transmitted, encrypted, etc.

Third-party record of every transaction

*Quantum Money*



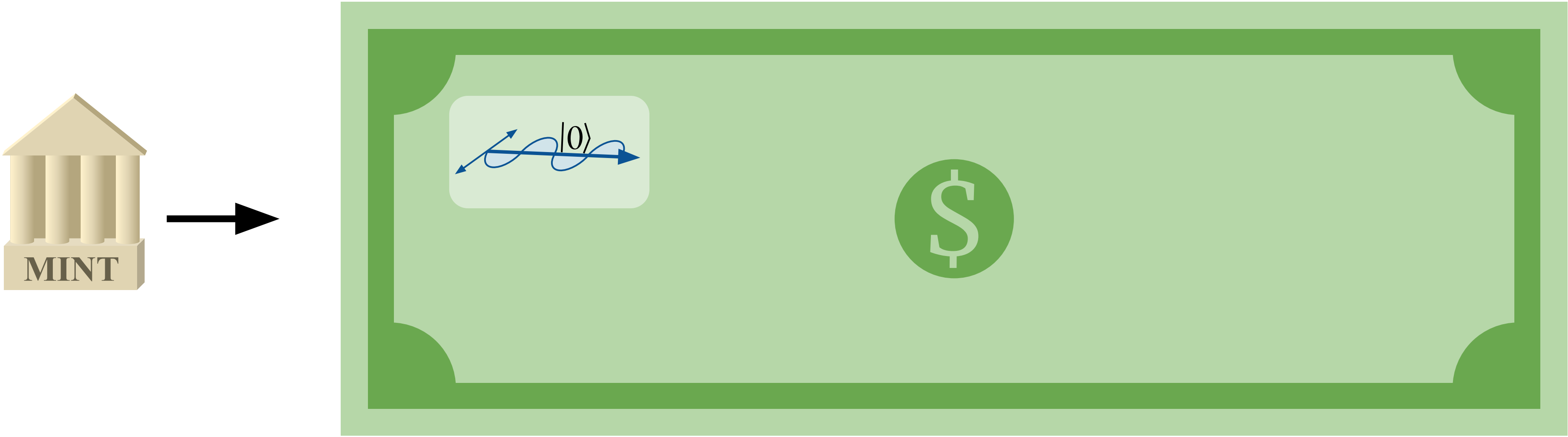
# Wiesner's Quantum Money [Wiesner '68]



# Wiesner's Quantum Money [Wiesner '68]

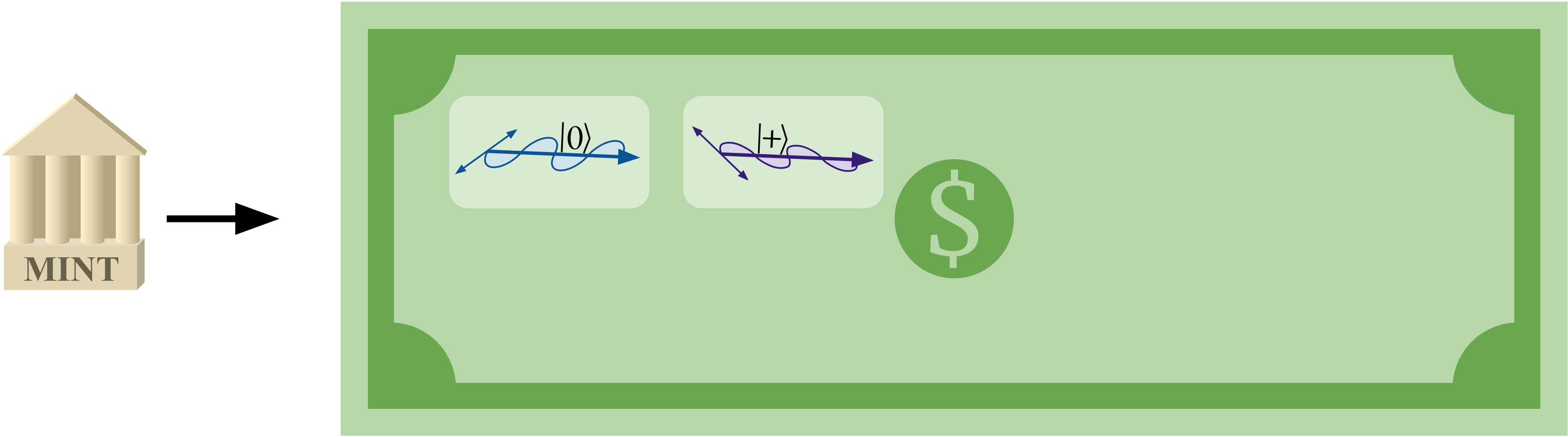
Barak Nehoran (Postdoc, CS Department, Columbia University)

# Wiesner's Quantum Money [Wiesner '68]

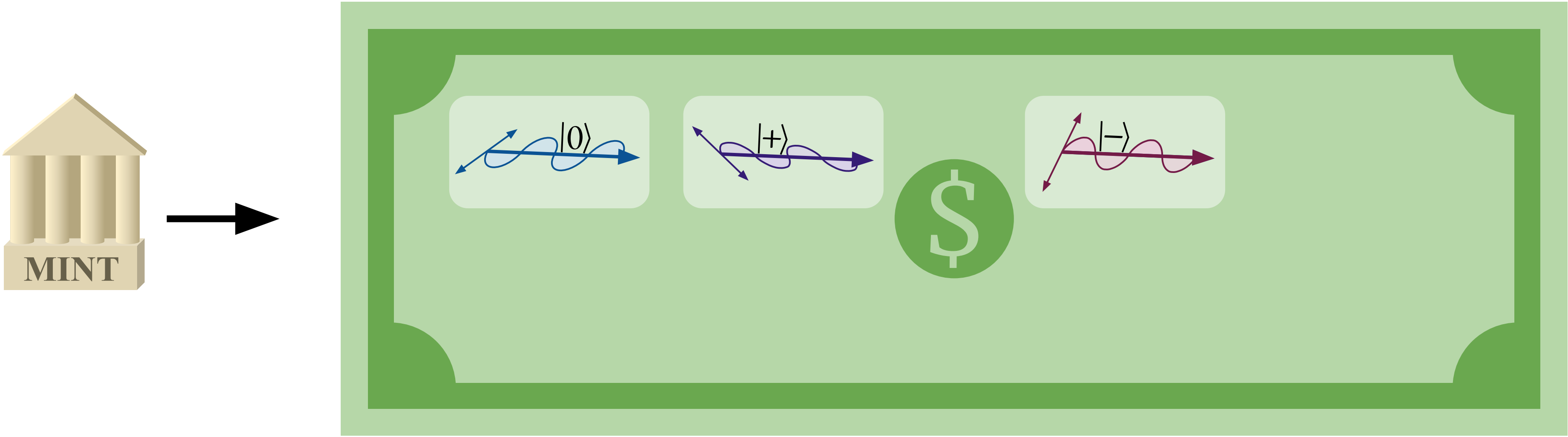


Barak Nehoran (Postdoc, CS Department, Columbia University)

# Wiesner's Quantum Money [Wiesner '68]

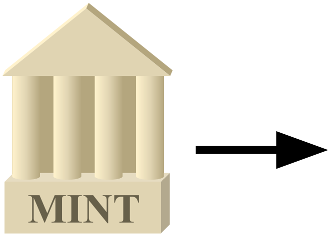


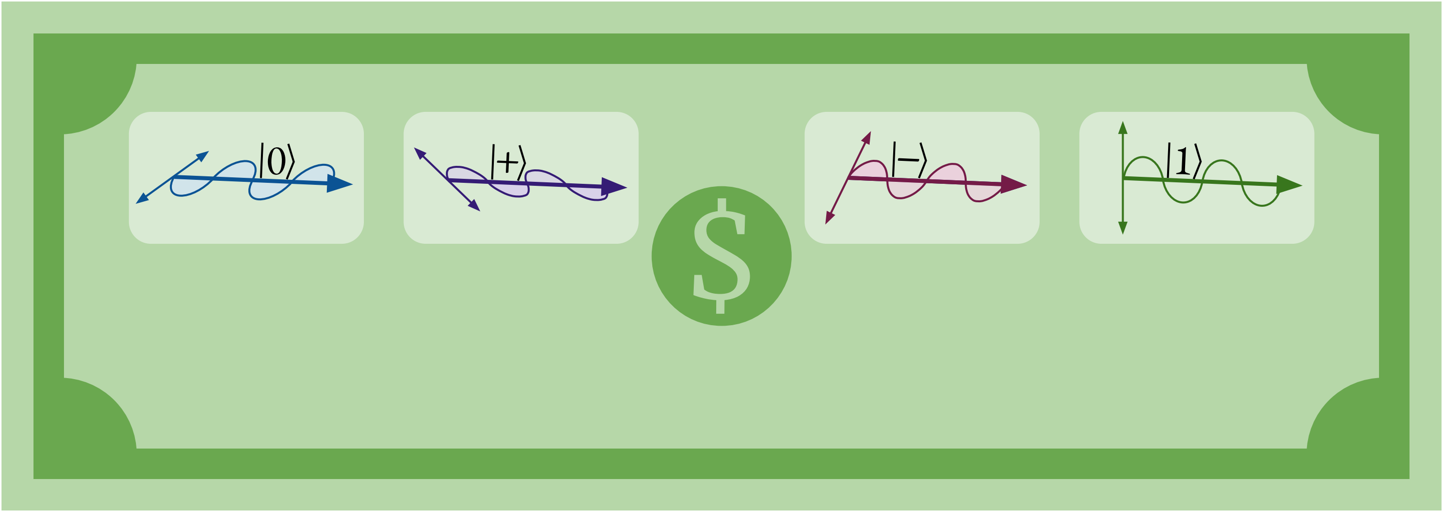
# Wiesner's Quantum Money [Wiesner '68]



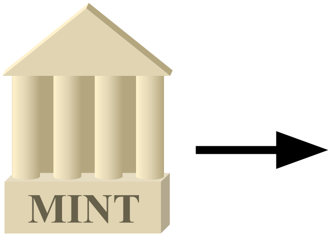
Barak Nehoran (Postdoc, CS Department, Columbia University)

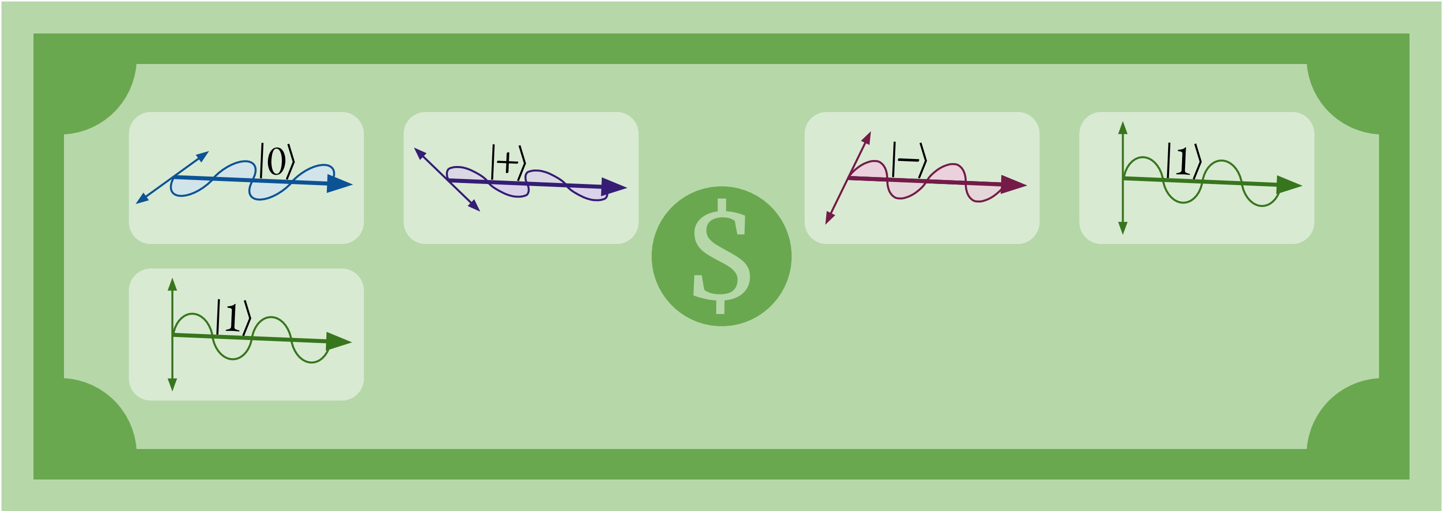

# Wiesner's Quantum Money [Wiesner '68]



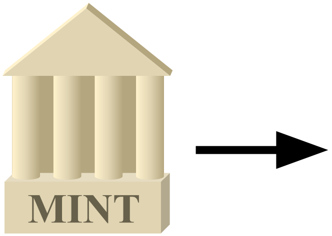



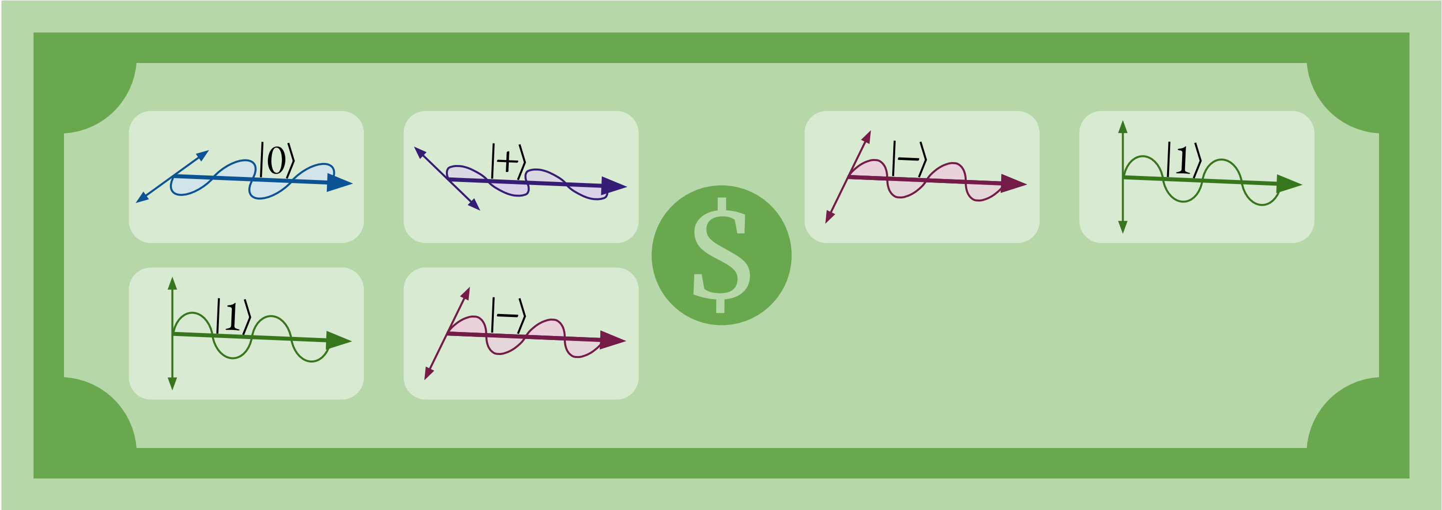
# Wiesner's Quantum Money [Wiesner '68]



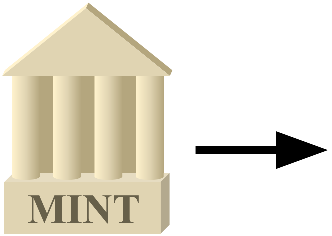
# Wiesner's Quantum Money [Wiesner '68]

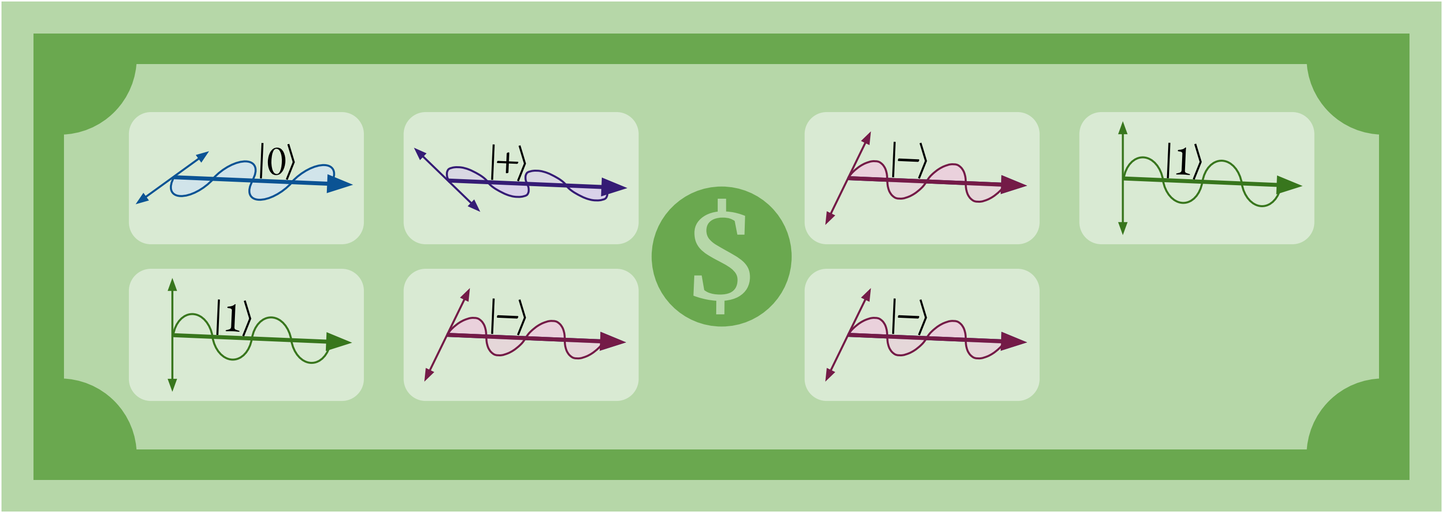


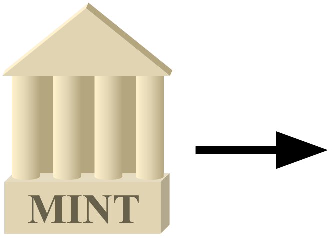
Barak Nehoran (Postdoc, CS Department, Columbia University)

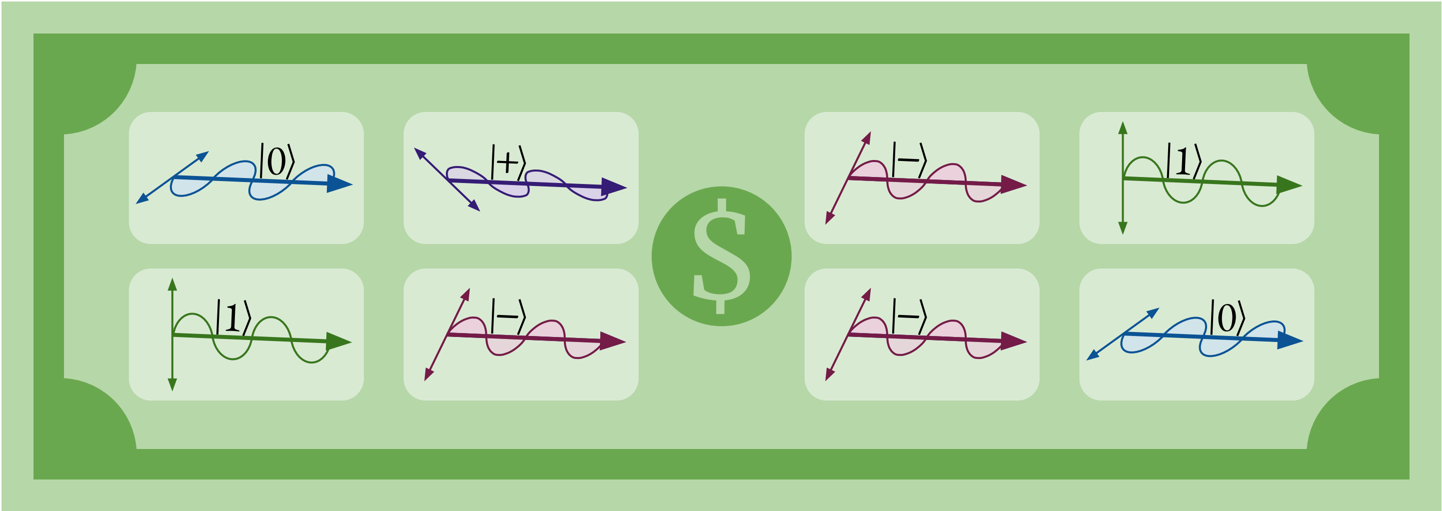
# Wiesner's Quantum Money [Wiesner '68]



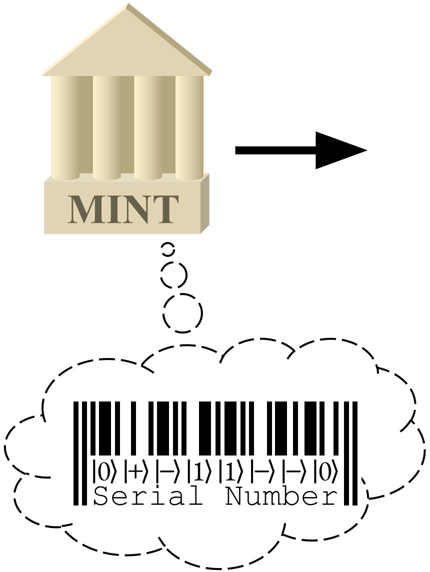



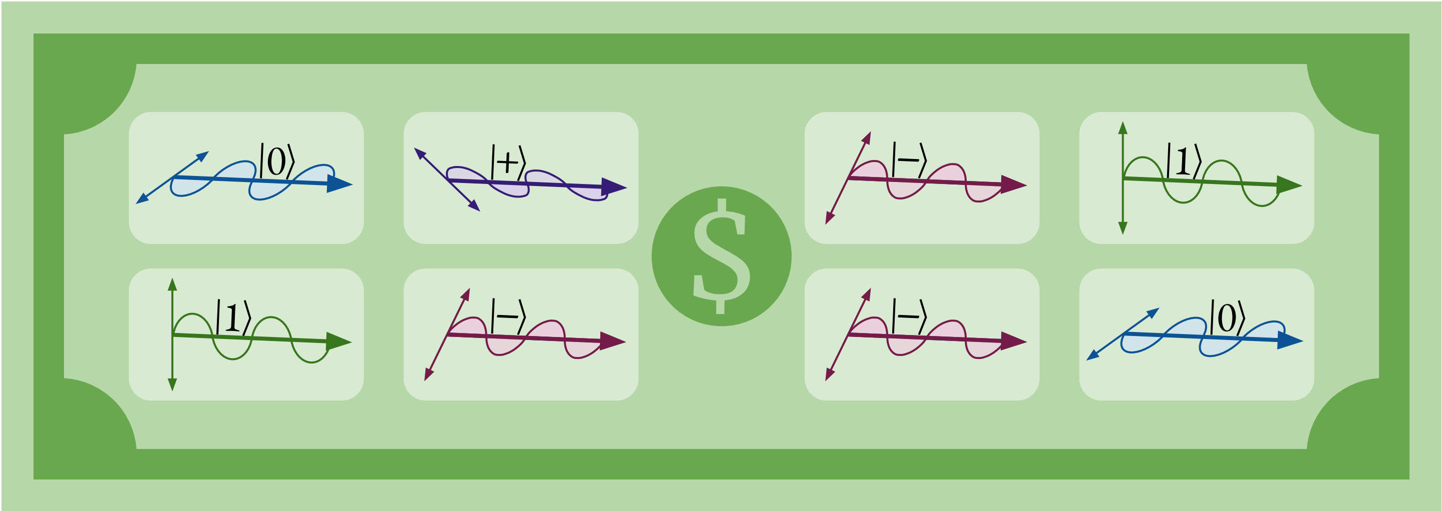
# Wiesner's Quantum Money [Wiesner '68]



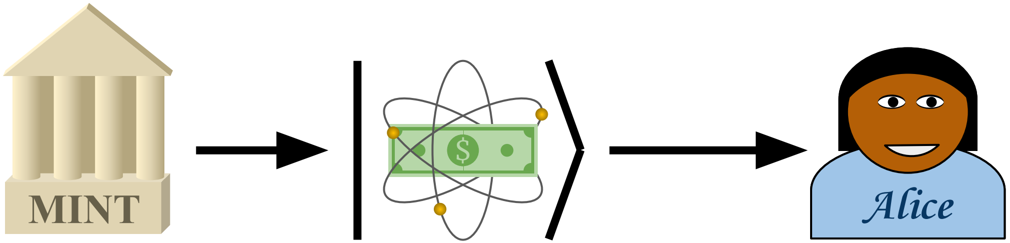



# Wiesner's Quantum Money [Wiesner '68]

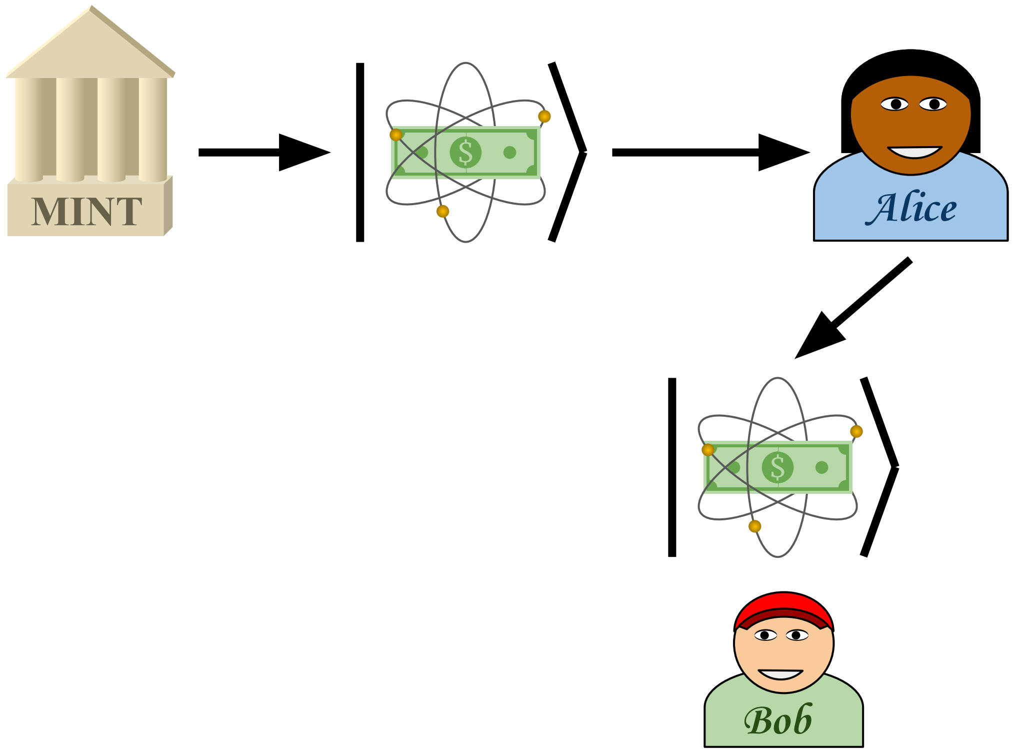


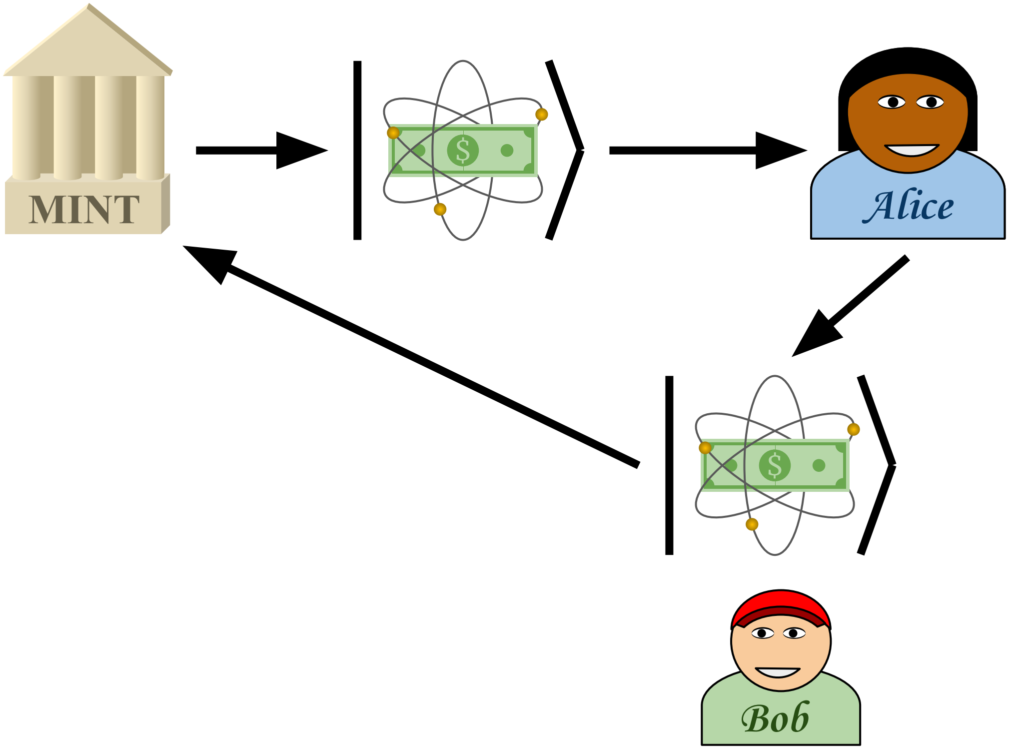
# Quantum Money [Wiesner '68]



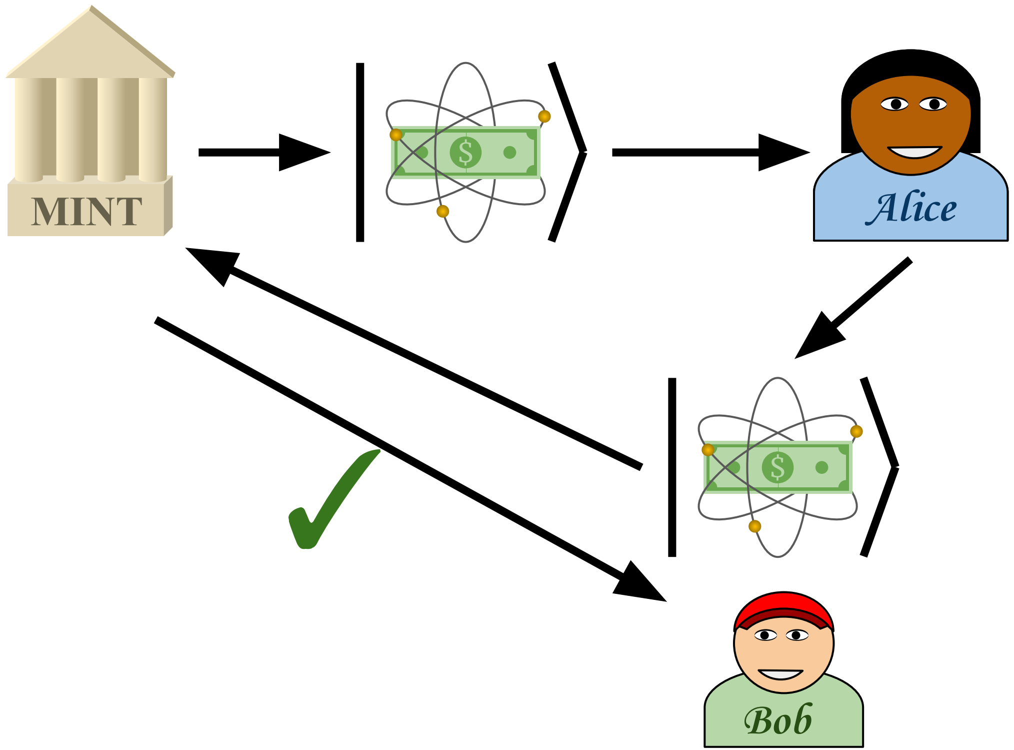
# Quantum Money [Wiesner '68]



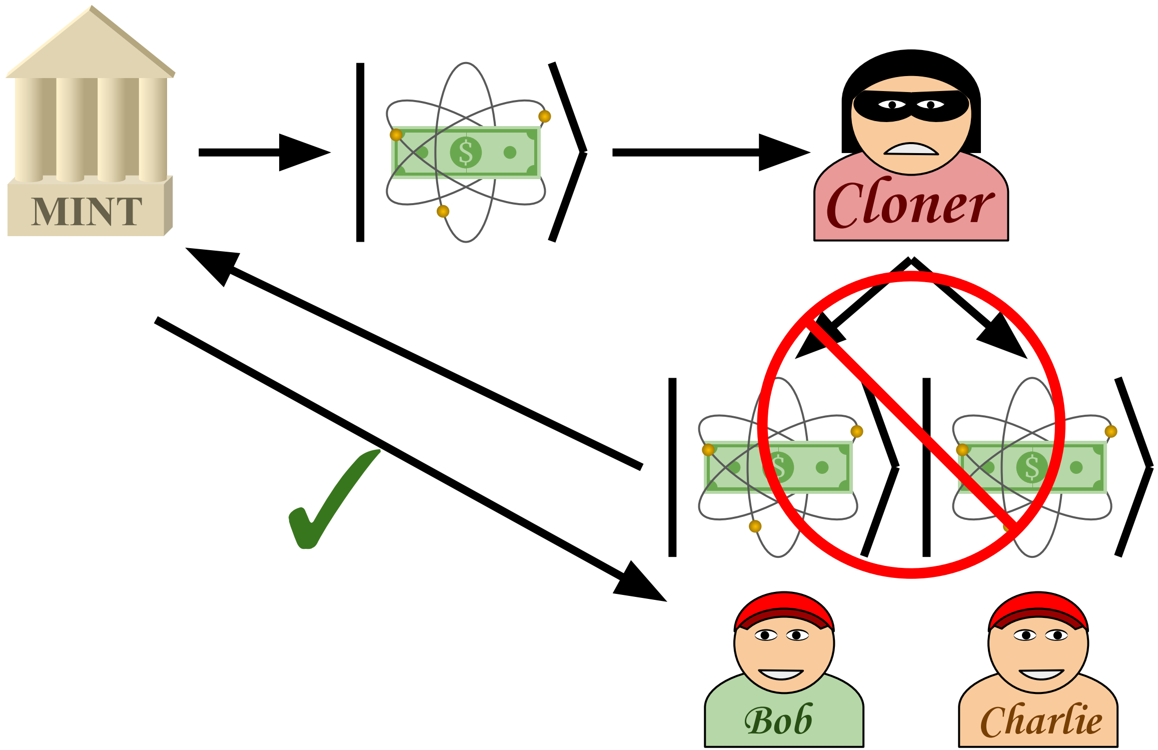
# Quantum Money [Wiesner '68]



# Quantum Money [Wiesner '68]



# Quantum Money [Wiesner '68]



# What “cannot be cloned” means precisely

There is no two-qubit unitary $U$ such that for **every** single-qubit state $|\psi\rangle$,

$$U\Big(|\psi\rangle \otimes \underbrace{|0\rangle}_{\text{blank slate}}\Big) = |\psi\rangle \otimes |\psi\rangle\,.$$

# What “cannot be cloned” means precisely

There is no two-qubit unitary $U$ such that for **every** single-qubit state $|\psi\rangle$,

$$U\Big(|\psi\rangle \otimes \underbrace{|0\rangle}_{\text{blank slate}}\Big) = |\psi\rangle \otimes |\psi\rangle\,.$$

Note what is *not* claimed: a machine that copies only $|0\rangle$ and $|1\rangle$ is easy — that is just CNOT. The theorem rules out one machine that works for **all** states at once.

## Proof sketch

Suppose such a $U$ existed. Then

$$U|0\rangle|0\rangle = |0\rangle|0\rangle \qquad \text{and} \qquad U|+\rangle|0\rangle = |+\rangle|+\rangle .$$

## Proof sketch

Suppose such a $U$ existed. Then

$$U|0\rangle|0\rangle = |0\rangle|0\rangle \qquad \text{and} \qquad U|+\rangle|0\rangle = |+\rangle|+\rangle\,.$$

Unitaries preserve inner products. The inputs have inner product

$$\left(\langle 0| \otimes \langle 0|\right)\left(|+\rangle \otimes |0\rangle\right) = \frac{1}{\sqrt{2}},$$

while the outputs have

$$\left(\langle 0| \otimes \langle 0|\right)\left(|+\rangle \otimes |+\rangle\right) = \frac{1}{2}.$$

# Proof sketch

Suppose such a $U$ existed. Then

$$U|0\rangle|0\rangle = |0\rangle|0\rangle \qquad \text{and} \qquad U|+\rangle|0\rangle = |+\rangle|+\rangle.$$

Unitaries preserve inner products. The inputs have inner product

$$(\langle 0| \otimes \langle 0|)(|+\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}},$$

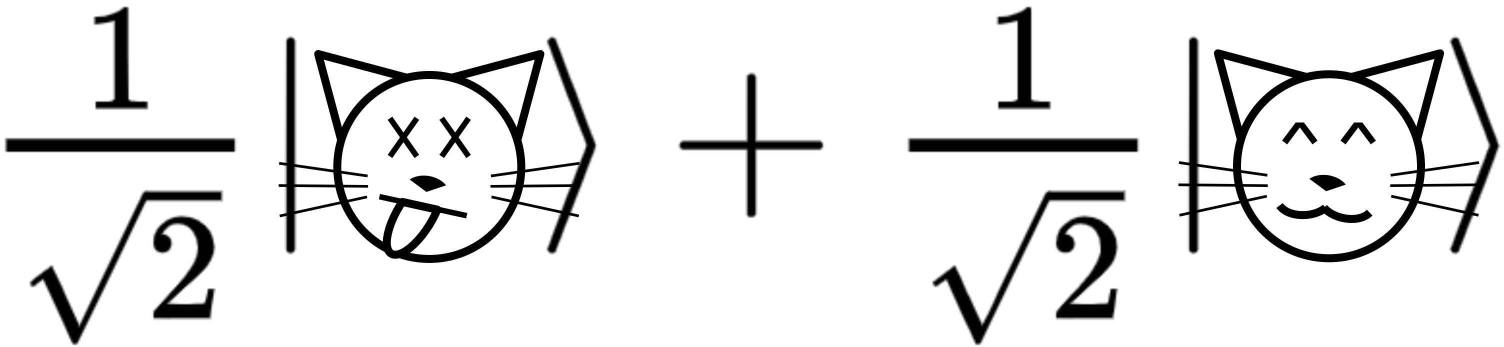
while the outputs have

$$(\langle 0| \otimes \langle 0|)(|+\rangle \otimes |+\rangle) = \frac{1}{2}.$$

$\frac{1}{\sqrt{2}} \neq \frac{1}{2}$, so no such $U$ exists. **Cloning would let you distinguish non-orthogonal states.**

Barak Nehoran (Postdoc, CS Department, Columbia University)

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK



# 10 minute break