Quantum Information Refresher

*Borrowed from a tutorial at the BIU Winter School on Cryptography 2021 by Henry Yuen

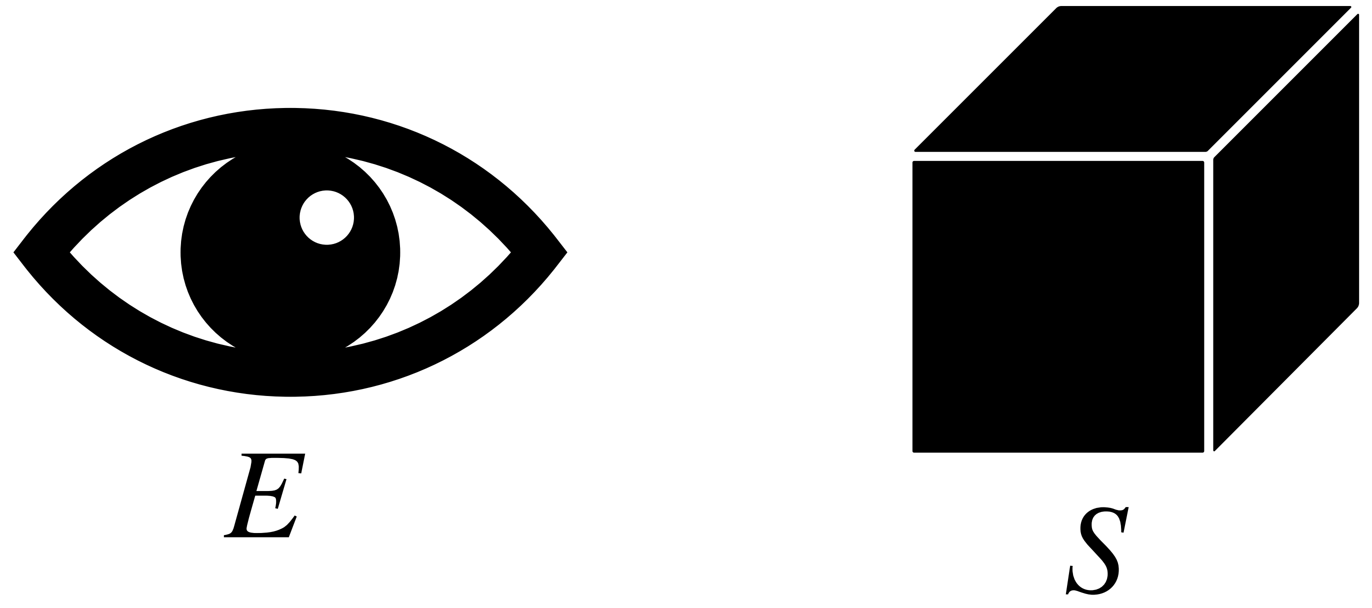
Starting Point

Starting Point

Quantum Information theory is a generalization of probability theory where probabilities can be negative or even complex numbers

Starting Point

Consider a system S with d distinguishable states, labeled $0, \ldots, d-1$ and an external observer E

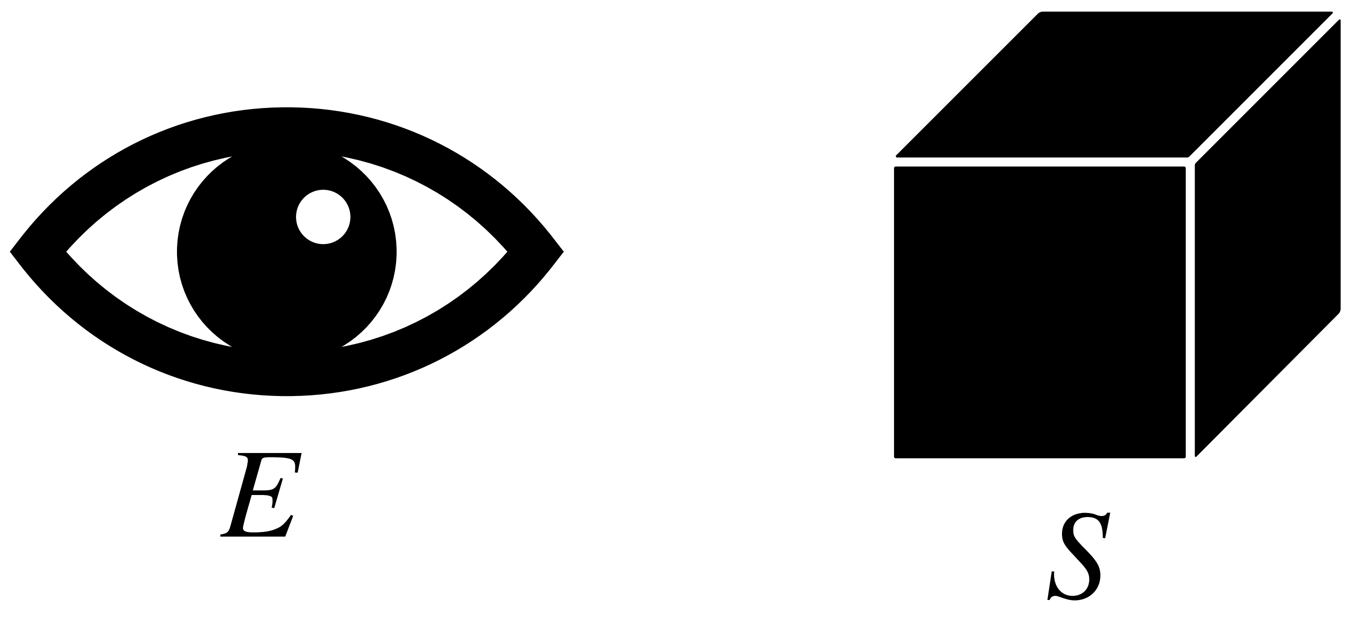


Measurement The external observer E can measure the state of S

Isolated Evolution The system S can evolve without interacting with the external observer E

Classical Physics

Initially the observer E assigns a state to the system S



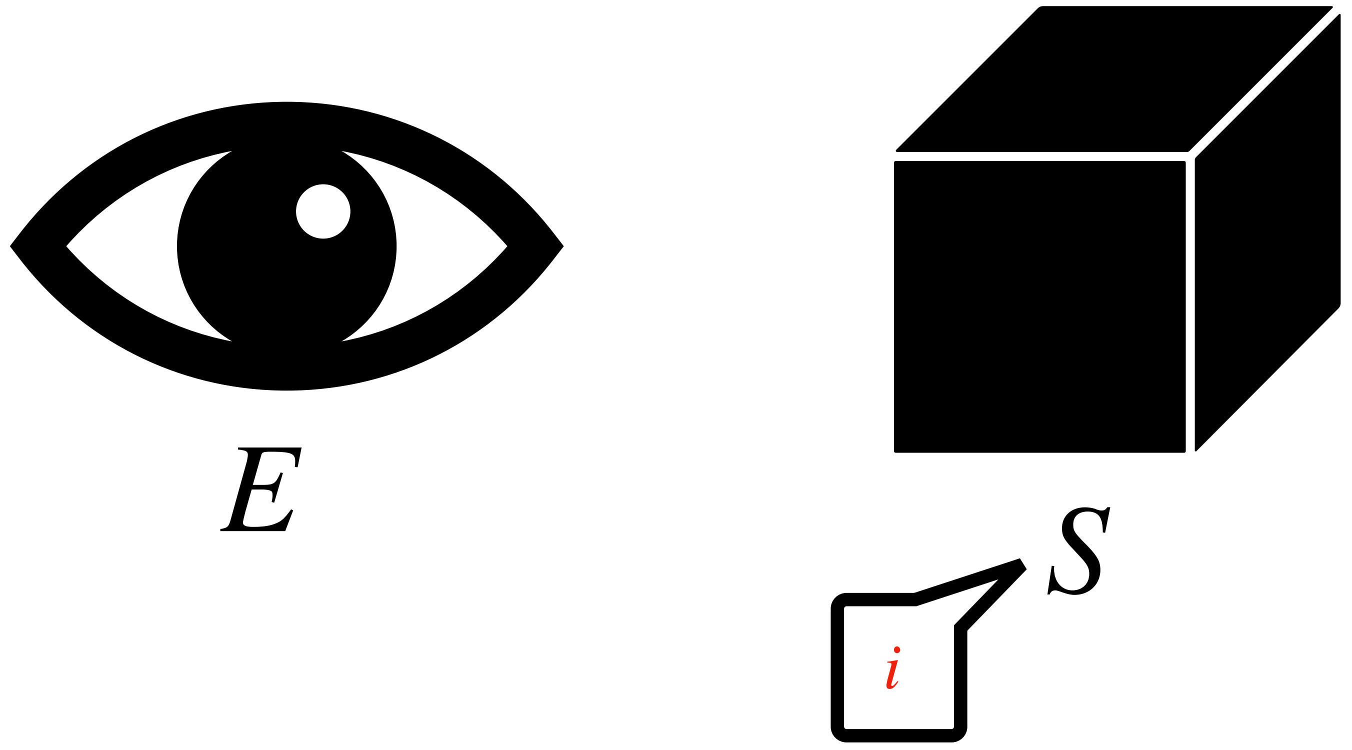
Classical physics models the state of the system S as a probability distribution over d states, represented as a column vector

$$s = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \in \mathbb{R}^d \qquad\qquad s_0 + \cdots + s_{d-1} = 1$$

≥ 0

Classical Physics

If the observer **measures** the system S, then E obtains measurement outcome i with probability s_i



State of the system gets updated to

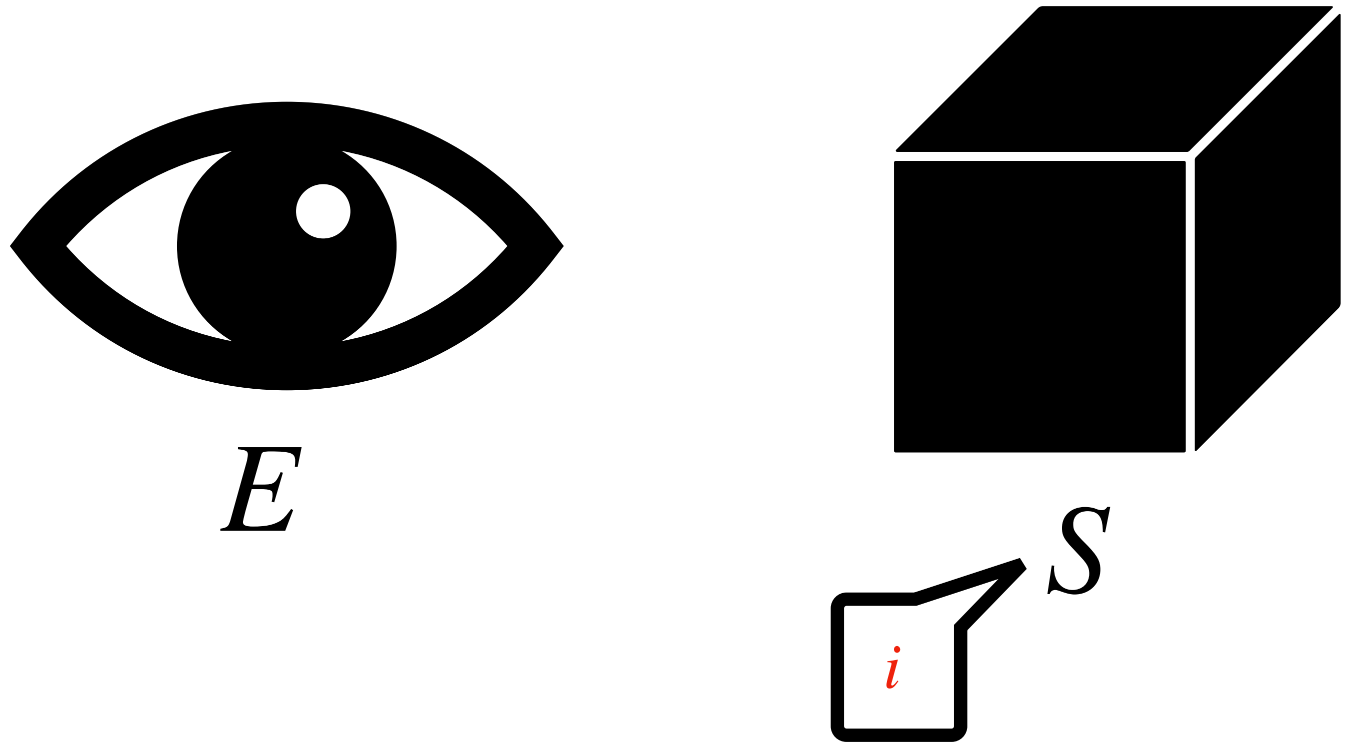
$$s = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \longrightarrow s' = \begin{array}{c} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \end{array} \begin{array}{l} \\ \\ i\text{-th coordinate} \\ \\ \\ \end{array}$$

Pre-measurement

Post-measurement

Classical Physics

If the observer **measures** the system S, then E obtains measurement outcome i with probability s_i



State of the system gets updated to

$$s = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \qquad \longrightarrow \qquad s' = \begin{array}{c} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \end{array} \begin{array}{l} \\ \\ i\text{-th coordinate} \\ \\ \\ \end{array}$$

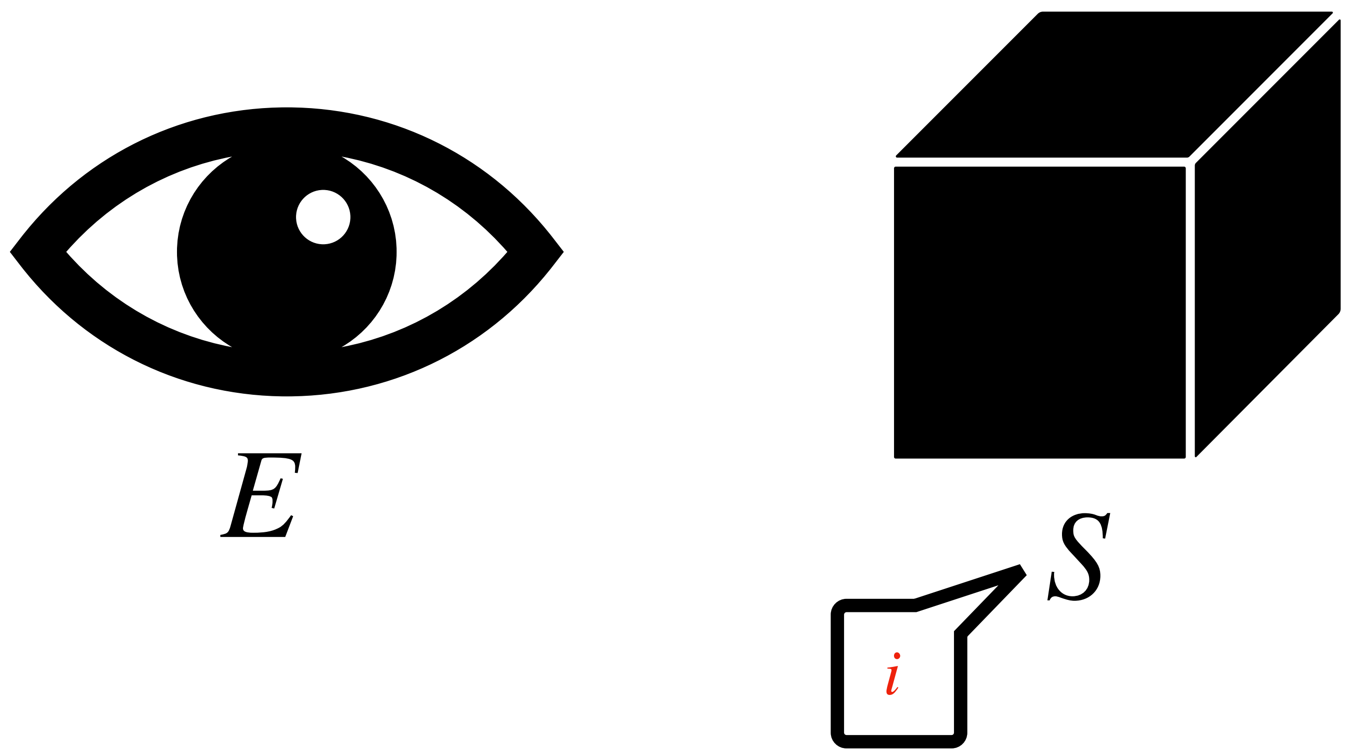
Pre-measurement

Post-measurement

What happens if the observer measures again?

Classical Physics

If the observer **measures** the system S, then E obtains measurement outcome i with probability s_i



State of the system gets updated to

$$s = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \longrightarrow s' = \begin{array}{cl} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} & \begin{array}{l} \\ \\ i\text{-th coordinate} \\ \\ \\ \end{array} \end{array}$$

Pre-measurement

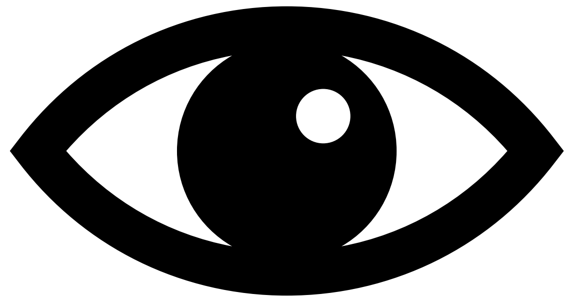
Post-measurement

What happens if the observer measures again?

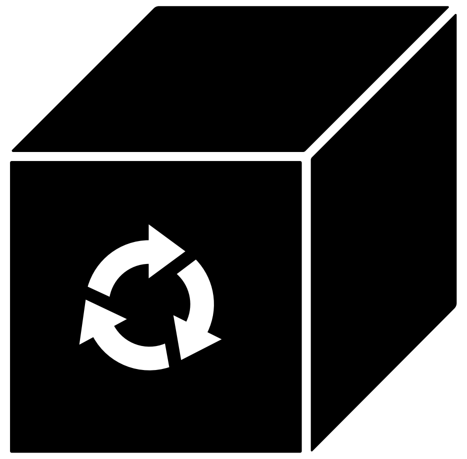
Outcome state i with probability one

Classical Physics

If the system S undergoes **isolated evolution**, then the state of the system S gets updated via a multiplication by a **stochastic** matrix



E



S

$$s = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \longrightarrow s' = A \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix}$$

$$\boxed{A}$$

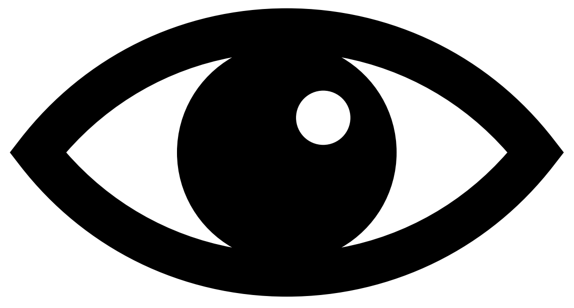
$d \times d$

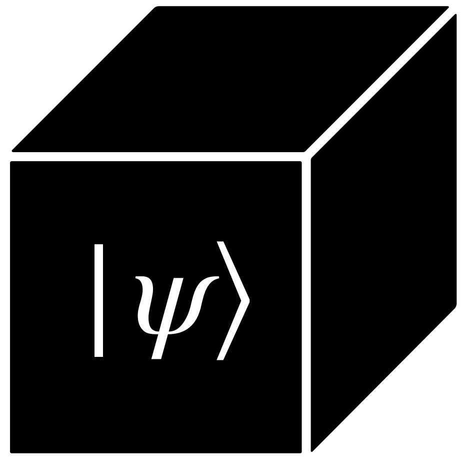
Matrix is stochastic if all entries are non-negative and each column sum is one

Stochastic matrices map probability vectors to probability vectors

Quantum Physics

Initially the observer E assigns a state to the system S





Quantum physics models the state of the system S as a **complex unit vector**, represented as a column vector

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \in \mathbb{C}^d \qquad |\alpha_0|^2 + \cdots + |\alpha_{d-1}|^2 = 1$$

α's are called amplitudes

Quantum Physics

Quantum physics models the state of the system S as a **complex unit vector**, represented as a column vector

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \in \mathbb{C}^d$$

The d distinguishable states are represented by

Also called "classical" or "basis" states

$$|0\rangle = \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix} \qquad \cdots \qquad |d-1\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$$

These vectors form an orthonormal basis for $\mathbb{C}^d$ called the standard basis

A general quantum state is a **superposition** of classical basis states

$$|\psi\rangle = \alpha_0 |0\rangle + \cdots + \alpha_{d-1} |d-1\rangle$$

This is called the **Dirac notation**

Quantum Physics

Quantum physics models the state of the system S as a **complex unit vector**, represented as a column vector

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \in \mathbb{C}^d$$

The d distinguishable states are represented by

$$|0\rangle = \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix} \qquad \cdots \qquad |d-1\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$$

Also called "classical" or "basis" states

These vectors form an orthonormal basis for $\mathbb{C}^d$ called the standard basis

A general quantum state is a **superposition** of classical basis states

A quantum state of the form $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ is called a qubit

This is called the **Dirac notation**

Dirac Notation

- Mathematically $|\psi\rangle$ is a column vector

called "ket psi"

called "bra psi"

- The complex conjugate of $|\psi\rangle$ (which is a row vector) is denoted $\langle\psi|$

$$|\psi\rangle = \binom{\alpha}{\beta} \qquad \langle\psi| = \left(\alpha*, \beta*\right) = \alpha*\langle 0| + \beta*\langle 1|$$

$\alpha*$ denotes the complex conjugate of α

$\langle 0| = (1,0)$ and $\langle 1| = (0,1)$

- Inner product between a column vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and row vector $\langle\theta| = \gamma\langle 0| + \delta\langle 1|$ is

$$\boxed{\langle\theta|\psi\rangle}$$

called "braket"

Dirac Notation

- Outer Product $|\psi\rangle\langle\theta|$ is a matrix

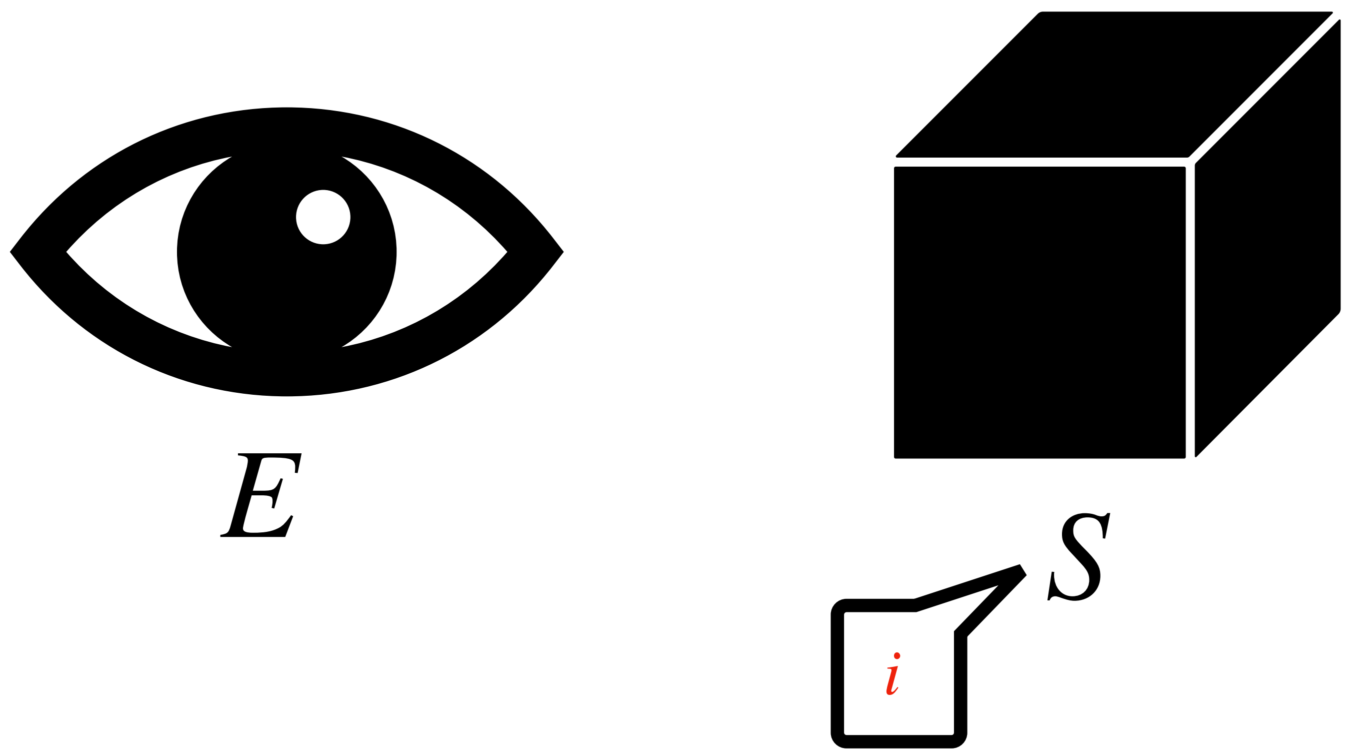
- The matrix vector multiplication of Matrix $M = |\psi\rangle\langle\theta|$ and vector $|\phi\rangle$

- Every matrix M with entries $\{M_{ij}\}$ can be written as

$$M = \sum_{ij} M_{ij} |i\rangle\langle j|$$

Quantum Physics

Born's rule If the observer **measures** the system S, then E obtains measurement outcome i with probability $|\alpha_i|^2$



State of the system gets "**collapsed**" to $|i\rangle$

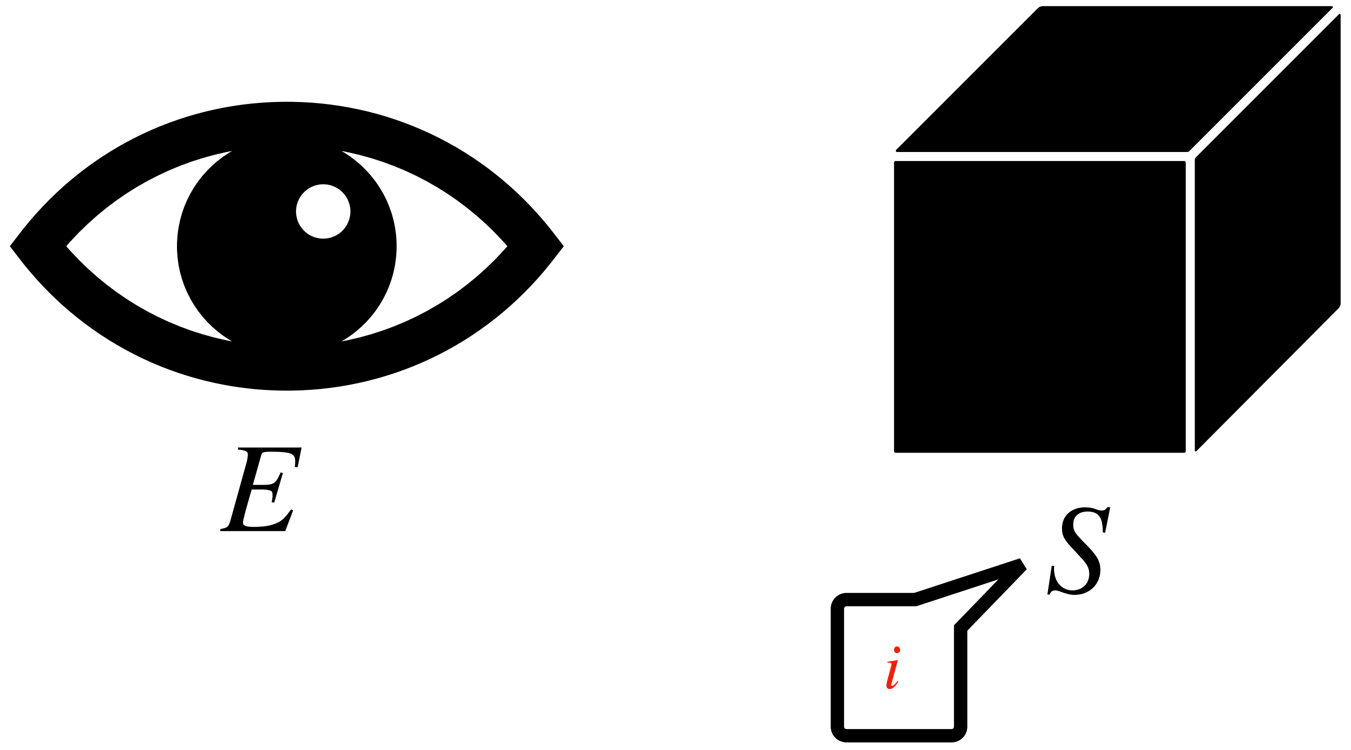
$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \longrightarrow |\psi'\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \\ \\ i\text{-th coordinate} \\ \\ \\ \end{matrix}$$

Pre-measurement

After measuring outcome i

Quantum Physics

Born's rule If the observer **measures** the system S, then E obtains measurement outcome i with probability $|\alpha_i|^2$



State of the system gets **"collapsed"** to $|i\rangle$

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \longrightarrow |\psi'\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad i\text{-th coordinate}$$

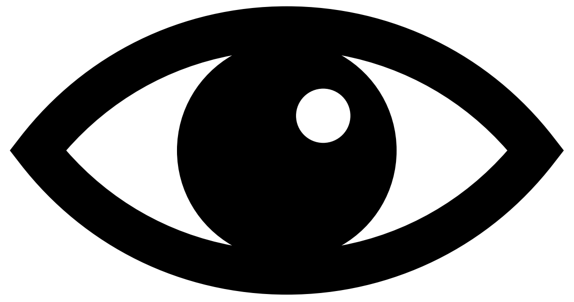
Pre-measurement

After measuring outcome i

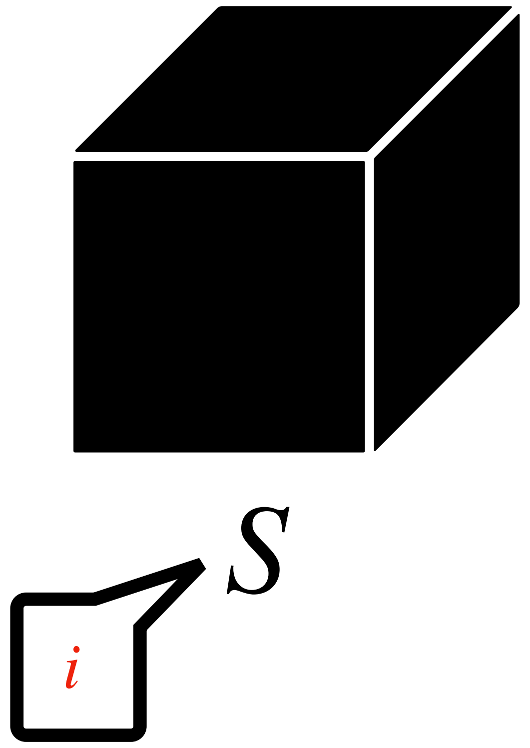
What happens if the observer measures again?

Quantum Physics

Born's rule If the observer **measures** the system S, then E obtains measurement outcome i with probability $|\alpha_i|^2$



E



State of the system gets **"collapsed"** to $|i\rangle$

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \longrightarrow |\psi'\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

i-th coordinate

Pre-measurement

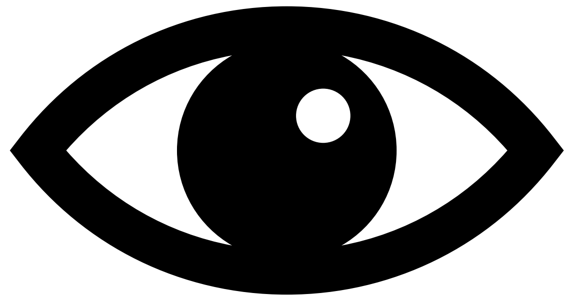
After measuring outcome i

What happens if the observer measures again?

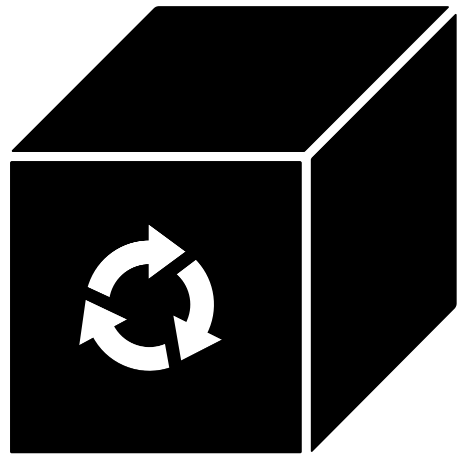
Outcome state i with probability one

Quantum Physics

If the system S undergoes **isolated evolution**, then the state of the system S gets updated via a multiplication by a **unitary** matrix



E



S

$$|\psi\rangle \longrightarrow |\psi'\rangle = U|\psi\rangle$$

$$U \in \mathbb{C}^{d\times d}$$

A $d \times d$ complex matrix is **unitary** if $U^{-1} = U^{\dagger}$

$U^{\dagger}$ is the Hermitian conjugate of U: take transpose, then complex conjugate each entry, i.e. $U^{\dagger}_{ij} = (U_{ji})^*$

Quantum Physics

Equivalent definitions of a unitary matrix

$\boxed{U} \in \mathbb{C}^{d \times d}$

- $U^{-1} = U^\dagger$

- U preserves the length of vectors

In particular, U maps (complex) unit vectors to unit vectors

- U preserves the inner product between vectors

Quantum Physics

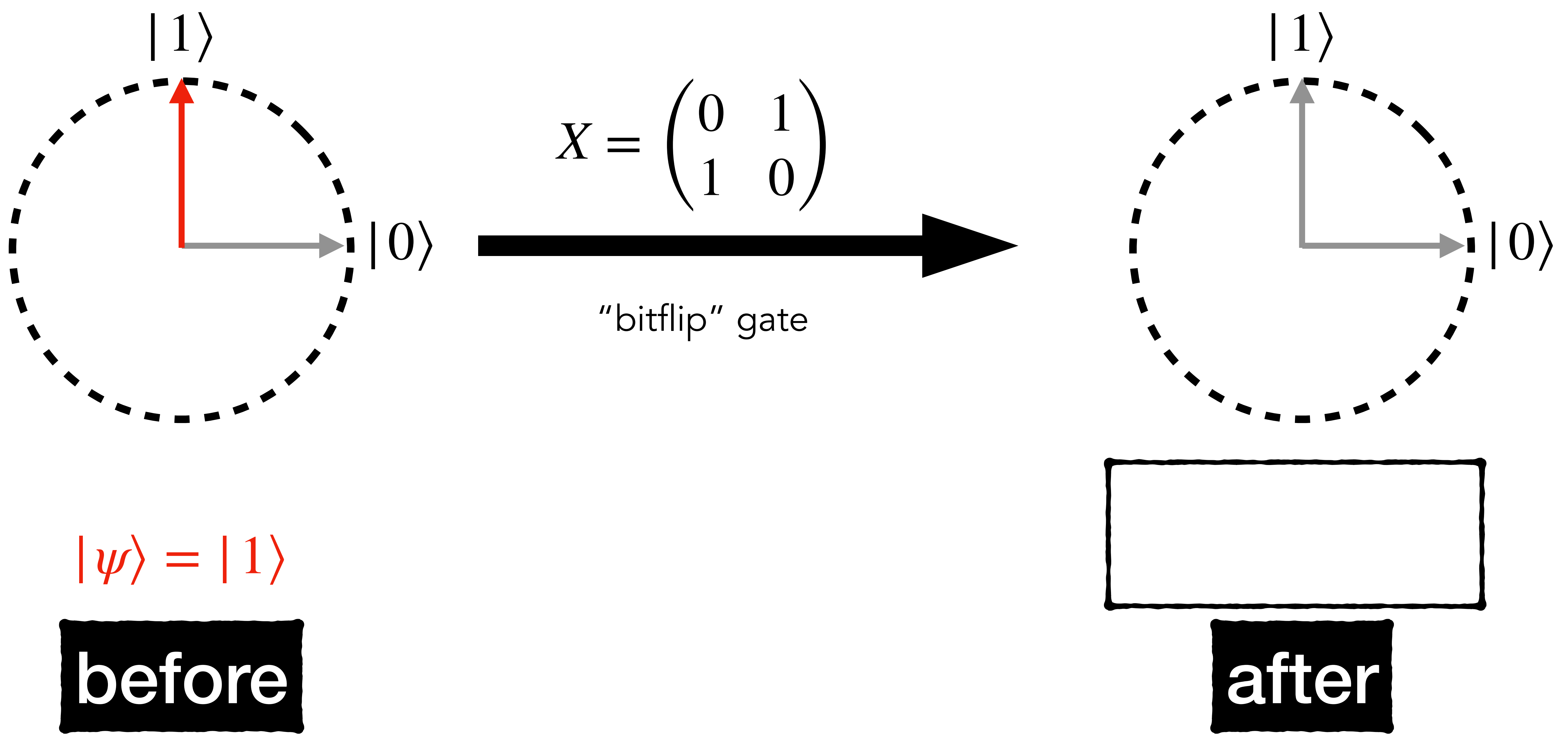
Equivalent definitions of a unitary matrix

$\boxed{U} \in \mathbb{C}^{d\times d}$

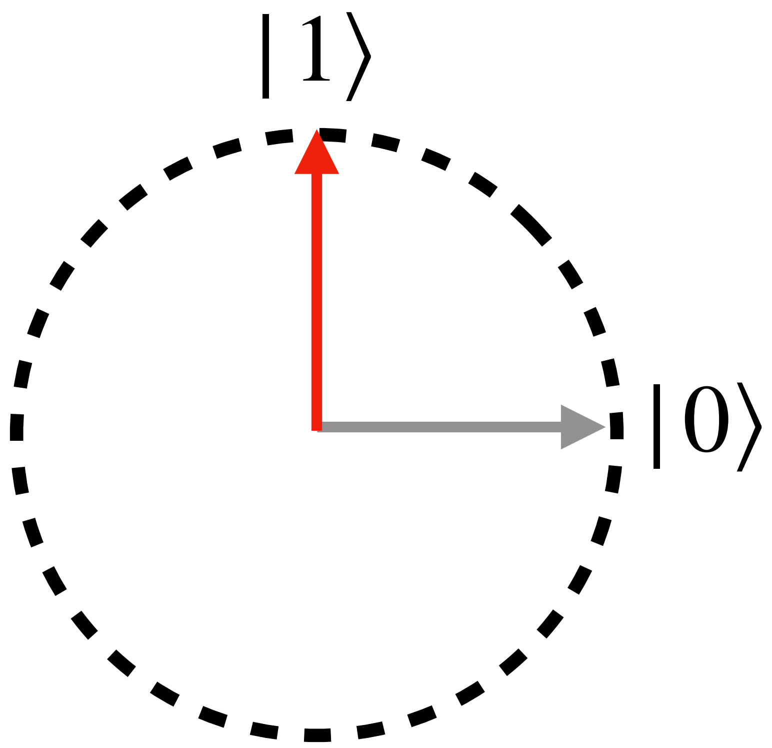
- Columns of U form an orthonormal basis of $\mathbb{C}^d$
- Rows of U form an orthonormal basis of $\mathbb{C}^d$
- U maps one orthonormal basis of $\mathbb{C}^d$ to another

U can be thought of as a change of basis operator

Unitary Evolution of a Qubit

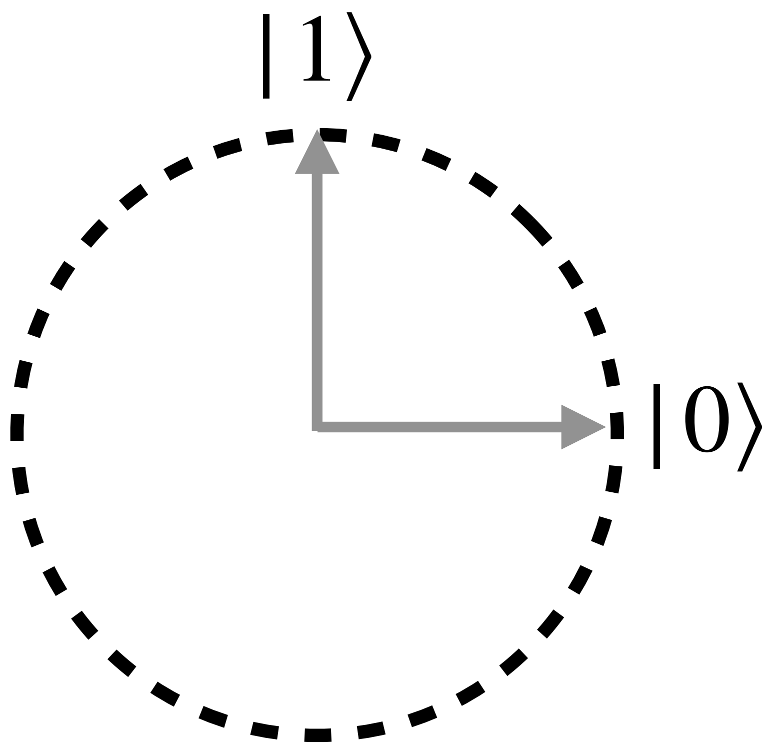


Unitary Evolution of a Qubit



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

Hadamard gate

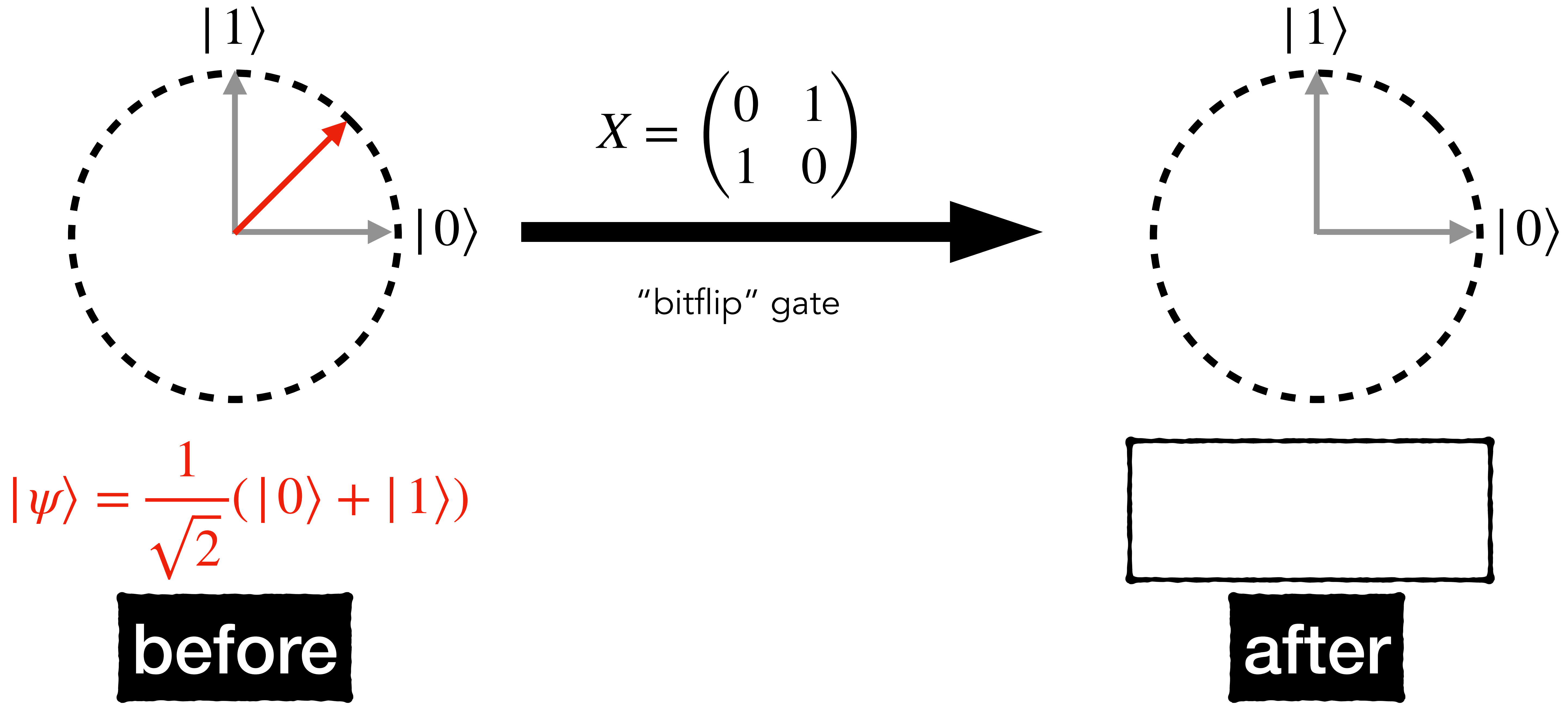


$|\psi\rangle = |1\rangle$

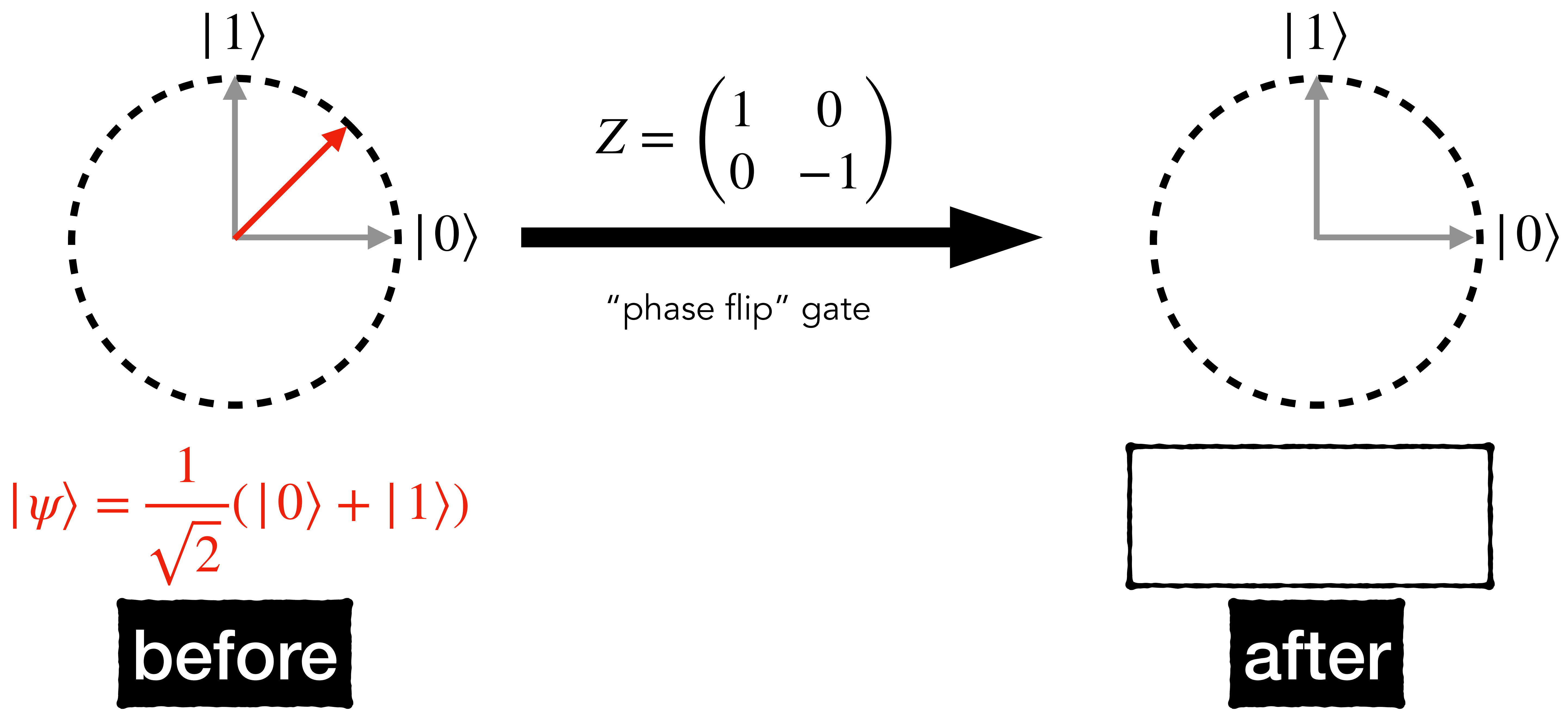
before

after

Unitary Evolution of a Qubit



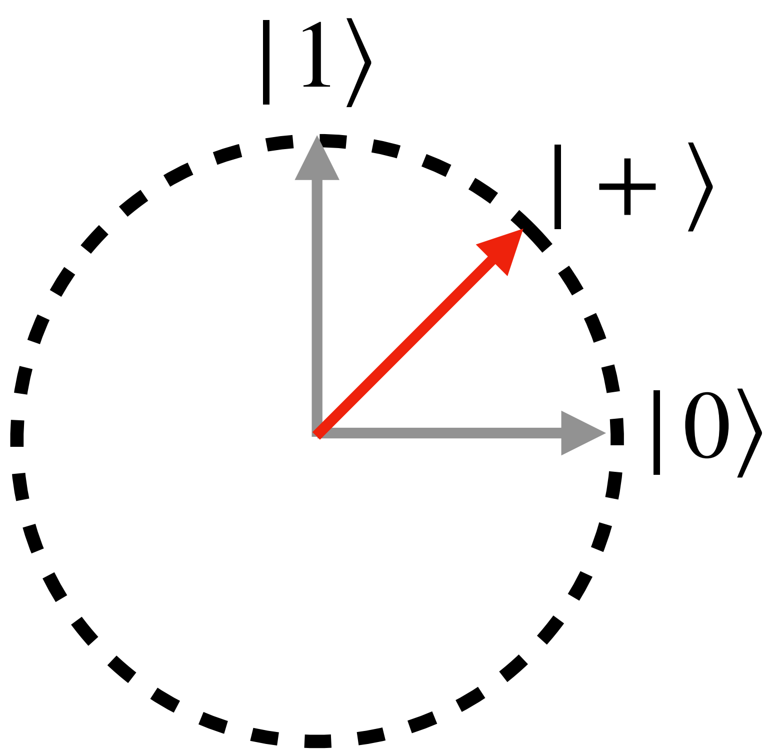
Unitary Evolution of a Qubit

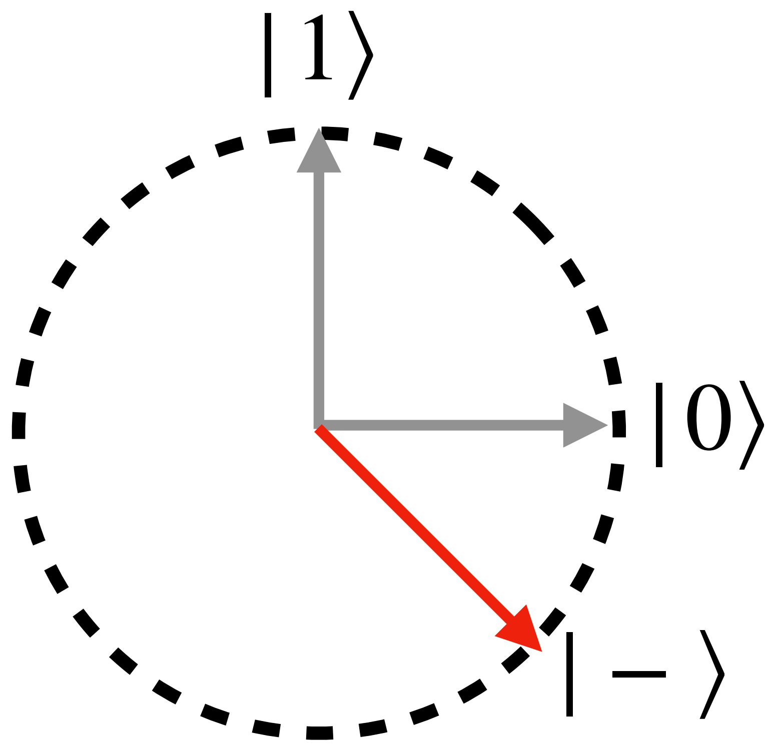


Quantum vs Classical Bits

Is there an essential difference between a quantum bit and a classical bit? Does allowing negative or complex amplitudes make a discernible difference?

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





What happens when we measure these two states?

Quantum vs Classical Bits

$|+\rangle$ and $|-\rangle$ are orthogonal to each other

$\langle - | + \rangle$

In quantum mechanics, orthogonal states are
perfectly distinguishable from one another

Quantum vs Classical Bits

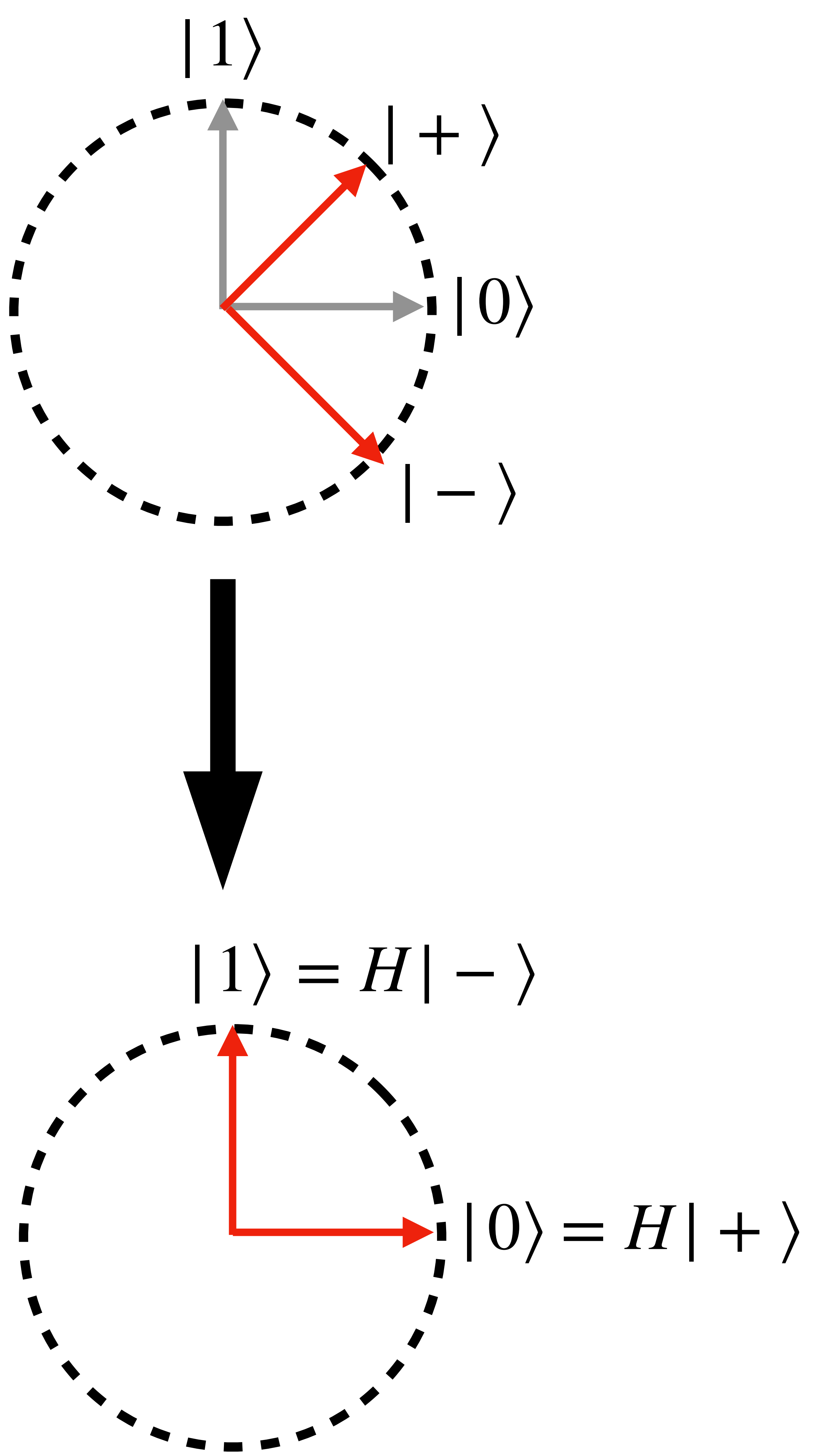
Unknown state $|\psi\rangle$ that is either $|+\rangle$ or $|-\rangle$

How could an observer tell the difference?

- Before measuring, apply a unitary $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

$H|+\rangle =$ $\qquad\qquad$ $H|-\rangle =$

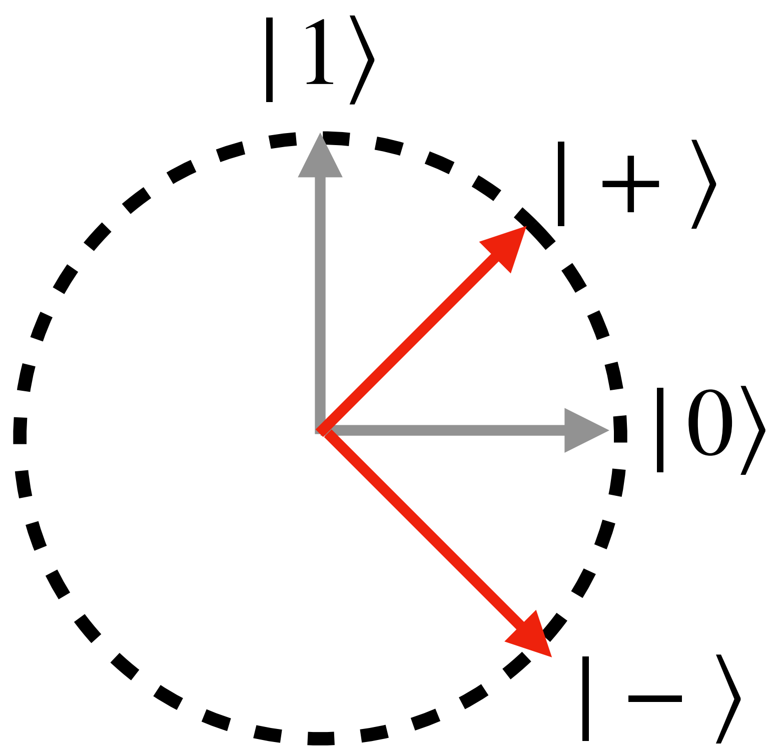
- Measuring the rotated state tell us what $|\psi\rangle$ was



Quantum vs Classical Bits

Takeaway: Minus signs in the amplitude matter!

More precisely, relative phases between the classical basis states matter



On the other hand global phases don't matter

- There is no quantum process (unitary + measurement) that can distinguish $|\psi\rangle$ from $-|\psi\rangle$
- Because $U(-|\psi\rangle) = -U|\psi\rangle$ and measurements at the end destroy sign information, since we take absolute values of the amplitudes!

Or in fact $|\psi\rangle$ from $e^{i\theta}|\psi\rangle$

Composite Quantum Systems

The state of a qubit is a unit vector in $\mathbb{C}^2$ which is also called the **Hilbert space** of the qubit

Hilbert space = complex vector space with inner product

Hilbert space of two qubits is the **tensor product space** $\mathbb{C}^2 \otimes \mathbb{C}^2$

- $\mathbb{C}^2$ has orthonormal basis $\{|0\rangle, |1\rangle\}$
- Tensor product space $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ is 4-dimensional with orthonormal basis

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \quad |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \quad |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \quad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array}$$

Shorthand

$$|00\rangle = |0,0\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle$$

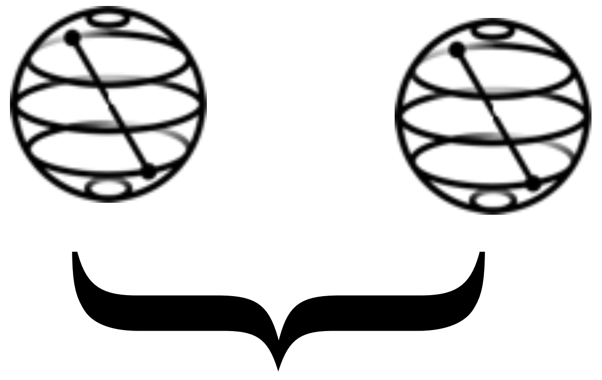
- This basis represents the **classical** states of two qubits

Composite Quantum Systems

Tensor Product of Vectors

If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\theta\rangle = \gamma|0\rangle + \delta|1\rangle$ then the state of two qubits together is

$|\psi\rangle$ $|\theta\rangle$



$|\psi\rangle \otimes |\theta\rangle$

Composite Quantum Systems

- A two qubit state $|\psi\rangle$ is a unit vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$

$$|\psi\rangle = \textstyle\sum_{ij} \alpha_{ij} |i\rangle \otimes |j\rangle \qquad \displaystyle\sum_{ij} |\alpha_{ij}|^2 = 1$$

- A general two-qubit states cannot be written as a tensor product

$$|\psi\rangle \neq |\phi\rangle \otimes |\theta\rangle \quad \text{for one qubit states } |\phi\rangle, |\theta\rangle \in \mathbb{C}^2$$

- States that cannot be written in tensor product form are called **entangled**. Otherwise, they are unentangled

Composite Quantum Systems

- A two qubit state $|\psi\rangle$ is a unit vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$

$$|\psi\rangle = \textstyle\sum_{ij} \alpha_{ij} |i\rangle \otimes |j\rangle \qquad \displaystyle\sum_{ij} |\alpha_{ij}|^2 = 1$$

- A general two-qubit states cannot be written as a tensor product

$$|\psi\rangle \neq |\phi\rangle \otimes |\theta\rangle \quad \text{for one qubit states } |\phi\rangle, |\theta\rangle \in \mathbb{C}^2$$

- States that cannot be written in tensor product form are called **entangled**. Otherwise, they are unentangled

Composite Quantum Systems

- **Example:** $|EPR\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is entangled

- **Example:** $|\psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$ is unentangled

Composite Quantum Systems

- Taking inner products in $\mathbb{C}^2 \otimes \mathbb{C}^2$: let $|a\rangle, |b\rangle, |c\rangle, |d\rangle \in \mathbb{C}^2$

$$(\langle a| \otimes \langle b|)(|c\rangle \otimes |d\rangle) = \langle a|c\rangle \cdot \langle b|d\rangle$$

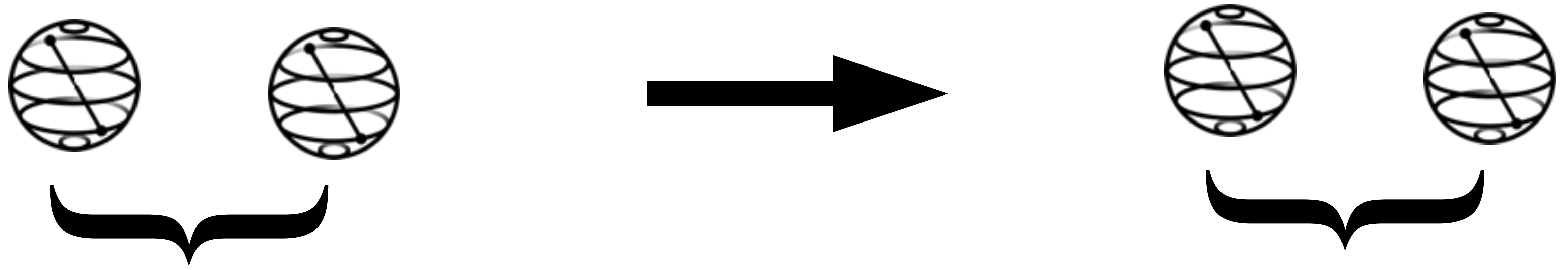
- Let $|\psi\rangle = \sum_{ij} \alpha_{ij}|i,j\rangle$ and $|\theta\rangle = \sum_{ij} \beta_{ij}|i,j\rangle$

$$\langle\psi|\theta\rangle =$$

Measurements

Measuring a two qubit state $|\psi\rangle = \sum_{ij} \alpha_{ij} |i,j\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$

- Obtain classical outcome $(i,j) \in \{0,1\}^2$ with probability $|\alpha_{ij}|^2$
- Post-measurement state of $|\psi\rangle$ is $|i,j\rangle$



$|\psi\rangle$

$|\psi'\rangle = |i\rangle \otimes |j\rangle$

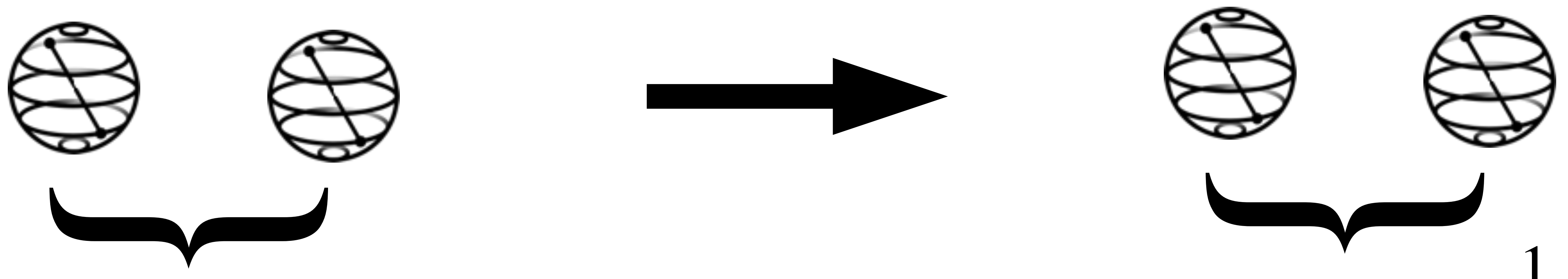
Partial Measurements

Measuring the first qubit in a two qubit state $|\psi\rangle = \sum_{ij} \alpha_{ij} |i,j\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$

- Obtain classical outcome $i \in \{0,1\}$ with probability

$$p_i = |\alpha_{i0}|^2 + |\alpha_{i1}|^2$$

- Post-measurement state of $|\psi\rangle$ is $\frac{1}{\sqrt{p_i}} \left(\alpha_{i0} |i0\rangle + \alpha_{i1} |i1\rangle\right)$



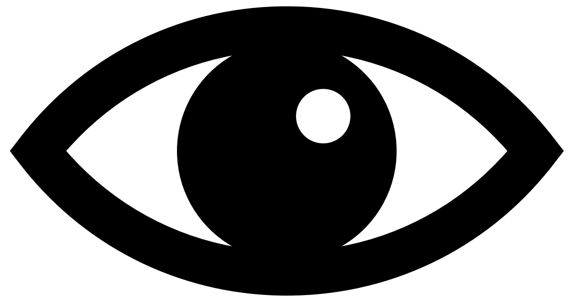
$|\psi\rangle$

$|\psi'\rangle = |i\rangle \otimes \frac{1}{\sqrt{p_i}} \left(\alpha_{i0} |0\rangle + \alpha_{i1} |1\rangle\right)$

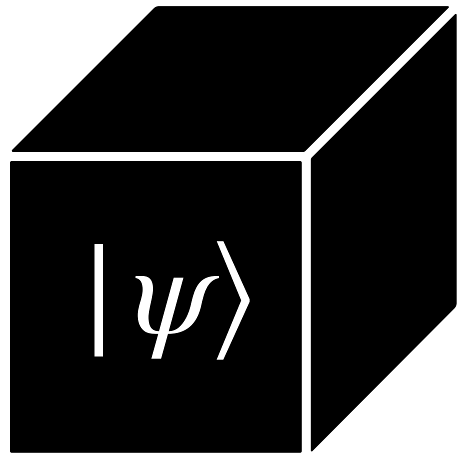
RECAP

Quantum Physics

Initially the observer E assigns a state to the system S



E



S

Quantum physics models the state of the system S as a **complex unit vector**, represented as a column vector

$$\mathbb{C}^d \ni |\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} = \alpha_0 |0\rangle + \cdots + \alpha_{d-1} |d-1\rangle$$

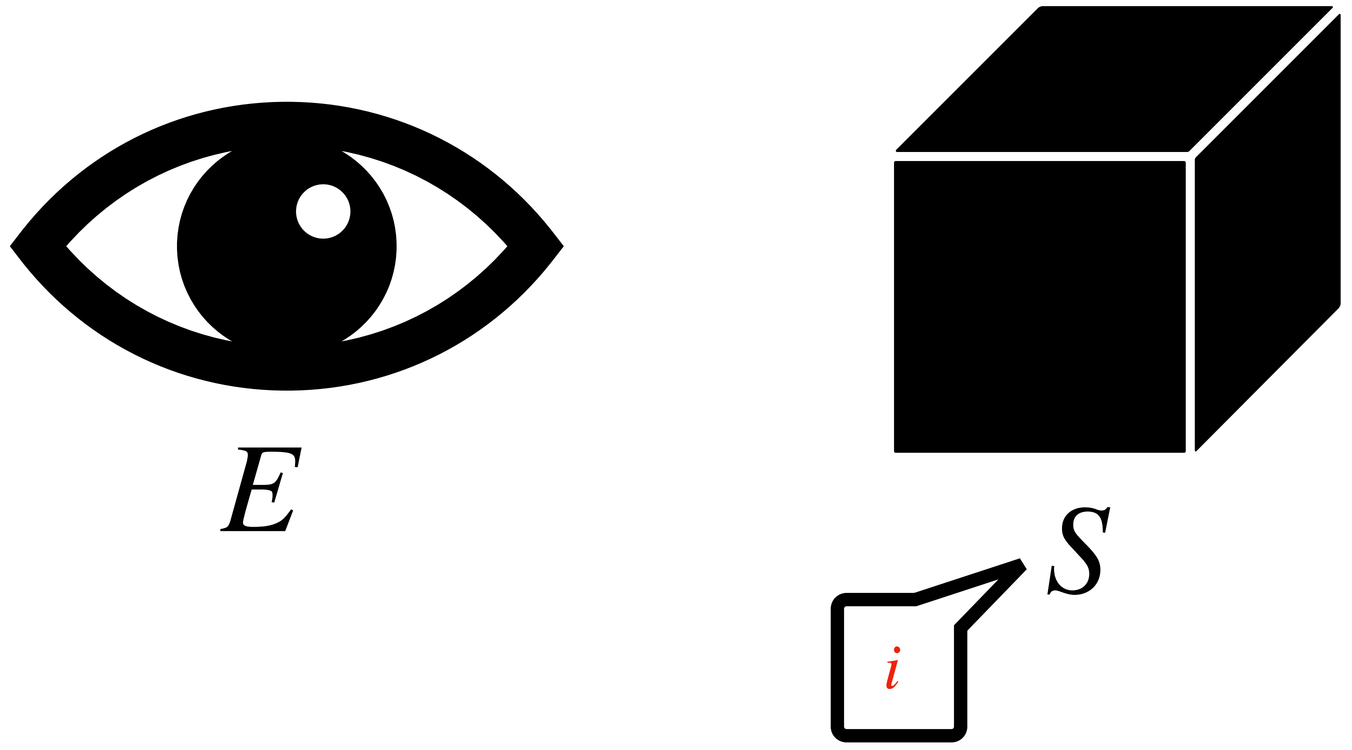
where $|\alpha_0|^2 + \cdots + |\alpha_{d-1}|^2 = 1$

α's are called amplitudes

$|i\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ i-th coordinate

Quantum Physics

Born's rule If the observer **measures** the system S, then E obtains measurement outcome i with probability $|\alpha_i|^2$



State of the system gets **"collapsed"** to $|i\rangle$

$$|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} \longrightarrow |\psi'\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

i-th coordinate

Pre-measurement

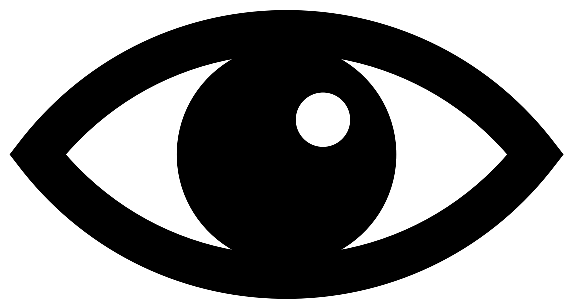
After measuring outcome i

What happens if the observer measures again?

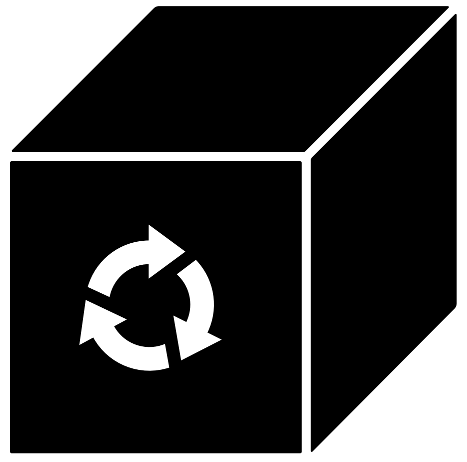
Outcome state i with probability one

Quantum Physics

If the system S undergoes **isolated evolution**, then the state of the system S gets updated via a multiplication by a **unitary** matrix



E



S

$$|\psi\rangle \longrightarrow |\psi'\rangle = U|\psi\rangle$$

$$\boxed{U} \in \mathbb{C}^{d\times d}$$

A $d \times d$ complex matrix is **unitary** if $U^{-1} = U^{\dagger}$

$U^{\dagger}$ is the Hermitian conjugate of U: take transpose, then complex conjugate each entry, i.e. $U^{\dagger}_{ij} = (U_{ji})^*$

All unitary operations are **reversible**

Composite Quantum Systems

- A two qubit state $|\psi\rangle$ is a unit vector in $\mathbb{C}^2 \otimes \mathbb{C}^2$

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

- A general two-qubit states cannot be written as a tensor product

$$|\psi\rangle \neq |\phi\rangle \otimes |\theta\rangle \quad \text{for one qubit states } |\phi\rangle, |\theta\rangle \in \mathbb{C}^2$$

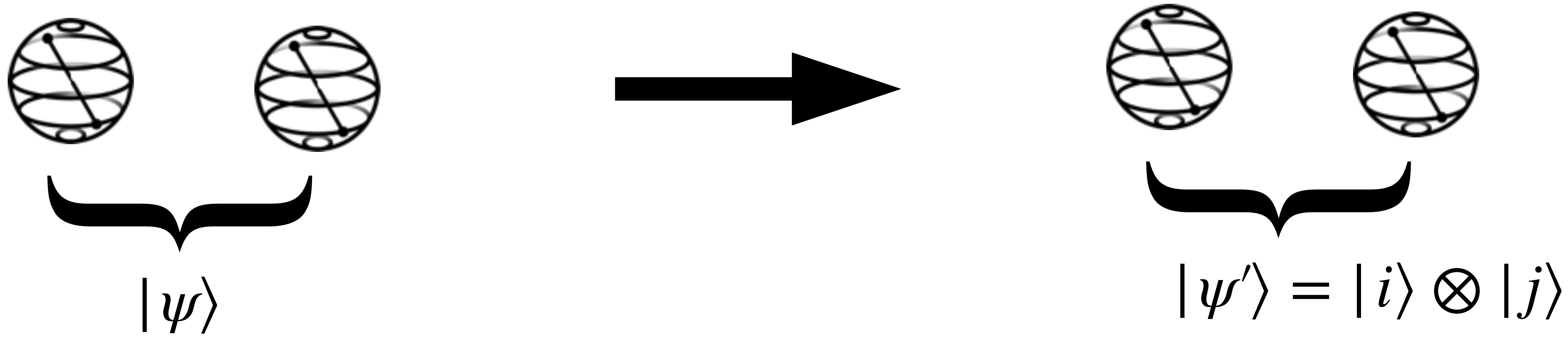
- States that cannot be written in tensor product form are called **entangled**. Otherwise, they are unentangled

  Example: $|EPR\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is entangled

Measurements

Measuring a two qubit state $|\psi\rangle = \sum_{ij} \alpha_{ij} |i,j\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$

- Obtain classical outcome $(i,j) \in \{0,1\}^2$ with probability $|\alpha_{ij}|^2$
- Post-measurement state of $|\psi\rangle$ is $|i,j\rangle$



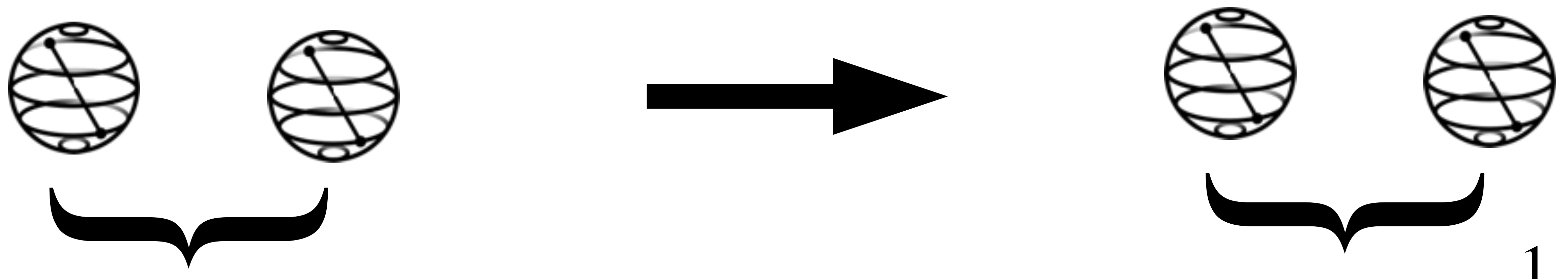
Partial Measurements

Measuring the first qubit in a two qubit state $|\psi\rangle = \sum_{ij} \alpha_{ij} |i, j\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$

- Obtain classical outcome $i \in \{0,1\}$ with probability

$$p_i = |\alpha_{i0}|^2 + |\alpha_{i1}|^2$$

- Post-measurement state of $|\psi\rangle$ is $\dfrac{1}{\sqrt{p_i}} \left(\alpha_{i0} |i0\rangle + \alpha_{i1} |i1\rangle \right)$

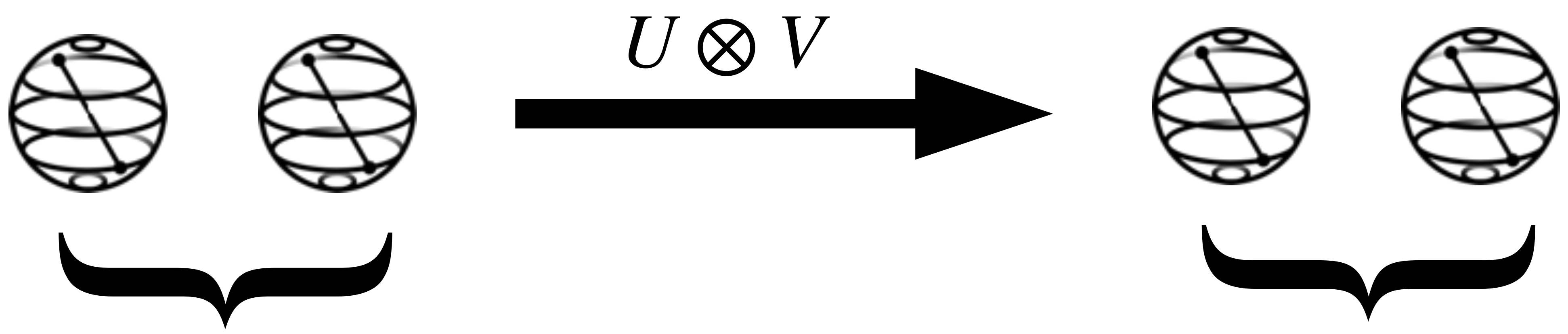


Unitary Evolution on Composite Systems

Two qubit systems in isolation evolve via unitary matrices on $\mathbb{C}^2 \otimes \mathbb{C}^2$

- Tensor product of one-qubit unitaries U, V:

$$\boxed{\begin{array}{c}\text{Applying } U \text{ to the first and } V \text{ to the second qubit} \\ \text{corresponds to applying } U \otimes V \text{ to the larger system}\end{array}}$$



$|\psi\rangle \otimes |\theta\rangle$

$(U \otimes V)(|\psi\rangle \otimes |\theta\rangle) = (U|\psi\rangle) \otimes (V|\theta\rangle)$

Unitary Evolution on Composite Systems

Two qubit systems in isolation evolve via unitary matrices on $\mathbb{C}^2 \otimes \mathbb{C}^2$

- Tensor product of one-qubit unitaries U, V:

  Applying U to the first and V to the second qubit corresponds to applying $U \otimes V$ to the larger system

- Matrix representation

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \qquad V = \begin{pmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{pmatrix}$$

$$\Longrightarrow U \otimes V = \begin{pmatrix} u_{00}V & u_{01}V \\ u_{10}V & u_{11}V \end{pmatrix}$$

Matrix representation depends on how one indexes rows/columns

Unitary Evolution on Composite Systems

General two-qubit unitaries are not product operators; they are **entangling**

- **Example:** $CNOT$ acts on two qubits: for any $x \in \{0,1\}$

$$CNOT|x\rangle \otimes |0\rangle = |x\rangle \otimes |x\rangle$$

$$CNOT|x\rangle \otimes |1\rangle = |x\rangle \otimes |x \oplus 1\rangle$$

Control qubit

Target qubit

- **Example:** $|\psi\rangle = |+\rangle \otimes |0\rangle$

$$\boxed{CNOT|\psi\rangle = \qquad\qquad\qquad\qquad}$$

No Cloning Theorem

Classical bits are easily copied. Quantum Information is different

- Informal Statement: "There is no quantum Xerox machine"
- **Formally:** There is no unitary U acting on two qubits such that

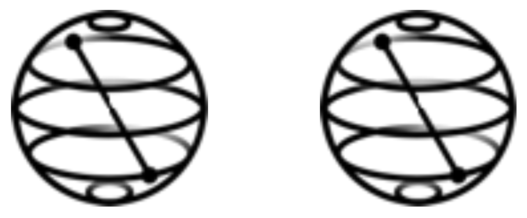
$$U|\psi\rangle \otimes \underbrace{|0\rangle}_{\text{ancilla}} = |\psi\rangle \otimes |\psi\rangle$$

for all one qubit states $|\psi\rangle$

No Cloning Theorem

Proof: try to copy $|0\rangle$ vs $|+\rangle$

Mixed State



$|\phi\rangle \otimes |\theta\rangle$

- Given two qubits in tensor product state $|\psi\rangle = |\phi\rangle \otimes |\theta\rangle$ what is the state of the first qubit?

- How about when the two qubits are in an **entangled state**?

Example: $|EPR\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is entangled

- In this case the state of the first qubit is described by measuring the first qubit and describing the state of the second qubit after the measurement

State of first qubit:
$$\left.\begin{array}{l} |0\rangle \text{ with probability } 1/2 \\ |1\rangle \text{ with probability } 1/2 \end{array}\right\}$$

Mixed State

- Mixed states can be represented by **density matrices**

Example: $|\psi_0\rangle$ with probability p_0
$|\psi_1\rangle$ with probability p_1

$$\left.\begin{array}{l} |\psi_0\rangle \text{ with probability } p_0 \\ |\psi_1\rangle \text{ with probability } p_1 \end{array}\right\} \rho = p_0 |\psi_0\rangle\langle\psi_0| + p_1 |\psi_1\rangle\langle\psi_1|$$

- Different probability mixtures can give rise to the same density matrix

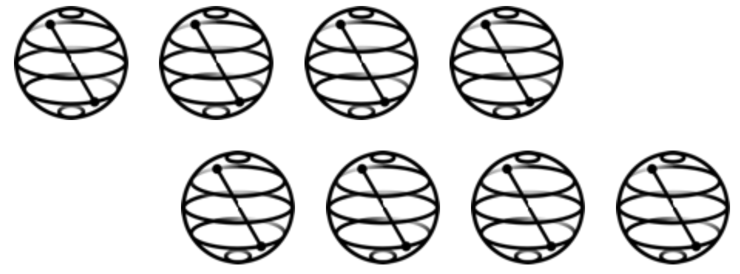
Example: $|0\rangle$ with probability $1/2$
$|1\rangle$ with probability $1/2$

Or: $|+\rangle$ with probability $1/2$
$|-\rangle$ with probability $1/2$

- No unitary or measurement can distinguish the mixture if the density matrices are the same
- One can define measurement and unitary evolution for density matrices (later)

Exponentialty of Quantum Mechanics

- Nature is doing an incredible amount of work for us



- However, we can only access the exponential information stored in $|\psi\rangle$ in a limited way

$$|\psi\rangle = \begin{pmatrix} \alpha_{0\dots0} \\ \vdots \\ \alpha_{1\dots1} \end{pmatrix}$$

- This leads to a fundamental tension in quantum information:

Exponentialty vs Fragility of Quantum States

- This tension makes quantum information and computation subtle, mysterious and extremely interesting

Supplementary Homework

If you don't have a background in quantum information

- Read first few chapters in Nielsen-Chuang
- Look at lecture notes and material for CS498QC: Introduction to Quantum Computing
- Supplementary homework from CS498QC to internalize notation and refresh linear algebra concepts