Crash Course in Quantum Computing

Hour 1: Quantum Information Fundamentals

BIU Winter School on Cryptography 2021

Lecturer: Henry Yuen

Hour 1

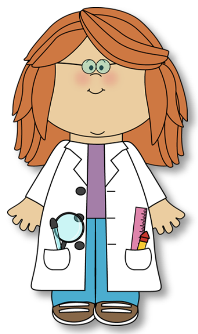
- Basic postulates of Quantum Mechanics & Dirac Notation
- Quantum vs classical bits
- Composite quantum systems

Starting point

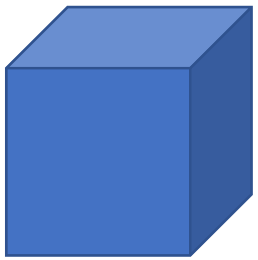
Quantum information theory is a generalization of classical probability theory where probabilities can be negative, or even complex numbers.

Starting point

- Consider a physical system S with d distinguishable states, numbered $0, 1, \dots, d-1$
- There is also an observer E external to the system



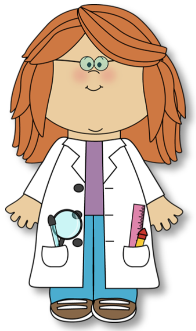
E



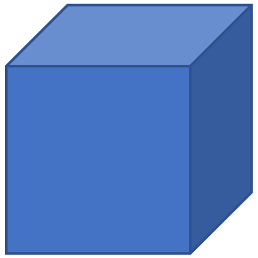
S

Starting point

- Consider a physical system S with *d* distinguishable states, numbered $0, 1, \ldots, d-1$
- There is also an observer E external to the system
- There are two things that can occur:
  - **Measurement**: the external observer E can **measure** the state of S
  - **Isolated evolution**: the system S can change, without interacting with the external observer E



E



S

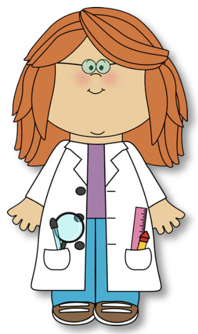
Classical physics

- Initially, the observer E assigns a **state** to the system S.
- According to classical physics, we can model the state of the system S as a **probability distribution** over d states, represented as a column vector:

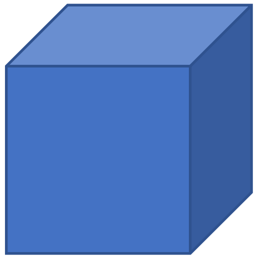
$$s = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \in \mathbb{R}^d$$

For all i, $s_i \geq 0$

$$s_0 + \cdots + s_{d-1} = 1$$



E



S

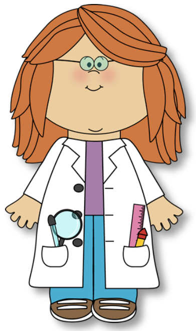
Classical physics

- If the observer **measures** (i.e. "observes") the system S, then E obtains a measurement outcome i with probability s_i, and then the state of the system S gets updated to

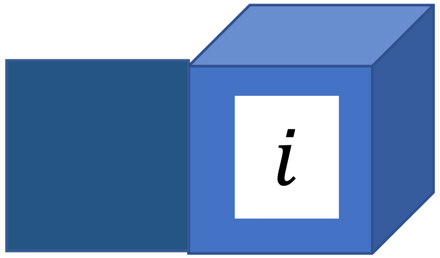
$$s = \begin{pmatrix} s_0 \\ \vdots \\ s_{d-1} \end{pmatrix} \quad \mapsto \quad s' = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

i'th position

If the observer measures again, then gets state i with probability 1 (nothing has changed).



E



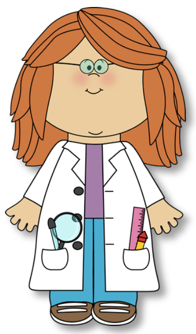
S

Classical physics

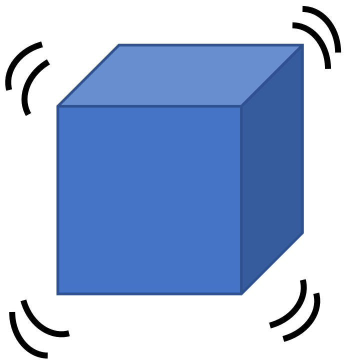
- If the system S undergoes **isolated evolution** (i.e. "following the laws of physics"), then the state of the system S gets updated via multiplication by a **stochastic** matrix

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

- A $d \times d$ matrix A is ***stochastic*** if entries are nonnegative, and each column sums to 1.
- Stochastic matrices map probability vectors to probability vectors.



E



S

Quantum physics

- Initially, the observer E assigns a **state** to the system S.
- According to quantum physics, we can model the state of the system S as a **complex unit vector** in $\mathbb{C}^d$, represented as a column vector:

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

The α's are called **amplitudes.**

Quantum physics

- Initially, the observer E assigns a **state** to the system S.
- According to quantum physics, we can model the state of the system S as a **complex unit vector** in $\mathbb{C}^d$, represented as a column vector:

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

The α's are called **amplitudes.**

- The *d* distinguishable states (also called "classical states") are represented by

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

This forms an orthogonal basis for $\mathbb{C}^d$, called the ***standard basis***.

Quantum physics

- Initially, the observer E assigns a **state** to the system S.
- According to quantum physics, we can model the state of the system S as a **complex unit vector** in $\mathbb{C}^d$, represented as a column vector:

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

The α's are called **amplitudes.**

- The *d* distinguishable states (also called "classical states") are represented by

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

This forms an orthogonal basis for $\mathbb{C}^d$, called the ***standard basis***.

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

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{d-1}|d-1\rangle$$

Dirac notation

- The $|\psi\rangle$ notation is called *Dirac notation*, used to represent quantum states.
- Mathematically, $|\psi\rangle$ ("ket vector") is a **column vector**.

Dirac notation

- The $|\psi\rangle$ notation is called *Dirac notation*, used to represent quantum states.
- Mathematically, $|\psi\rangle$ (“ket vector”) is a **column vector**.
- The **dual/Hermitian conjugate** of column vectors (i.e. row vectors), are called “bra vectors”:

$$|\psi\rangle = \binom{\alpha}{\beta}$$

“ket psi”

$$\langle\psi| = (\alpha^*, \beta^*) = \alpha^*\langle 0| + \beta^*\langle 1|$$

“bra psi”

α^*, β^* are **complex conjugates** of α, β.

- Example: duals of the standard basis vectors: $\langle 0| = (1,0)$ and $\langle 1| = (0,1)$

Dirac notation

- The $|\psi\rangle$ notation is called *Dirac notation*, used to represent quantum states.
- Mathematically, $|\psi\rangle$ ("ket vector") is a **column vector**.
- The **dual/Hermitian conjugate** of column vectors (i.e. row vectors), are called "bra vectors":

$$|\psi\rangle = \binom{\alpha}{\beta}$$

"ket psi"

$$\langle\psi| = (\alpha^*, \beta^*) = \alpha^*\langle 0| + \beta^*\langle 1|$$

"bra psi"

α^*, β^* are **complex conjugates** of α, β.

- Example: duals of the standard basis vectors: $\langle 0| = (1,0)$ and $\langle 1| = (0,1)$
- The inner product between a column vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and a row vector $\langle\theta| = \gamma\,\langle 0| + \delta\,\langle 1|$ is

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

- Notation is helpful for quickly identifying scalars, row and column vectors in complicated expressions.
- Naming: "bra" + "ket" = "bracket"

Dirac notation

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

- Matrix $M = |\psi\rangle\langle\theta|$, and vector $|\phi\rangle$. Then matrix-vector multiplication becomes:

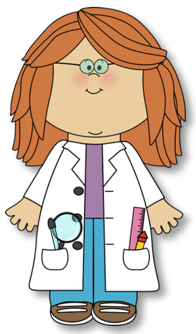
- Every matrix M with matrix entries $\{M_{ij}\}$ can be written as $M = \sum_{i,j} M_{ij} \, |i\rangle\langle j|$

Quantum physics

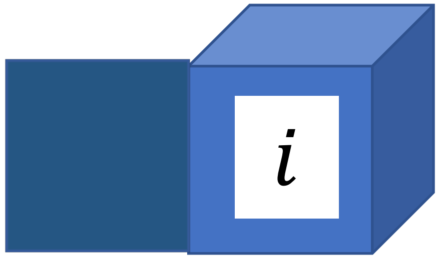
- If the observer **measures** the system S, then E obtains a measurement outcome i with probability $|\alpha_i|^2$, and then the state of the system S gets updated (gets "**collapsed**") from $|\psi\rangle$ to the classical state $|i\rangle$.

- If the observer measures again, then it gets state $|i\rangle$ with probability 1.

This is called the **Born Rule**.

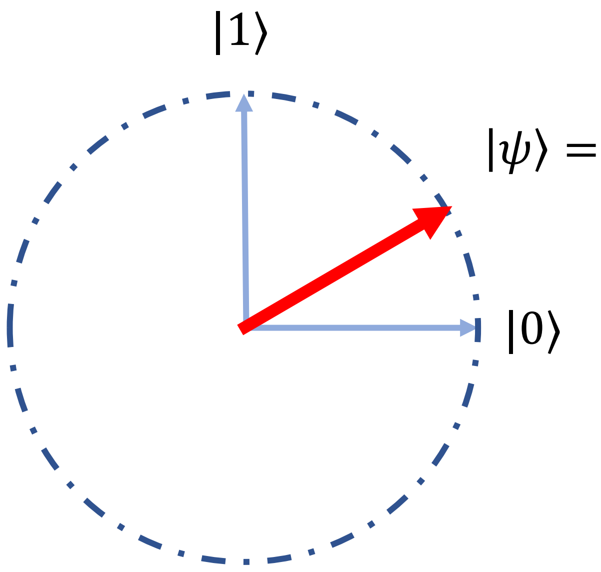


E



S

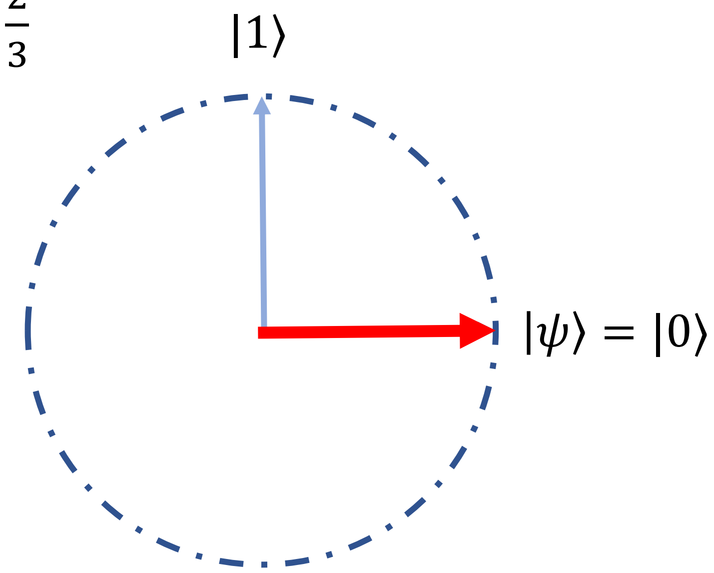
Measuring a qubit



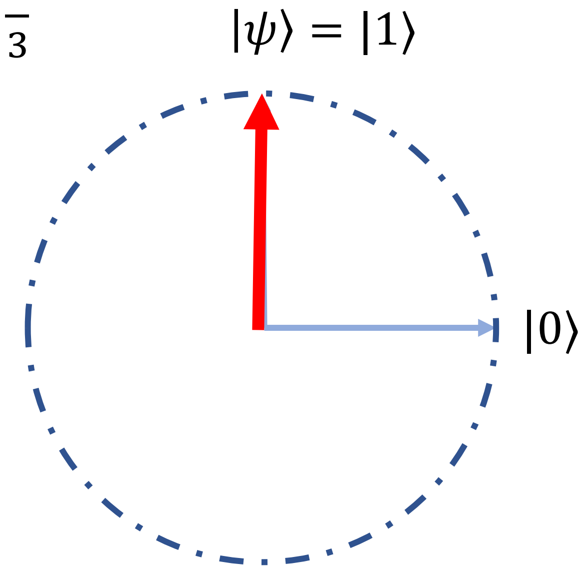
$$|\psi\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$$

Before

After, w/ prob. $|\alpha|^2 = \frac{2}{3}$



After, w/ prob. $|\beta|^2 = \frac{1}{3}$



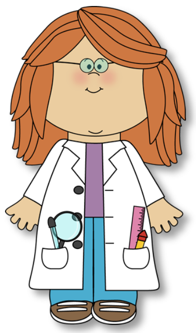
Quantum physics

- If the system S undergoes **isolated evolution** (i.e. "following the laws of physics"), then the state of the system S gets updated via multiplication by a **unitary** matrix

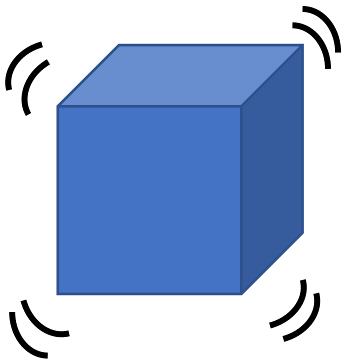
$$|\psi\rangle \quad \mapsto \quad |\psi'\rangle = U|\psi\rangle$$

- $U^\dagger$ denotes the **Hermitian conjugate** of U: transposing the matrix, then complex-conjugating every entry: the (i, j)'th entry of $U^\dagger$ is U^*_{ji}.

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



E



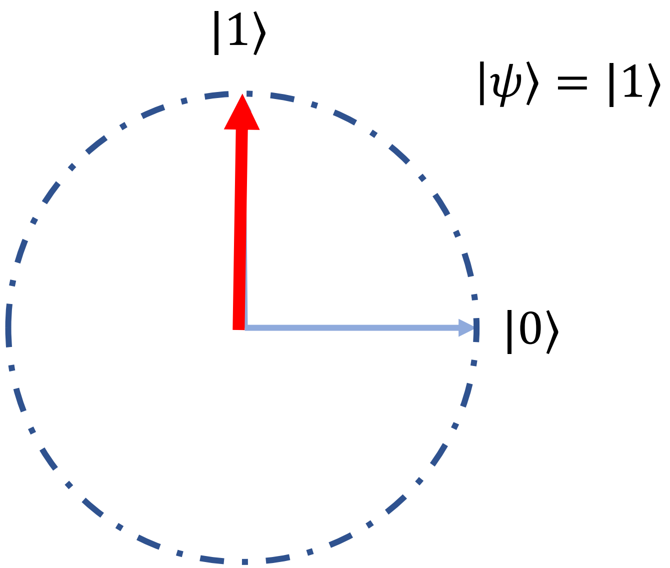
S

Quantum physics

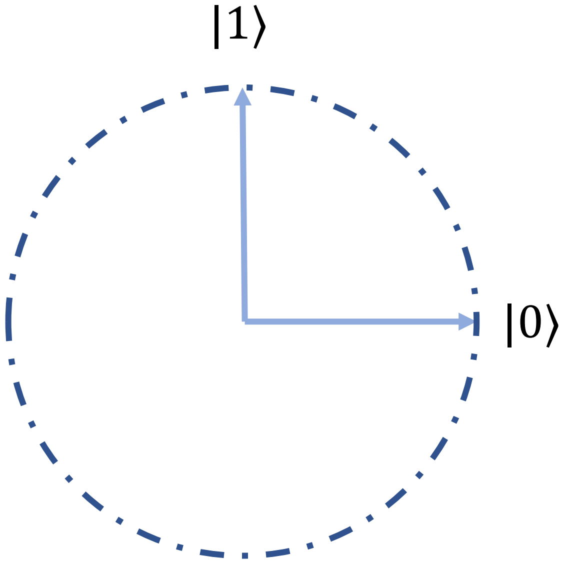
Equivalent definitions of a unitary matrix:

- $U^{-1} = U^{\dagger}$
- U maps unit vectors to unit vectors
- U preserves the inner product between vectors

Unitary evolution of a qubit



Before

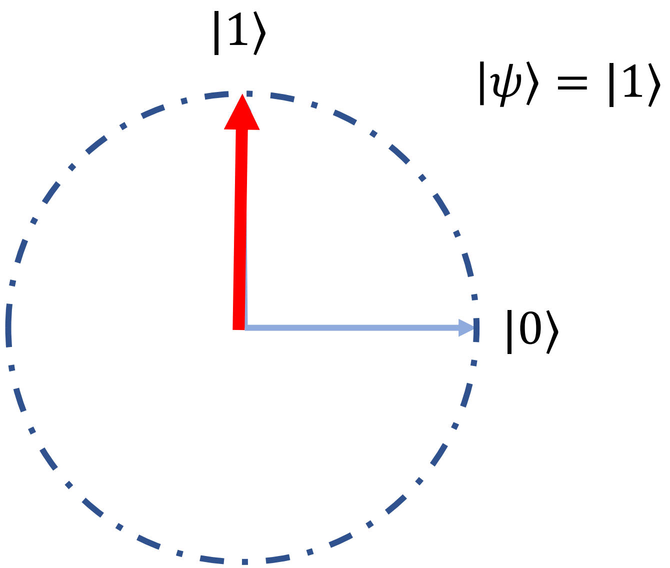


After

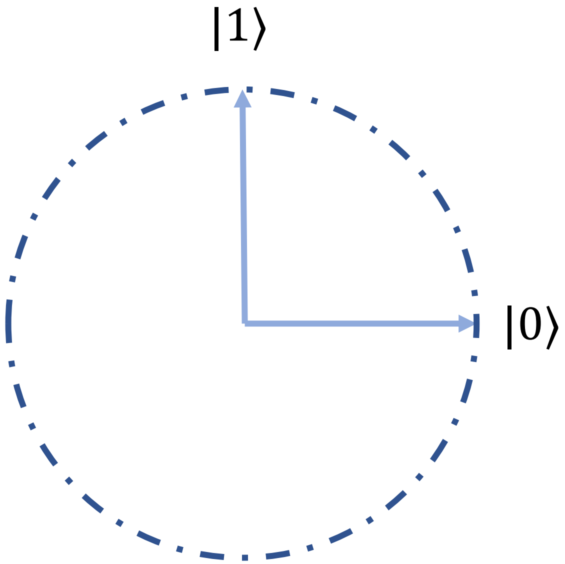
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

"bitflip" gate

Unitary evolution of a qubit



Before

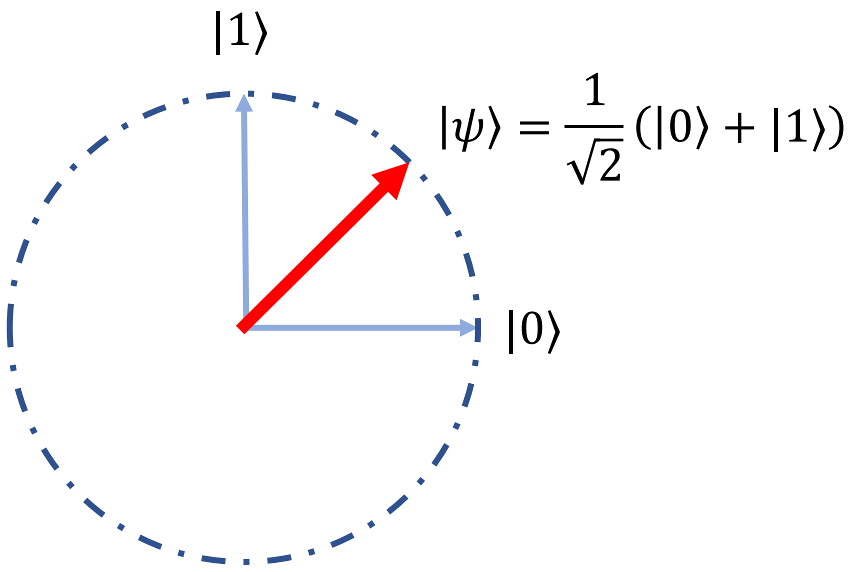


After

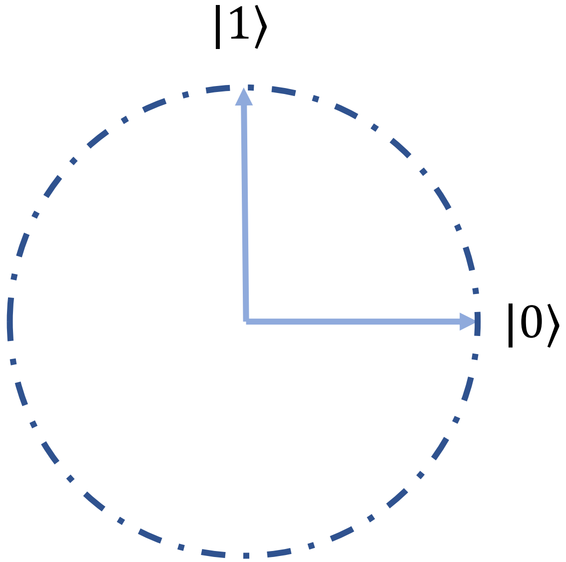
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Hadamard gate

Unitary evolution of a qubit



Before

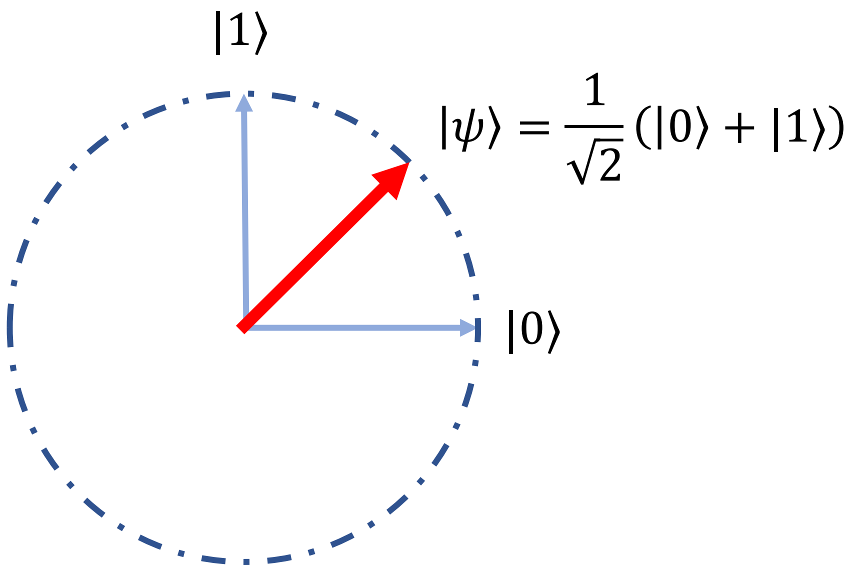


After

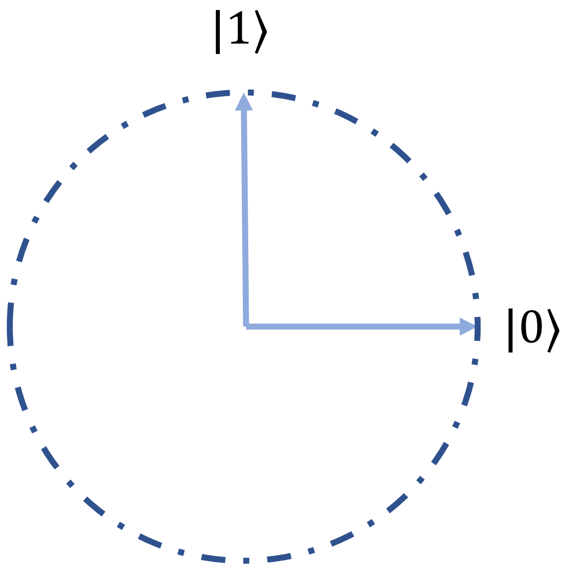
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

"bitflip" gate

Unitary evolution of a qubit



Before



After

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

”phase flip” gate

Measuring in different bases

By default, observer measures with respect to **standard basis** $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$

Observe can also measure a state $|\psi\rangle \in \mathbb{C}^d$ with respect to **arbitrary basis** $B = \{|b_0\rangle, \dots, |b_{d-1}\rangle\}$:

- Get outcome $|b_i\rangle$ with probability $|\langle\psi|b_i\rangle|^2$.

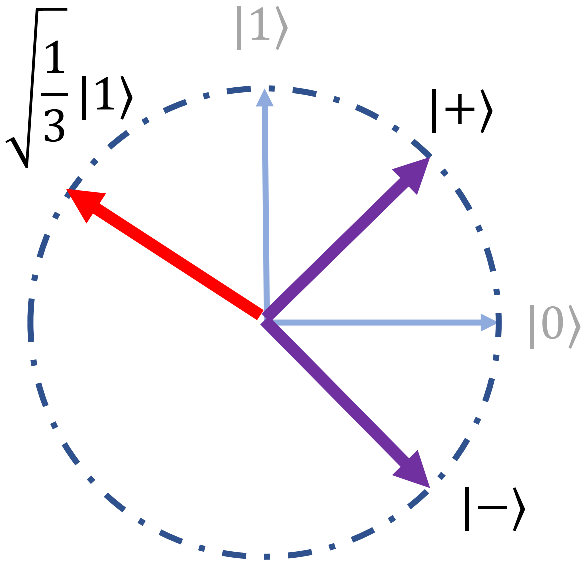
  i.e. square overlap with $|b_i\rangle$

- State gets **collapsed** to $|b_i\rangle$.

  i.e. state is projected to $|b_i\rangle$

Measuring in different bases

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

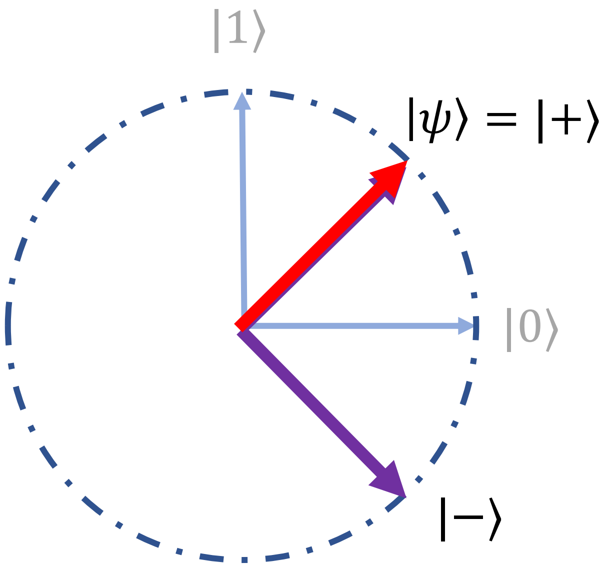


Before

Diagonal Basis

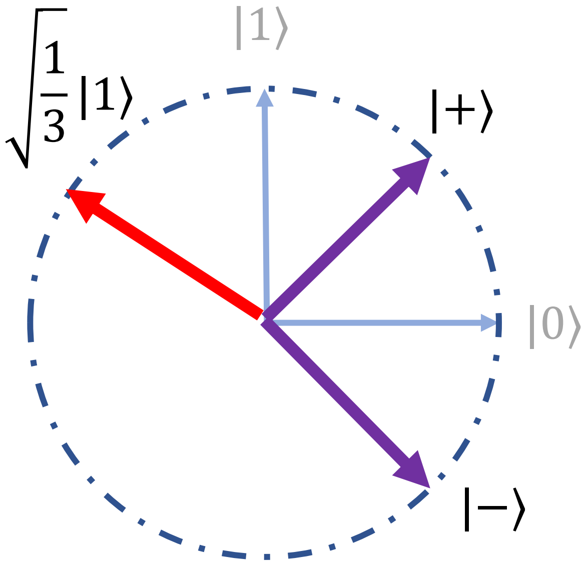
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Obtain $|+\rangle$ with probability $|\langle\psi|+\rangle|^2$



Measuring in different bases

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

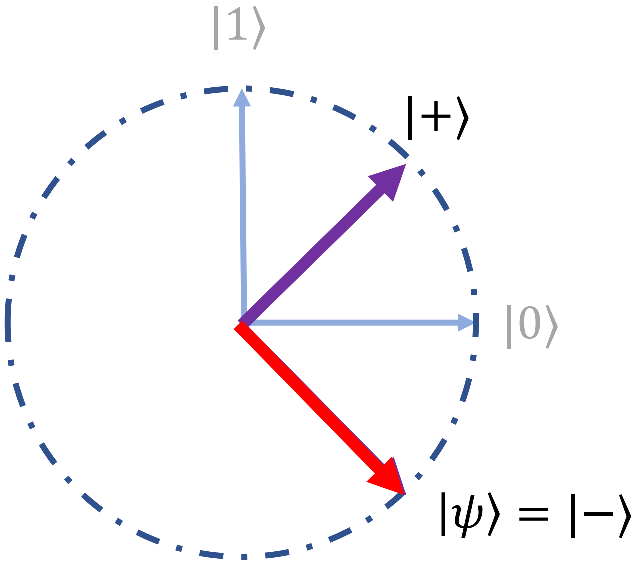


Before

Diagonal Basis

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

Obtain $|-\rangle$ with probability $|\langle\psi|-\rangle|^2$

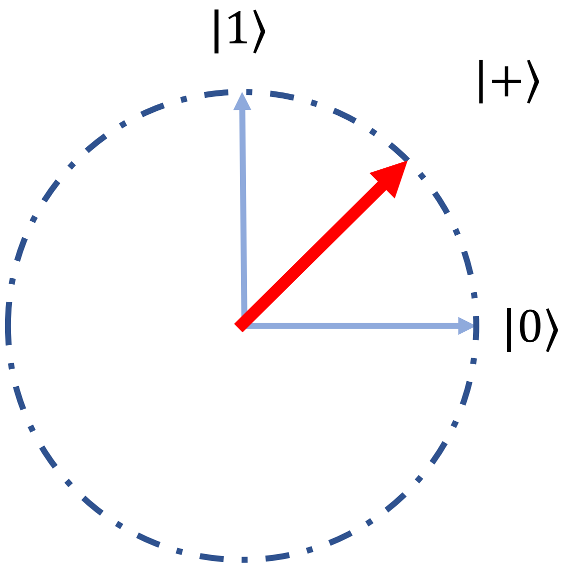


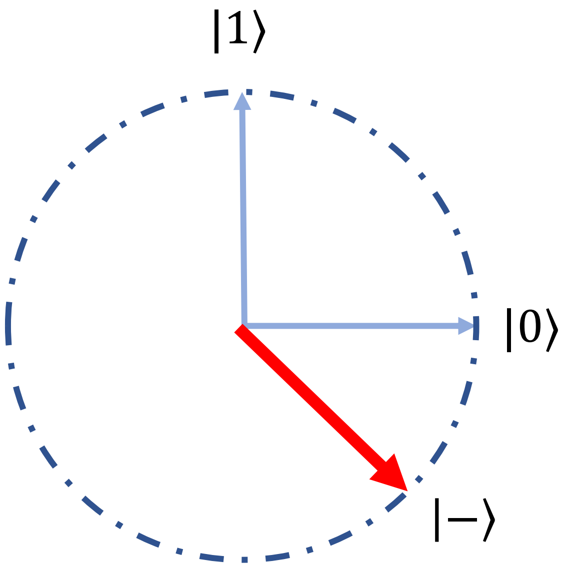
Quantum vs classical bits

Quantum vs classical bits

- Is there an essential difference between a quantum bit and a classical bit? For example, does allowing negative or complex amplitudes actually make a discernible difference?

- **Ex**: $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ versus $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$





What happens when we measure these two states?

Quantum vs classical bits

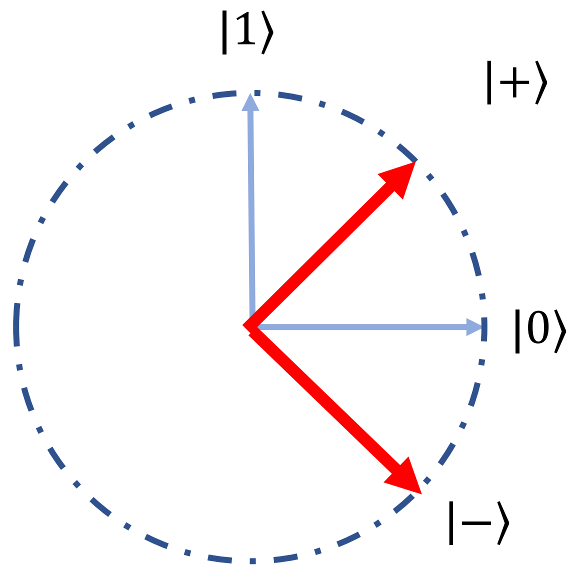
- $|+\rangle$ and $|-\rangle$ states are *orthogonal* to each other. To see this using the Dirac notation:

$$\langle -|+\rangle =$$

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

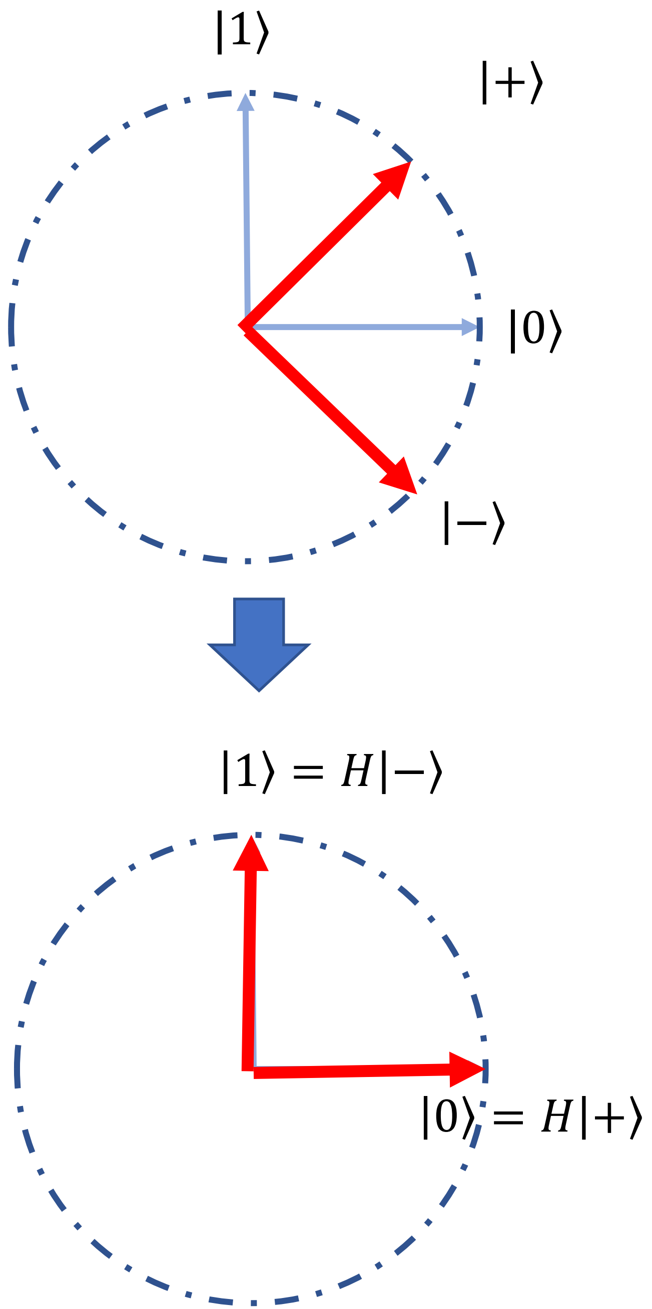
Quantum vs classical bits

- Suppose we had an unknown state $|\psi\rangle$ that was either $|+\rangle$ or $|-\rangle$. How could the observer tell the difference?

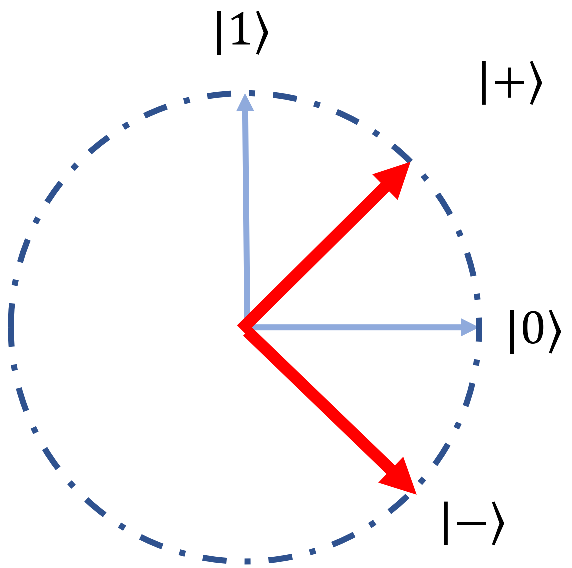


Quantum vs classical bits

- Suppose we had an unknown state $|\psi\rangle$ that was either $|+\rangle$ or $|-\rangle$. How could the observer tell the difference?
- Before measuring, apply a **unitary** $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
    - Also known as the *Hadamard gate*
    - Unitaries can be thought as ***change-of-basis operators***
- $H|+\rangle =$
- $H|-\rangle =$
- Measuring the rotated state now tells us what $|\psi\rangle$ originally was!



Quantum vs classical bits



- **Takeaway:** Minus signs in the amplitudes 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) to distinguish between $|\psi\rangle$ and $-|\psi\rangle$, or in fact $\alpha|\psi\rangle$ for any complex number α of norm 1.
  - This is because $U(-|\psi\rangle) = -U|\psi\rangle$, and measurements at the end destroy sign information, because we're taking the absolute value of the amplitudes!

Heisenberg Uncertainty Principle

Popular Science Physics: *Cannot simultaneously know the position and velocity of a particle.*

Heisenberg Uncertainty Principle (HUP) refers to measurements of a state with respect to ***incompatible*** bases.

Heisenberg Uncertainty Principle

Popular Science Physics: *Cannot simultaneously know the position and velocity of a particle.*

Heisenberg Uncertainty Principle (HUP) refers to measurements of a state with respect to ***incompatible*** bases.

Def: Bases $A = \{|a_0\rangle, \ldots, |a_{d-1}\rangle\}$ and $B = \{|b_0\rangle, \ldots, |b_{d-1}\rangle\}$ are ***compatible*** if A and B are the same up to permutation and global phases.

- **Ex**: $A = \{|0\rangle, |1\rangle\}$ and $B = \{\ |1\rangle\ \ ,\ \ i|0\rangle\ \}$ are compatible.

Otherwise, they are ***incompatible***.

- **Ex**: $A = \{|0\rangle, |1\rangle\}$ and $B = \{\ |+\rangle,\ \ |-\rangle\ \}$ are *in*compatible.

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

Heisenberg Uncertainty Principle

Def: A state $|\psi\rangle \in \mathbb{C}^d$ is ***determined*** in a basis $B = \{|b_0\rangle, \dots, |b_{d-1}\rangle\}$ if measuring according to B yields a fixed state $|b_i\rangle$ with probability 1.

HUP for Qubits (simplest version): A qubit state $|\psi\rangle \in \mathbb{C}^2$ cannot be simultaneously determined in two incompatible bases.

Heisenberg Uncertainty Principle

Def: $Var(|\psi\rangle, A) = 4\, p_0 \cdot p_1$, where p_i = probability of obtaining outcome $|a_i\rangle$ when measuring $|\psi\rangle$ with respect to basis A.

HUP for Qubits (quantitative): Let A = standard basis, B = diagonal basis. For all $|\psi\rangle \in \mathbb{C}^2$,

$$Var(|\psi\rangle, A) + Var(|\psi\rangle, B) \geq 1.$$

Quantum Zeno Effect

Quantum version of the idiom "*A watched pot never boils*."

Intermediate measurements can drastically change
the outcome of a quantum experiment:

Experiment A (pot left alone)

1. Qubit starts in $|0\rangle$ state.
2. Repeat $\mathrm{k} = \lceil \frac{\pi}{2\theta} \rceil$ times:
   1. Apply $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ to qubit.
3. Measure qubit in standard basis.

Quantum Zeno Effect

Quantum version of the idiom "*A watched pot never boils.*"

Intermediate measurements can drastically change the outcome of a quantum experiment:

Experiment A (pot left alone)

1. Qubit starts in $|0\rangle$ state.
2. Repeat $\mathrm{k} = \lceil \frac{\pi}{2\theta} \rceil$ times:
    1. Apply $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ to qubit.
3. Measure qubit in standard basis.

Experiment B (watched pot)

1. Qubit starts in $|0\rangle$ state.
2. Repeat $\mathrm{k} = \lceil \frac{\pi}{2\theta} \rceil$ times:
    1. Apply R_θ to qubit.
    2. Measure in standard basis.
3. Measure qubit in standard basis.

Quantum Zeno Effect

1. Qubit starts in $|0\rangle$ state.
2. Repeat $\mathrm{k} = \lceil \frac{\pi}{2\theta} \rceil$ times:
    1. Apply R_θ to qubit.
3. Measure qubit in standard basis.

- $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is a rotation by angle θ.
- If $|\psi\rangle = \cos\alpha\ |0\rangle + \sin\alpha\ |1\rangle$, then $R_\theta|\psi\rangle = \cos\,(\alpha+\theta)\ |0\rangle + \sin(\alpha+\theta)\ |1\rangle$
- **Experiment A** (pot left alone): final state is $R_\theta^k|0\rangle$

Quantum Zeno Effect

1. Qubit starts in $|0\rangle$ state.
2. Repeat $\mathrm{k} = [\frac{\pi}{2\theta}]$ times:
    1. Apply R_θ to qubit.
    2. Measure in standard basis.
3. Measure qubit in standard basis.

- $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is a rotation by angle θ.
- If $|\psi\rangle = \cos\alpha\ |0\rangle + \sin\alpha\ \ |1\rangle$, then $R_\theta|\psi\rangle = \cos\,(\alpha+\theta)\ |0\rangle + \sin(\alpha+\theta)\ \ |1\rangle$
- **Experiment B** (watched pot):

Composite quantum systems

Composite quantum systems

- The state of a qubit is a unit vector in the space $\mathbb{C}^2$.
  - Also called the **Hilbert space** of a qubit.
  - Hilbert space = complex vector space with inner product.

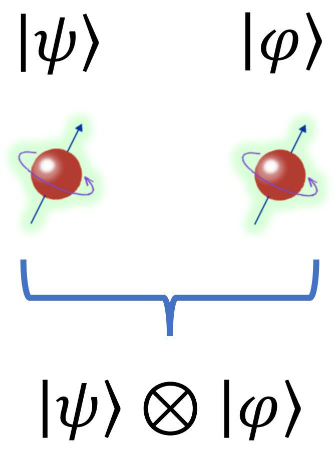
Composite quantum systems

- The state of a qubit is a unit vector in the space $\mathbb{C}^2$.
  - Also called the **Hilbert space** of a qubit.
  - Hilbert space = complex vector space with inner product.
- The Hilbert space of 2 qubits is the **tensor product space** $\mathbb{C}^2 \otimes \mathbb{C}^2$
  - $\mathbb{C}^2$ has orthonormal basis $\{|0\rangle, |1\rangle\}$.
  - The tensor product space $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$ is 4-dimensional, with orthonormal basis

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

  - Shorthand: $|ij\rangle = |i, j\rangle = |i\rangle|j\rangle = |i\rangle \otimes |j\rangle$.
  - This basis represents the **classical** states of the two qubits.

Composite quantum systems



- **Tensor product of vectors:** if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and $|\varphi\rangle = \gamma|0\rangle + \delta|1\rangle$, then the state of the two qubits together is

$$|\psi\rangle \otimes |\varphi\rangle =$$

Composite quantum systems

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

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

- General two-qubit states **cannot** be written as a tensor product state

$$|\psi\rangle \neq |\varphi\rangle \otimes |\theta\rangle$$

  for one-qubit states $|\varphi\rangle, |\theta\rangle \in \mathbb{C}^2$.

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

Composite quantum systems

- **Ex**: $|EPR\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$ is entangled.

- **Ex**: $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ 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 $|\psi\rangle = \sum_{i,j} \alpha_{ij}\, |i,j\rangle$ and $|\theta\rangle = \sum_{i,j} \beta_{ij}\, |i,j\rangle$. Then

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

Measurements

- **Measuring** two-qubit states $|\psi\rangle = \sum \alpha_{ij} |ij\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$:
    - Obtain classical outcome $(i, j) \in \{0,1\}^2$ with probability $|\alpha_{ij}|^2$.
    - The **post-measurement** state of $|\psi\rangle$ is then $|i, j\rangle$

Partial Measurements

- What if we only want to measure the first qubit?
- To compute probability of obtaining outcome $i \in \{0,1\}$:
- State gets **projected** to basis states where the first qubit is in the state $|i\rangle$.

$$|\psi_i'\rangle = \sum_j \alpha_{ij} |ij\rangle$$

Unnormalized state

- Probability p_i is squared length of $|\psi'\rangle$, which is $\sum_j |\alpha_{ij}|^2$.
- The **post-measurement** state is $|\psi'\rangle$ renormalized:

$$|\psi_i\rangle = \frac{1}{\sqrt{p_i}} \sum_j \alpha_{ij} |ij\rangle = |i\rangle \otimes \frac{1}{\sqrt{p_i}} \sum_j \alpha_{ij} |j\rangle$$

Partial Measurements

Ex: measure first qubit of $|\psi\rangle = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{6}}|01\rangle - \sqrt{\frac{1}{6}}|11\rangle$

Unitaries on multiple qubits

- Two-qubit systems in isolation undergo evolution via unitary operators acting on $\mathbb{C}^2 \otimes \mathbb{C}^2$.
- Tensor product of unitaries:
  - Let U, V be one-qubit unitaries.
  - Applying U to the left qubit and V to the right qubit, from the perspective of the larger system, corresponds to the unitary $U \otimes V$.

- Matrix representation:
  - $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}, V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}$
  - $U \otimes V = \begin{pmatrix} u_{11}V & u_{12}V \\ u_{21}V & u_{22}V \end{pmatrix}$ is a 4×4 matrix

Matrix representation depends on how you label your rows/columns!

Unitaries on multiple qubits

- **Ex**: $|\psi\rangle = |0\rangle \otimes |0\rangle, U = V = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- **Ex**: $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle), \;\; U = V = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Unitaries on multiple qubits

- **Ex**: $|\psi\rangle = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{6}}|01\rangle - \sqrt{\frac{1}{6}}|11\rangle,\ U = V = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Unitaries on multiple qubits

- In general, two-qubit unitaries are not product operators; they are **entangling**.
- **Ex:** CNOT ("controlled-NOT") acts on 2-qubits: for all $x \in \{0,1\}$

$$CNOT|x\rangle \otimes |0\rangle = |x\rangle \otimes |x\rangle$$
$$CNOT|x\rangle \otimes |1\rangle = |x\rangle \otimes |x \oplus 1\rangle$$

Ctrl Tgt

CNOT flips a target qubit, based on control qubit.

- **Ex**: $|\psi\rangle = |+\rangle \otimes |0\rangle$. $\mathrm{CNOT}|\psi\rangle =$
- Explicit matrix representation of CNOT (not that useful)

The 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

$$U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

ancilla qubit

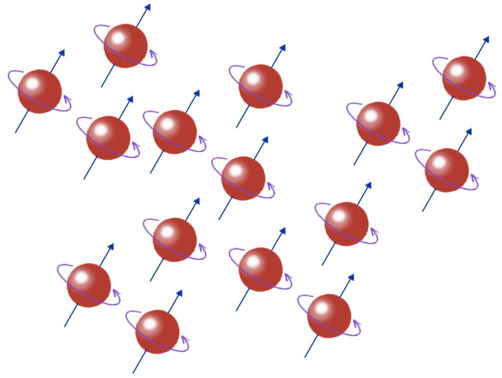
- for all one-qubit states $|\psi\rangle$.

The No-Cloning Theorem

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

The exponentiality of QM

- The joint state of n qubits is represented as a vector in $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$:



$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x \, |x\rangle$$

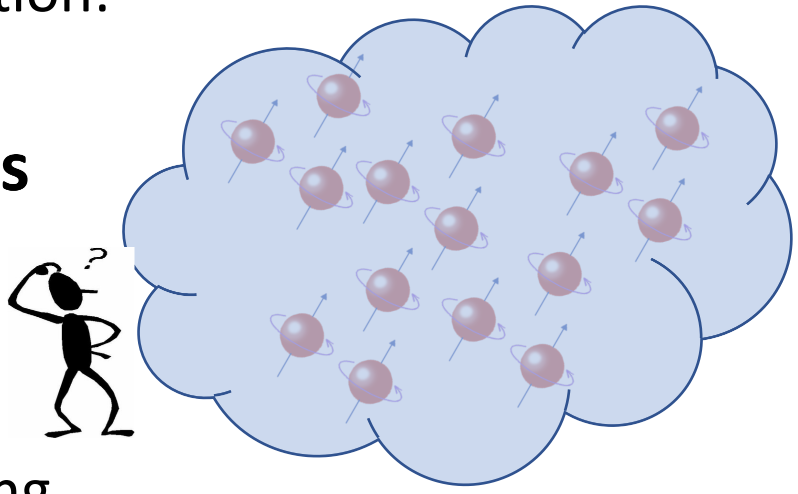
- Each additional qubit **doubles** the dimensionality of the Hilbert space.
- Applying a unitary U to an n-qubit state $|\psi\rangle$ appears to be doing exponentially many computations in parallel:

$$U|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x \, U|x\rangle$$

The exponentiality of QM, redux

- Nature is doing an incredible amount of work for us.
- However, this extravagance is hidden behind the veil of **measurement**.
- We can only access the exponential information stored in $|\psi\rangle$ in a limited way.
- This leads to a fundamental tension in quantum information:

The exponentiality vs fragility of quantum states



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