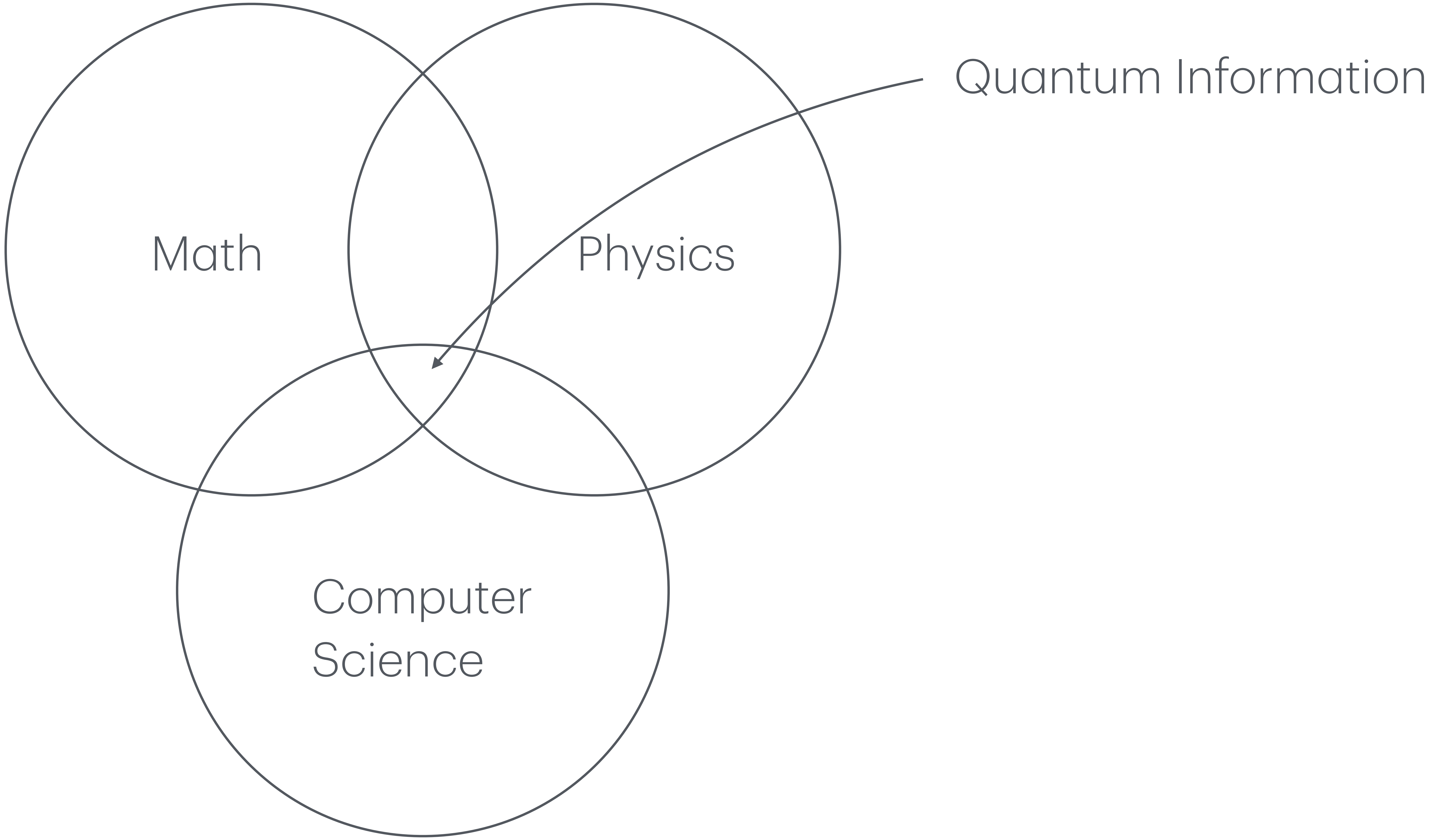
Introduction to Quantum Information

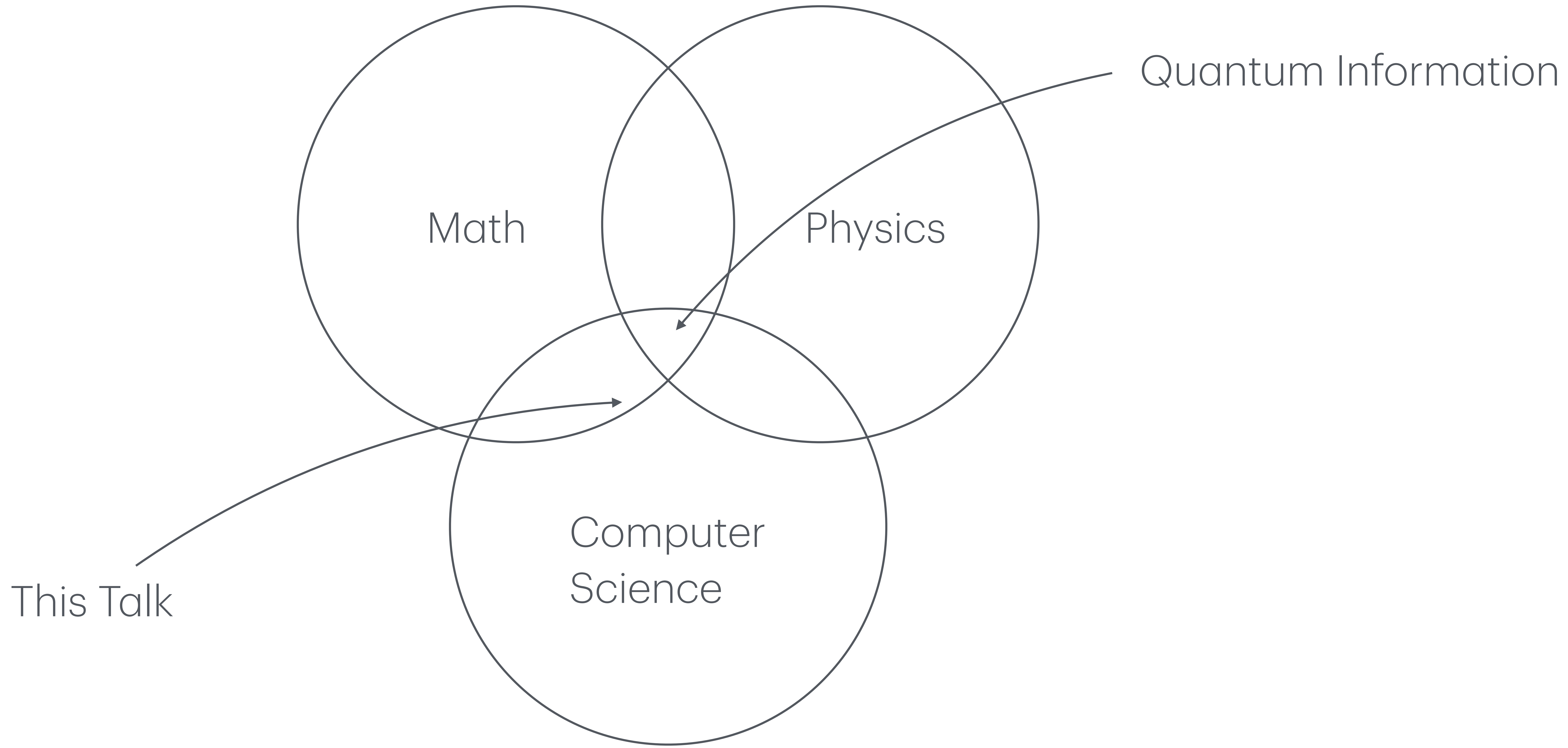
Giulio Malavolta

Bocconi University

Quantum Information



Quantum Information



Linear Algebra Review

Linear Algebra Review

- A complex number $\alpha \in \mathbb{C}$ is expressed as

$$\alpha = a + ib \qquad a, b \in \mathbb{R}$$

Linear Algebra Review

- A complex number $\alpha \in \mathbb{C}$ is expressed as

$$\alpha = a + ib \qquad a, b \in \mathbb{R}$$

- Conjugate: $\alpha^* = a - ib$

Linear Algebra Review

- A complex number $\alpha \in \mathbb{C}$ is expressed as

$$\alpha = a + ib \qquad a, b \in \mathbb{R}$$

- Conjugate: $\alpha^* = a - ib$
- Norm: $|\alpha| = \sqrt{a^2 + b^2}$

Linear Algebra Review

- A complex number $\alpha \in \mathbb{C}$ is expressed as

$$\alpha = a + ib \qquad a, b \in \mathbb{R}$$

- Conjugate: $\alpha^* = a - ib$
- Norm: $|\alpha| = \sqrt{a^2 + b^2}$
- Inner product:

$$< \phi, \psi > = \sum_i \phi_i^* \cdot \psi_i \qquad \phi, \psi \in \mathbb{C}^n$$

Linear Algebra Review

- A complex number $\alpha \in \mathbb{C}$ is expressed as

$$\alpha = a + ib \qquad a, b \in \mathbb{R}$$

- Conjugate: $\alpha^* = a - ib$
- Norm: $|\alpha| = \sqrt{a^2 + b^2}$
- Inner product:

$$< \phi, \psi > = \sum_i \phi_i^* \cdot \psi_i \qquad \phi, \psi \in \mathbb{C}^n$$

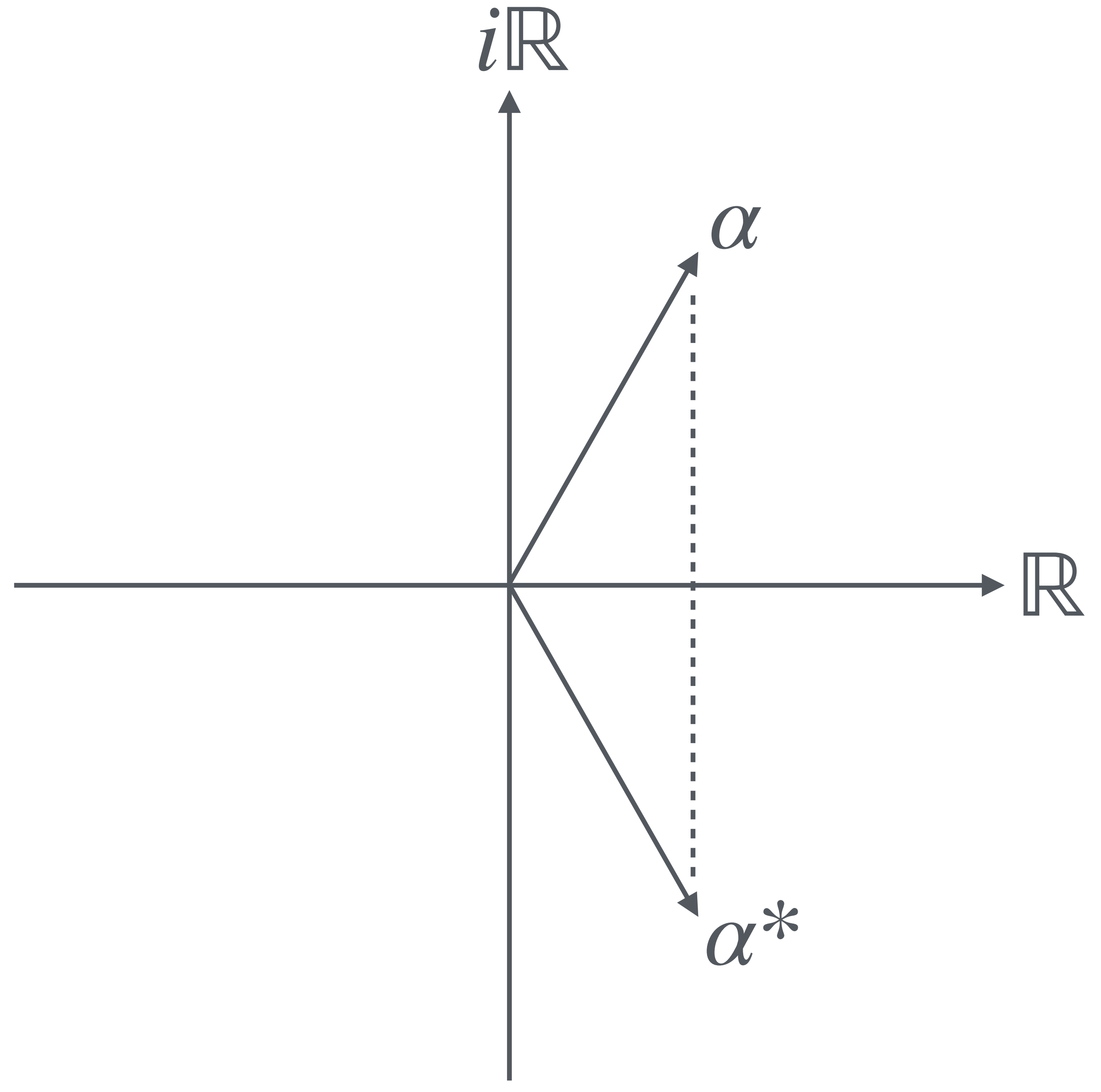
- Matrix conjugate: $M^\dagger_{i,j} = M^*_{j,i}$ where $M \in \mathbb{C}^{n \times n}$

Linear Algebra Review

- A complex number $\alpha \in \mathbb{C}$ is expressed as

$$\alpha = a + ib \qquad a, b \in \mathbb{R}$$

- Conjugate: $\alpha^* = a - ib$
- Norm: $|\alpha| = \sqrt{a^2 + b^2}$



The Basic Unit of Information

The Basic Unit of Information

The Basic Unit of Information

- A qubit is a unit vector in $\mathbb{C}^2$

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

The Basic Unit of Information

- A qubit is a unit vector in $\mathbb{C}^2$

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

- Without loss of generality, I can write a qubit as:

$$|\psi> = \alpha|0> + \beta|1>$$

$$\alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

The Basic Unit of Information

- A qubit is a unit vector in $\mathbb{C}^2$

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

- Without loss of generality, I can write a qubit as:

$$|\psi> = \alpha|0> + \beta|1>$$

$$\alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

- If both amplitudes are non-zero, then we say that the qubit is in superposition

The Basic Unit of Information

The Basic Unit of Information

- A qubit is a unit vector in $\mathbb{C}^2$

$$|\psi> = \alpha|0> + \beta|1>$$

$$\alpha, \beta \in \mathbb{C}$$

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

The Basic Unit of Information

- A qubit is a unit vector in $\mathbb{C}^2$

$$|\psi> = \alpha|0> + \beta|1>$$

$$\alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

- A bit is a variable $b \in \{0,1\}$

The Basic Unit of Information

- A qubit is a unit vector in $\mathbb{C}^2$

$$|\psi> = \alpha|0> + \beta|1>$$

$$\alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

- A bit is a variable $b \in \{0,1\}$

- A binary random variable X is 0 with probability p and 1 with probability 1-p

$$X = \alpha|0> + \beta|1>$$

$$\alpha, \beta \in \mathbb{R}^+$$
$$\alpha + \beta = 1$$

The Basic Unit of Information

- A qubit is a unit vector in $\mathbb{C}^2$

$$|\psi> = \alpha|0> + \beta|1>$$

$$\alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

- A bit is a variable $b \in \{0,1\}$
- A binary random variable X is 0 with probability p and 1 with probability 1-p

$$X = \alpha|0> + \beta|1>$$
$$\|X\|_1 = 1$$

$$\alpha, \beta \in \mathbb{R}^+$$
$$\alpha + \beta = 1$$

The Basic Unit of Information

The Basic Unit of Information

- Take two qubits

$$|\psi_0> = \alpha_0|0> + \beta_0|1> \qquad |\psi_1> = \alpha_1|0> + \beta_1|1>$$

The Basic Unit of Information

- Take two qubits

$$|\psi_0> = \alpha_0|0> + \beta_0|1> \qquad\qquad |\psi_1> = \alpha_1|0> + \beta_1|1>$$

- To describe the joint state of the system we need to expand the space to $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$

The Basic Unit of Information

- Take two qubits

$$|\psi_0 > = \alpha_0|0 > + \beta_0|1 > \qquad |\psi_1 > = \alpha_1|0 > + \beta_1|1 >$$

- To describe the joint state of the system we need to expand the space to $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$

- The description of the joint state is obtained by:

$$|\psi_0 > \otimes |\psi_1 > = |\psi_0 > |\psi_1 > = |\psi_0, \psi_1 >$$

The Basic Unit of Information

- Take two qubits

$$|\psi_0 > = \alpha_0|0 > + \beta_0|1 > \qquad\qquad |\psi_1 > = \alpha_1|0 > + \beta_1|1 >$$

- To describe the joint state of the system we need to expand the space to $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$
- The description of the joint state is obtained by:

$$|\psi_0 > \otimes |\psi_1 > = |\psi_0 > |\psi_1 > = |\psi_0, \psi_1 >$$

- We can think of a qubit as being physically located in a register and the act of adjoining two registers is equivalent to taking the *tensor product* of the two states

The Basic Unit of Information

- Take two qubits

$$|\psi_0> = \alpha_0|0> + \beta_0|1> \qquad\qquad |\psi_1> = \alpha_1|0> + \beta_1|1>$$

- To describe the joint state of the system we need to expand the space to $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$
- The description of the joint state is obtained by:

$$|\psi_0> \otimes |\psi_1> = |\psi_0>|\psi_1> = |\psi_0, \psi_1>$$

- We can think of a qubit as being physically located in a register and the act of adjoining two registers is equivalent to taking the *tensor product* of the two states
- Of course nothing stops us from introducing more qubits to the system…

Quantum States

Quantum States

- POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$

Quantum States

- POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$
- For instance an n-qubit state lives in an $N = 2^n$ dimensional space

Quantum States

- POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$
- For instance an n-qubit state lives in an $N = 2^n$ dimensional space
- To represent such vector, we can use any basis of $\mathbb{C}^N$, the canonical choice is the standard/computational basis:

$$|0> = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad |1> = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \cdots \quad |N-1> = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Quantum States

- POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$
- For instance an n-qubit state lives in an $N = 2^n$ dimensional space
- To represent such vector, we can use any basis of $\mathbb{C}^N$, the canonical choice is the standard/computational basis:

$$|0> = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad |1> = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \cdots \quad |N-1> = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

- Any (pure) quantum state can be written as:

$$|\psi> = \sum_x \alpha_x |x> \qquad \sum_x |\alpha_x|^2 = 1$$

Entanglement

Entanglement

- We have just seen that we can always compose quantum states in a joint system by taking their tensor product

Entanglement

- We have just seen that we can always compose quantum states in a joint system by taking their tensor product
    - The result is another quantum state in a larger Hilbert space

Entanglement

- We have just seen that we can always compose quantum states in a joint system by taking their tensor product
  - The result is another quantum state in a larger Hilbert space
- What about the reverse operation?

Entanglement

- We have just seen that we can always compose quantum states in a joint system by taking their tensor product
  - The result is another quantum state in a larger Hilbert space
- What about the reverse operation?
  - It turns out that we *cannot* always decompose a quantum state into a tensor product of states in smaller Hilbert spaces

Entanglement

- We have just seen that we can always compose quantum states in a joint system by taking their tensor product
    - The result is another quantum state in a larger Hilbert space
- What about the reverse operation?
    - It turns out that we *cannot* always decompose a quantum state into a tensor product of states in smaller Hilbert spaces
    - States that cannot be decomposed into tensors are called entangled

Examples

Examples

- Some examples of single-qubit states:

Examples

- Some examples of single-qubit states:

$$|+> = \frac{1}{\sqrt{2}} \left(|0> + |1> \right)$$

Examples

- Some examples of single-qubit states:

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

Examples

- Some examples of single-qubit states:

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

- Some examples of two-qubit states:

Examples

- Some examples of single-qubit states:

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

- Some examples of two-qubit states:

$$\frac{1}{2}\left(|00> + |01> + |10> + |11>\right) = |+> \otimes |+>$$

Examples

- Some examples of single-qubit states:

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

- Some examples of two-qubit states:

$$\frac{1}{2}\left(|00> + |01> + |10> + |11>\right) = |+> \otimes |+>$$

$$\frac{1}{\sqrt{2}}\left(|00> + |11>\right) = |EPR>$$

Some Remarks on Notation

Some Remarks on Notation

- The notation $|\psi >$ for a column vector is called a “ket”

Some Remarks on Notation

- The notation $|\psi>$ for a column vector is called a "ket"
- Its conjugate transpose is denoted by the "bra" $<\psi|$

Some Remarks on Notation

- The notation $|\psi>$ for a column vector is called a "ket"
- Its conjugate transpose is denoted by the "bra" $<\psi|$
- So the "bra-ket" is actually the inner product

$$<\psi|\psi> = \sum_i \psi_i^* \cdot \psi_i = 1$$

Some Remarks on Notation

- The notation $|\psi>$ for a column vector is called a "ket"
- Its conjugate transpose is denoted by the "bra" $<\psi|$
- So the "bra-ket" is actually the inner product

$$<\psi|\psi> = \sum_i \psi_i^* \cdot \psi_i = 1$$

- Besides "pure" quantum states, one can also consider (classical) probability distributions over quantum states

Some Remarks on Notation

- The notation $|\psi>$ for a column vector is called a "ket"
- Its conjugate transpose is denoted by the "bra" $<\psi|$
- So the "bra-ket" is actually the inner product

$$<\psi|\psi> = \sum_i \psi_i^* \cdot \psi_i = 1$$

- Besides "pure" quantum states, one can also consider (classical) probability distributions over quantum states
  - This is called a "mixed" state

Manipulating Quantum States

The Schrödinger Equation

The Schrödinger Equation

- Similarly to how we operate on classical variables, we can also manipulate quantum states

The Schrödinger Equation

- Similarly to how we operate on classical variables, we can also manipulate quantum states
    - The rules are different though, are we need to define what are the legal operations

The Schrödinger Equation

- Similarly to how we operate on classical variables, we can also manipulate quantum states
  - The rules are different though, are we need to define what are the legal operations
- POSTULATE #2: Quantum states evolve according to the Schrödinger equation

$$|\psi_t > = e^{-iHt} |\psi_0 >$$

The Schrödinger Equation

- Similarly to how we operate on classical variables, we can also manipulate quantum states
  - The rules are different though, are we need to define what are the legal operations
- POSTULATE #2: Quantum states evolve according to the Schrödinger equation

$$|\psi_t> = e^{-iHt}|\psi_0>$$

  - H is a Hermitian matrix (called the Hamiltonian) describing the evolution of the system

The Schrödinger Equation

- Similarly to how we operate on classical variables, we can also manipulate quantum states
    - The rules are different though, are we need to define what are the legal operations
- POSTULATE #2: Quantum states evolve according to the Schrödinger equation

$$|\psi_t> = e^{-iHt}|\psi_0>$$

- H is a Hermitian matrix (called the Hamiltonian) describing the evolution of the system
- For convenience, we have set the Planck constant to 1

Unitary Evolution

Unitary Evolution

- From a computing perspective, working with the Schrödinger equation is cumbersome

Unitary Evolution

- From a computing perspective, working with the Schrödinger equation is cumbersome
  - By “discretizing” the passage of time, we can restate the axiom in a more convenient (but completely equivalent) form

Unitary Evolution

- From a computing perspective, working with the Schrödinger equation is cumbersome
  - By “discretizing” the passage of time, we can restate the axiom in a more convenient (but completely equivalent) form
- POSTULATE #2: Quantum states evolve according to unitary operations

Unitary Evolution

- From a computing perspective, working with the Schrödinger equation is cumbersome
  - By “discretizing” the passage of time, we can restate the axiom in a more convenient (but completely equivalent) form
- POSTULATE #2: Quantum states evolve according to unitary operations
- A matrix U is unitary if $U^\dagger U = I$

Unitary Evolution

- From a computing perspective, working with the Schrödinger equation is cumbersome
  - By "discretizing" the passage of time, we can restate the axiom in a more convenient (but completely equivalent) form
- POSTULATE #2: Quantum states evolve according to unitary operations
- A matrix U is unitary if $U^\dagger U = I$
- A unitary matrix preserves norms, and thus it maps quantum states to quantum states

$$\|U\psi\|^2 = < U\psi | U\psi > = < \psi | U^\dagger U | \psi > = < \psi | \psi > = 1$$

The Measurement

The Measurement

- Sadly, we are classical beings (= not quantum states) so we need a way to read classical information off a quantum state

The Measurement

- Sadly, we are classical beings (= not quantum states) so we need a way to read classical information off a quantum state
- Fortunately, quantum mechanics has a rule that determines what happens when a quantum state is *measured* by a classical observer

The Measurement

- Sadly, we are classical beings (= not quantum states) so we need a way to read classical information off a quantum state
- Fortunately, quantum mechanics has a rule that determines what happens when a quantum state is *measured* by a classical observer
  - This connects quantum states to good-old classical probability distributions

The Measurement

- Sadly, we are classical beings (= not quantum states) so we need a way to read classical information off a quantum state
- Fortunately, quantum mechanics has a rule that determines what happens when a quantum state is *measured* by a classical observer
  - This connects quantum states to good-old classical probability distributions
- POSTULATE #3: The probability that measuring a quantum state yields a given result is described by the Born rule

The Measurement

- Sadly, we are classical beings (= not quantum states) so we need a way to read classical information off a quantum state
- Fortunately, quantum mechanics has a rule that determines what happens when a quantum state is *measured* by a classical observer
  - This connects quantum states to good-old classical probability distributions
- POSTULATE #3: The probability that measuring a quantum state yields a given result is described by the Born rule
  - Any measurement will also change the quantum state in some way

The Measurement

- Sadly, we are classical beings (= not quantum states) so we need a way to read classical information off a quantum state
- Fortunately, quantum mechanics has a rule that determines what happens when a quantum state is *measured* by a classical observer
  - This connects quantum states to good-old classical probability distributions
- POSTULATE #3: The probability that measuring a quantum state yields a given result is described by the Born rule
  - Any measurement will also change the quantum state in some way
  - There is no notion of *passive* observer

The Born Rule (By Example)

The Born Rule (By Example)

- Measuring a qubit $|\psi> = \alpha|0> + \beta|1>$ yields

The Born Rule (By Example)

- Measuring a qubit $|\psi> = \alpha|0> + \beta|1>$ yields
  - 0 with probability $|\alpha|^2$ and the state collapses to $|0>$

The Born Rule (By Example)

- Measuring a qubit $|\psi> = \alpha|0> + \beta|1>$ yields
  - 0 with probability $|\alpha|^2$ and the state collapses to $|0>$
  - 1 with probability $|\beta|^2$ and the state collapses to $|1>$

The Born Rule (By Example)

- Measuring a qubit $|\psi> = \alpha|0> + \beta|1>$ yields
  - 0 with probability $|\alpha|^2$ and the state collapses to $|0>$
  - 1 with probability $|\beta|^2$ and the state collapses to $|1>$
- Performing the measurement again, will yield the same output, since the state is now collapsed to a basis state (one of the amplitudes = 1)

The Born Rule (By Example)

- Measuring a qubit $|\psi> = \alpha|0> + \beta|1>$ yields
  - 0 with probability $|\alpha|^2$ and the state collapses to $|0>$
  - 1 with probability $|\beta|^2$ and the state collapses to $|1>$
- Performing the measurement again, will yield the same output, since the state is now collapsed to a basis state (one of the amplitudes = 1)
- By default, measurements are done in the computational basis and the outcomes are defined by their basis states

The Born Rule (By Example)

- Measuring a qubit $|\psi> = \alpha|0> + \beta|1>$ yields
  - 0 with probability $|\alpha|^2$ and the state collapses to $|0>$
  - 1 with probability $|\beta|^2$ and the state collapses to $|1>$
- Performing the measurement again, will yield the same output, since the state is now collapsed to a basis state (one of the amplitudes = 1)
- By default, measurements are done in the computational basis and the outcomes are defined by their basis states
  - This is WLOG, since a basis change is a unitary operation

The Born Rule (By Example)

The Born Rule (By Example)

- We can also perform partial measurements on multi-qubit states

The Born Rule (By Example)

- We can also perform partial measurements on multi-qubit states
  - The residual state collapses to all basis states “consistent” with the outcome

The Born Rule (By Example)

- We can also perform partial measurements on multi-qubit states
  - The residual state collapses to all basis states “consistent” with the outcome
  - Amplitudes are normalized so that it is still a unit

The Born Rule (By Example)

- We can also perform partial measurements on multi-qubit states
  - The residual state collapses to all basis states “consistent” with the outcome
  - Amplitudes are normalized so that it is still a unit
- Measuring the first qubit of $|\psi> = \alpha_{00}|00> + \alpha_{01}|01> + \alpha_{10}|10> + \alpha_{11}|11>$

The Born Rule (By Example)

- We can also perform partial measurements on multi-qubit states
  - The residual state collapses to all basis states “consistent” with the outcome
  - Amplitudes are normalized so that it is still a unit
- Measuring the first qubit of $|\psi> = \alpha_{00}|00> + \alpha_{01}|01> + \alpha_{10}|10> + \alpha_{11}|11>$
  - 0 with probability $||\alpha_{00}||^2 + ||\alpha_{01}||^2$

    The state collapses to $\dfrac{\alpha_{00}|00> + \alpha_{01}|01>}{\sqrt{||\alpha_{00}||^2 + ||\alpha_{01}||^2}}$

The Born Rule (By Example)

- We can also perform partial measurements on multi-qubit states
  - The residual state collapses to all basis states “consistent” with the outcome
  - Amplitudes are normalized so that it is still a unit
- Measuring the first qubit of $|\psi> = \alpha_{00}|00> + \alpha_{01}|01> + \alpha_{10}|10> + \alpha_{11}|11>$
  - 1 with probability $\|\alpha_{10}\|^2 + \|\alpha_{11}\|^2$

    The state collapses to $\dfrac{\alpha_{10}|10> + \alpha_{11}|11>}{\sqrt{\|\alpha_{10}\|^2 + \|\alpha_{11}\|^2}}$

The No-Cloning Theorem

The No-Cloning Theorem

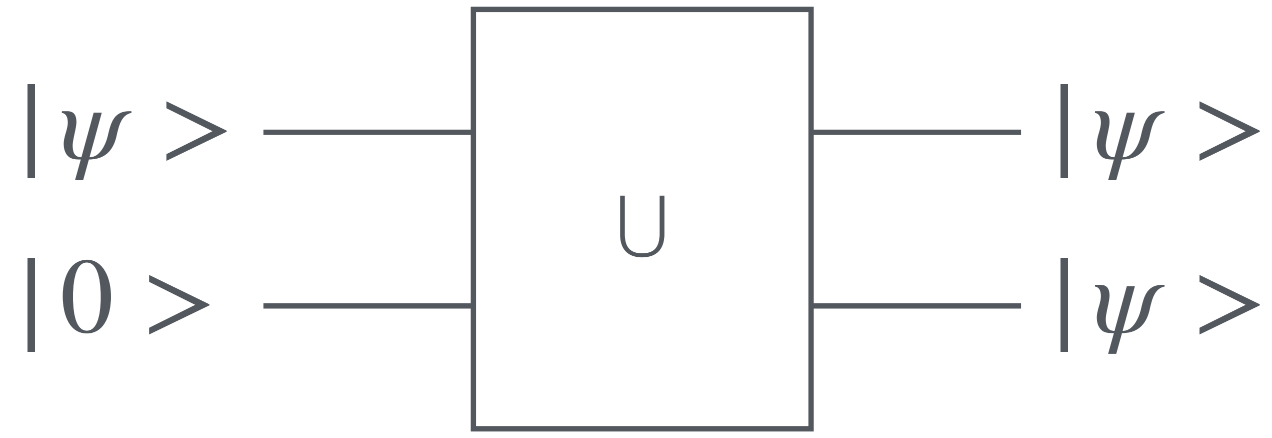
- An interesting consequence of the rules of quantum mechanics, is that it is in general impossible to create perfect copies of a given quantum state

The No-Cloning Theorem

- An interesting consequence of the rules of quantum mechanics, is that it is in general impossible to create perfect copies of a given quantum state
  - This is different from classical information, where it is easy to copy variables (cmd + C)

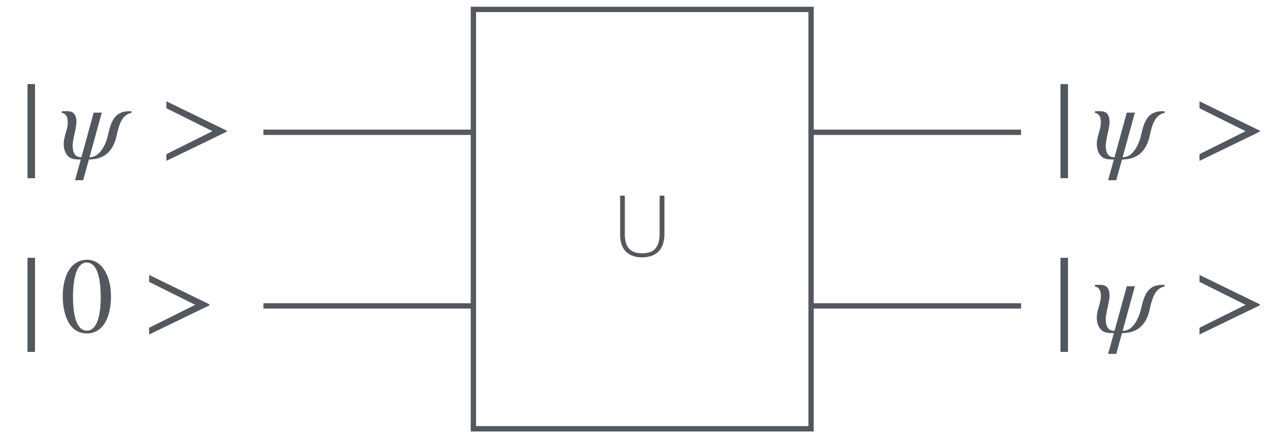
The No-Cloning Theorem

- An interesting consequence of the rules of quantum mechanics, is that it is in general impossible to create perfect copies of a given quantum state
    - This is different from classical information, where it is easy to copy variables (cmd + C)
- To see why, consider an ideal cloner



The No-Cloning Theorem

- An interesting consequence of the rules of quantum mechanics, is that it is in general impossible to create perfect copies of a given quantum state
  - This is different from classical information, where it is easy to copy variables (cmd + C)
- To see why, consider an ideal cloner



- This implements the mapping

$$U(\alpha|0> + \beta|1>) \otimes |0> \; = (\alpha|0> + \beta|1>) \otimes (\alpha|0> + \beta|1>)$$
$$= \alpha^2|00> + \alpha\beta|01> + \alpha\beta|10> + \beta^2|11>$$

which is not linear, and in particular not unitary

Computing with Quantum States

Recap of the Axioms

Recap of the Axioms

- Let us summarize what we have seen so far

Recap of the Axioms

- Let us summarize what we have seen so far
    - POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$

Recap of the Axioms

- Let us summarize what we have seen so far
  - POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$
  - POSTULATE #2: Quantum states evolve according to unitary operations

Recap of the Axioms

- Let us summarize what we have seen so far
  - POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$
  - POSTULATE #2: Quantum states evolve according to unitary operations
  - POSTULATE #3: The probability that measuring a quantum state yields a given result is described by the Born rule

Recap of the Axioms

- Let us summarize what we have seen so far
  - POSTULATE #1: A quantum state is a unit vector in a Hilbert space $\mathscr{H} \cong \mathbb{C}^N$
  - POSTULATE #2: Quantum states evolve according to unitary operations
  - POSTULATE #3: The probability that measuring a quantum state yields a given result is described by the Born rule
- Now that we know the rules, let us see how/what we can compute in this model

Warm Up: Computing Classical Functions

Warm Up: Computing Classical Functions

- Say that we want to compute a function $f: \{0,1\}^n \to \{0,1\}^n$ using the axioms of quantum mechanics

Warm Up: Computing Classical Functions

- Say that we want to compute a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ using the axioms of quantum mechanics
- In quantum terms, we want to find a unitary U such that

$$U|x> = |f(x)>$$

Warm Up: Computing Classical Functions

- Say that we want to compute a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ using the axioms of quantum mechanics

- In quantum terms, we want to find a unitary U such that

$$U|x > = |f(x) >$$

- It can be shown that, in order for such a unitary to exist, f has to be a bijection

Warm Up: Computing Classical Functions

- Say that we want to compute a function $f : \{0,1\}^n \to \{0,1\}^n$ using the axioms of quantum mechanics

- In quantum terms, we want to find a unitary U such that

$$U|x> = |f(x)>$$

- It can be shown that, in order for such a unitary to exist, f has to be a bijection

  - If U has collisions, it is not full rank, and thus it does not have an inverse (=> not unitary)

Warm Up: Computing Classical Functions

- Say that we want to compute a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ using the axioms of quantum mechanics

- In quantum terms, we want to find a unitary U such that

$$U|x> = |f(x)>$$

- It can be shown that, in order for such a unitary to exist, f has to be a bijection

  - If U has collisions, it is not full rank, and thus it does not have an inverse (=> not unitary)

  - The converse is also true

Warm Up: Computing Classical Functions

- Say that we want to compute a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ using the axioms of quantum mechanics

- In quantum terms, we want to find a unitary U such that

$$U|x> = |f(x)>$$

- It can be shown that, in order for such a unitary to exist, f has to be a bijection

  - If U has collisions, it is not full rank, and thus it does not have an inverse (=> not unitary)

  - The converse is also true

- So the question is, what kind of functions admit a “reversible” implementation?

Warm Up: Computing Classical Functions

Warm Up: Computing Classical Functions

- Clearly not all functions are reversible (think of the AND/XOR/OR functions) but some are (e.g. the NOT gate)

Warm Up: Computing Classical Functions

- Clearly not all functions are reversible (think of the AND/XOR/OR functions) but some are (e.g. the NOT gate)
- However, all logical gates can be "compiled" into a reversible gate

Warm Up: Computing Classical Functions

- Clearly not all functions are reversible (think of the AND/XOR/OR functions) but some are (e.g. the NOT gate)

- However, all logical gates can be "compiled" into a reversible gate

- The Toffoli gate is a reversible implementation of NAND (setting c = 1)

$$(a, b, c) \xrightarrow{\text{Toffoli}} (a, b, c \oplus a \wedge b)$$

the Toffoli gate it is its own inverse and thus can be implemented as a unitary

Warm Up: Computing Classical Functions

- Clearly not all functions are reversible (think of the AND/XOR/OR functions) but some are (e.g. the NOT gate)

- However, all logical gates can be "compiled" into a reversible gate

- The Toffoli gate is a reversible implementation of NAND (setting c = 1)

$$(a, b, c) \xrightarrow{\text{Toffoli}} (a, b, c \oplus a \wedge b)$$

  the Toffoli gate it is its own inverse and thus can be implemented as a unitary

- THEOREM: If f can be implemented using s-many NAND gates, it can be implemented using O(s)-many Toffoli gates

Warm Up: Computing Classical Functions

Warm Up: Computing Classical Functions

- COROLLARY: Any classical function f admits a unitary implementation U_f and furthermore if f is efficiently computable, then so is U_f

$$U_f|x>|0\ldots0> = |x>|f(x)>$$

Warm Up: Computing Classical Functions

- COROLLARY: Any classical function f admits a unitary implementation U_f and furthermore if f is efficiently computable, then so is U_f

$$U_f|x > |0\ldots0 > = |x > |f(x) >$$

- To make the transformation unitary, we had to add an extra state to the input $|0\ldots0 >$ which is referred to as the ancilla

Warm Up: Computing Classical Functions

- COROLLARY: Any classical function f admits a unitary implementation U_f and furthermore if f is efficiently computable, then so is U_f

$$U_f|x>|0\ldots0> = |x>|f(x)>$$

- To make the transformation unitary, we had to add an extra state to the input $|0\ldots0>$ which is referred to as the ancilla
  - There is nothing special about $0\ldots0$ you can use your favourite basis state and obtain $U_f|x>|y> = |x>|y \oplus f(x)>$

Warm Up: Computing Classical Functions

- COROLLARY: Any classical function f admits a unitary implementation U_f and furthermore if f is efficiently computable, then so is U_f

$$U_f|x>|0\ldots0> = |x>|f(x)>$$

- To make the transformation unitary, we had to add an extra state to the input $|0\ldots0>$ which is referred to as the ancilla
  - There is nothing special about $0\ldots0$ you can use your favourite basis state and obtain $U_f|x>|y> = |x>|y \oplus f(x)>$
- In complexity theory terms: P ⊆ BQP

Beyond Classical Functions?

Beyond Classical Functions?

- One may be tempted to believe that no classical computer can simulate a quantum process

Beyond Classical Functions?

- One may be tempted to believe that no classical computer can simulate a quantum process
- Sadly, this is not true. We know that BQP $\subseteq$ PSPACE

Beyond Classical Functions?

- One may be tempted to believe that no classical computer can simulate a quantum process
- Sadly, this is not true. We know that BQP $\subseteq$ PSPACE
  - Proof Sketch: Keep track of the evolution of the amplitudes. To make the space polynomial, use Feynman path integrals!

Beyond Classical Functions?

- One may be tempted to believe that no classical computer can simulate a quantum process
- Sadly, this is not true. We know that BQP $\subseteq$ PSPACE
  - Proof Sketch: Keep track of the evolution of the amplitudes. To make the space polynomial, use Feynman path integrals!
- The catch of course is that this simulation is *inefficient*

Beyond Classical Functions?

- One may be tempted to believe that no classical computer can simulate a quantum process
- Sadly, this is not true. We know that BQP $\subseteq$ PSPACE
  - Proof Sketch: Keep track of the evolution of the amplitudes. To make the space polynomial, use Feynman path integrals!
- The catch of course is that this simulation is *inefficient*
- The question to ask is: Are there quantum computations that we cannot simulate *efficiently* with classical computers?

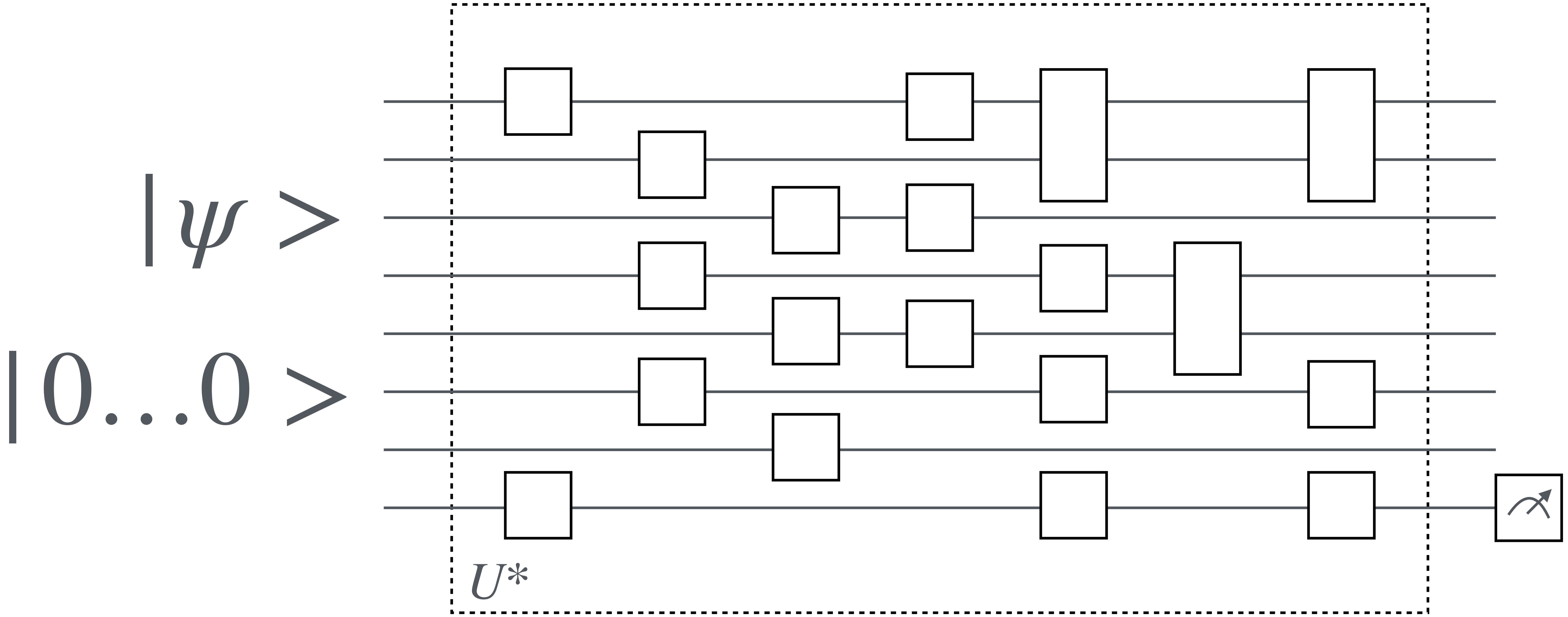
Quantum Circuits

Quantum Circuits

- Much like classical circuits, quantum circuits consist of collections of constant-size unitaries that together form a larger unitary

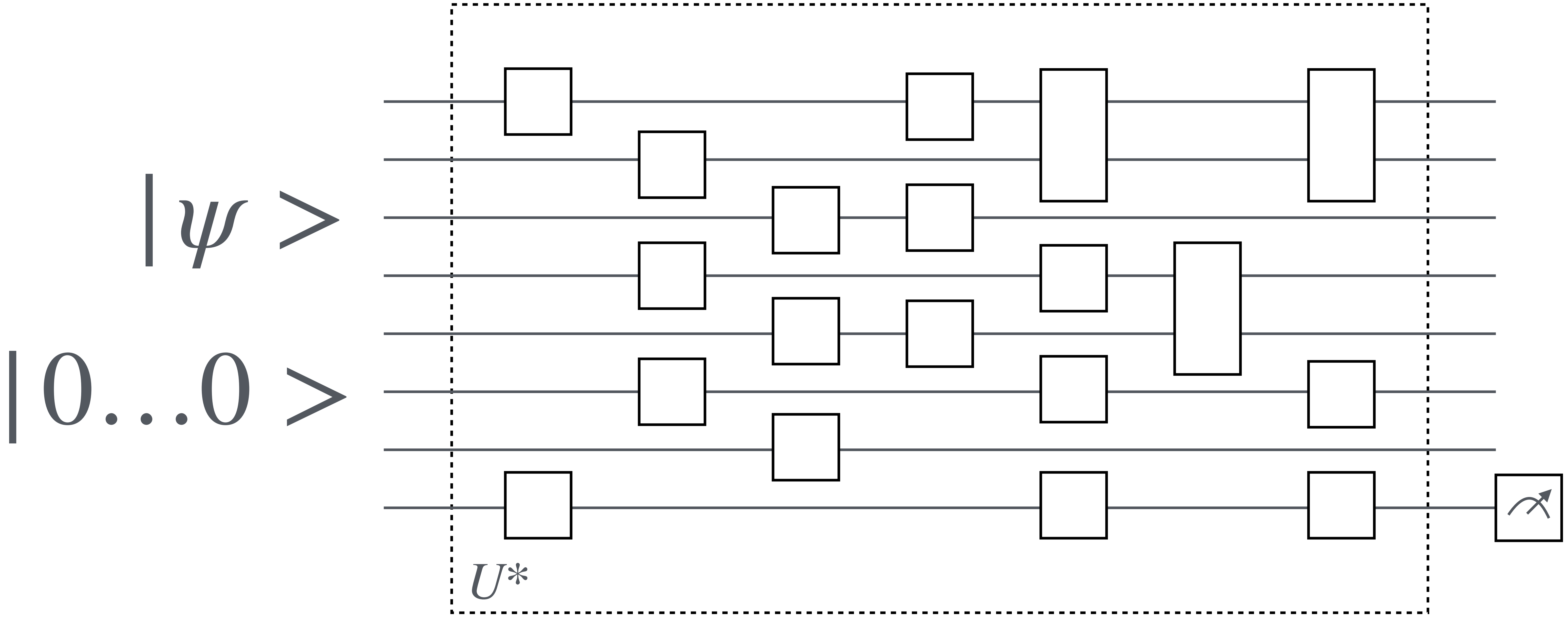
Quantum Circuits

- Much like classical circuits, quantum circuits consist of collections of constant-size unitaries that together form a larger unitary



Quantum Circuits

- Much like classical circuits, quantum circuits consist of collections of constant-size unitaries that together form a larger unitary



- Efficiency is measured in terms of number of gates (assuming each gate is a constant-size unitary)

Quantum Circuits

Quantum Circuits

- Also similarly to classical circuits, we can define sets of universal gates that allow us to approximate any unitary, with ε precision

Quantum Circuits

- Also similarly to classical circuits, we can define sets of universal gates that allow us to approximate any unitary, with ε precision

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

$$H | b > = \frac{1}{\sqrt{2}} (| 0 > + (-1)^b | 1 >)$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$T | b > = e^{b \cdot i\pi/4} | b >$$

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

$$CNOT | a, b > = | a, a \oplus b >$$

Quantum Circuits

- Also similarly to classical circuits, we can define sets of universal gates that allow us to approximate any unitary, with ε precision

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

$$H|b> = \frac{1}{\sqrt{2}}(|0> + (-1)^b|1>)$$

$$T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$$

$$T|b> = e^{b\cdot i\pi/4}|b>$$

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

$$CNOT|a,b> = |a, a \oplus b>$$

- The Solovay-Kitaev theorem bounds the number of gates (for *any* universal gate set) needed to approximate any (constant-dimension) unitary up to ε precision, by poly-log$(1/\varepsilon)$

Quantum Fourier Transform

Quantum Fourier Transform

- A recurring example of an operation that we believe is *not* simulatable classically is the Quantum Fourier Transform (QFT)

Quantum Fourier Transform

- A recurring example of an operation that we believe is *not* simulatable classically is the Quantum Fourier Transform (QFT)

- A special case of QFT ($\mathbb{F}_2^n$) is easily implemented with the Hadamard transform

$$H^{\otimes n} | x > = \frac{1}{\sqrt{N}} \sum_y (-1)^{x \cdot y} | y >$$

Quantum Fourier Transform

- A recurring example of an operation that we believe is *not* simulatable classically is the Quantum Fourier Transform (QFT)

- A special case of QFT ($\mathbb{F}_2^n$) is easily implemented with the Hadamard transform

$$H^{\otimes n}|x> = \frac{1}{\sqrt{N}}\sum_y (-1)^{x\cdot y}|y>$$

- The more general q-ary QFT is also efficiently computable, where $\omega_q = e^{2\pi i/q}$ is the q-th root of unity

$$QFT_q|x> = \frac{1}{\sqrt{N}}\sum_y \omega_q^{x\cdot y}|y>$$

Bonus: The CHSH Game

The EPR Paradox

The EPR Paradox

- A famous paper by Einstein-Podolski-Rosen considers the following scenario

The EPR Paradox

- A famous paper by Einstein-Podolski-Rosen considers the following scenario
- Prepare the 2-qubit state:

$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

The EPR Paradox

- A famous paper by Einstein-Podolski-Rosen considers the following scenario
- Prepare the 2-qubit state:

$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

- Send one qubit to Alice and the other to Bob (sitting at opposite sides of the universe)

The EPR Paradox

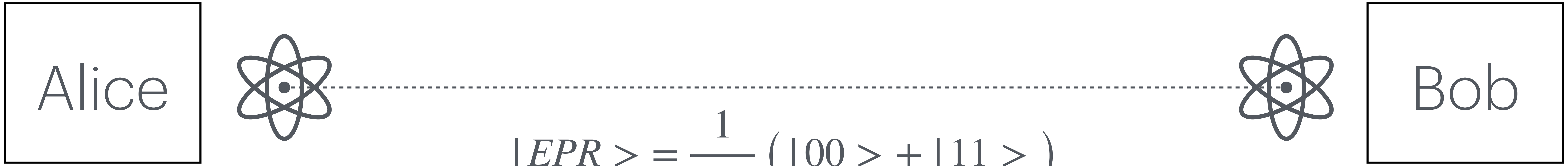
- A famous paper by Einstein-Podolski-Rosen considers the following scenario
- Prepare the 2-qubit state:

$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

- Send one qubit to Alice and the other to Bob (sitting at opposite sides of the universe)

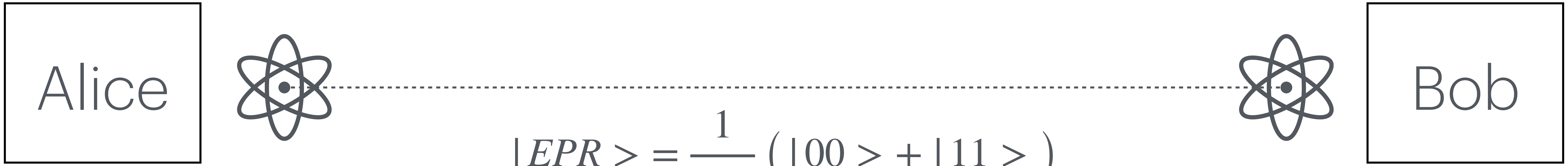
The EPR Paradox

The EPR Paradox



$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

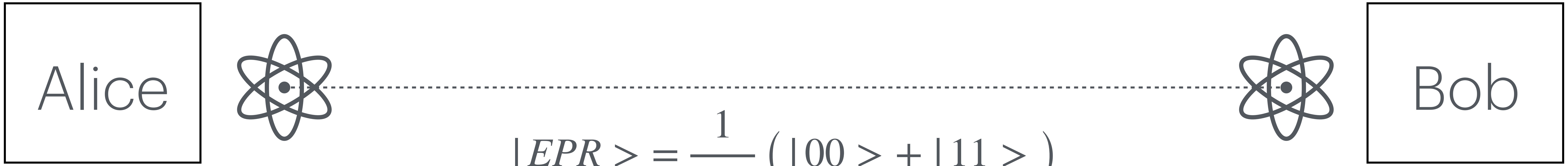
The EPR Paradox



$$|EPR> = \frac{1}{\sqrt{2}} \left(|00> + |11> \right)$$

- Measuring the qubits in the computational basis yields:

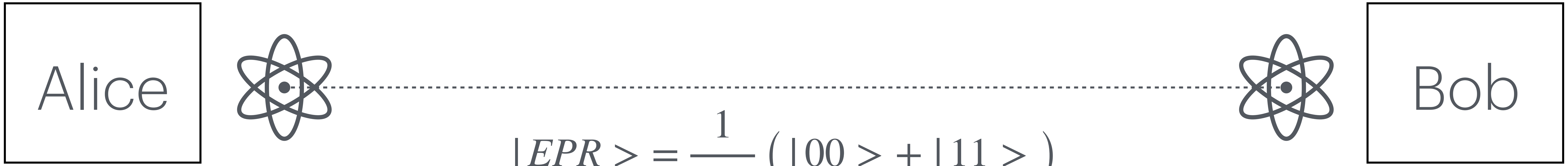
The EPR Paradox



$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

- Measuring the qubits in the computational basis yields:
  - With prob 1/2 Alice obtains 0 and Bob obtains 0

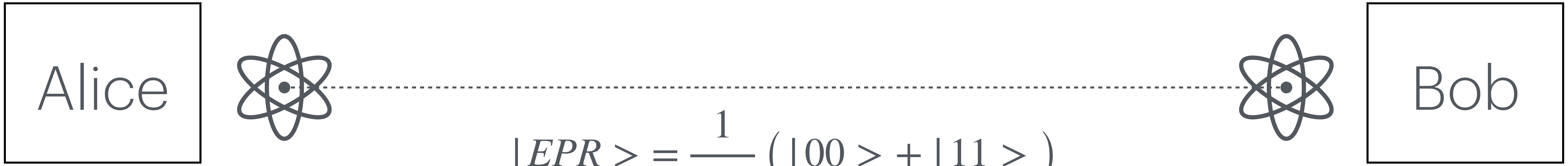
The EPR Paradox



$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

- Measuring the qubits in the computational basis yields:
  - With prob 1/2 Alice obtains 0 and Bob obtains 0
  - With prob 1/2 Alice obtains 1 and Bob obtains 1

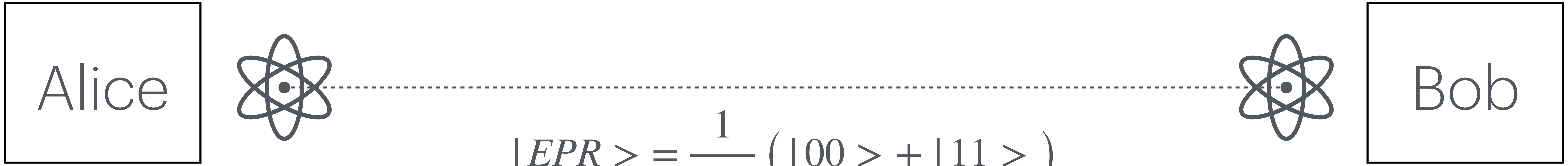
The EPR Paradox



$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

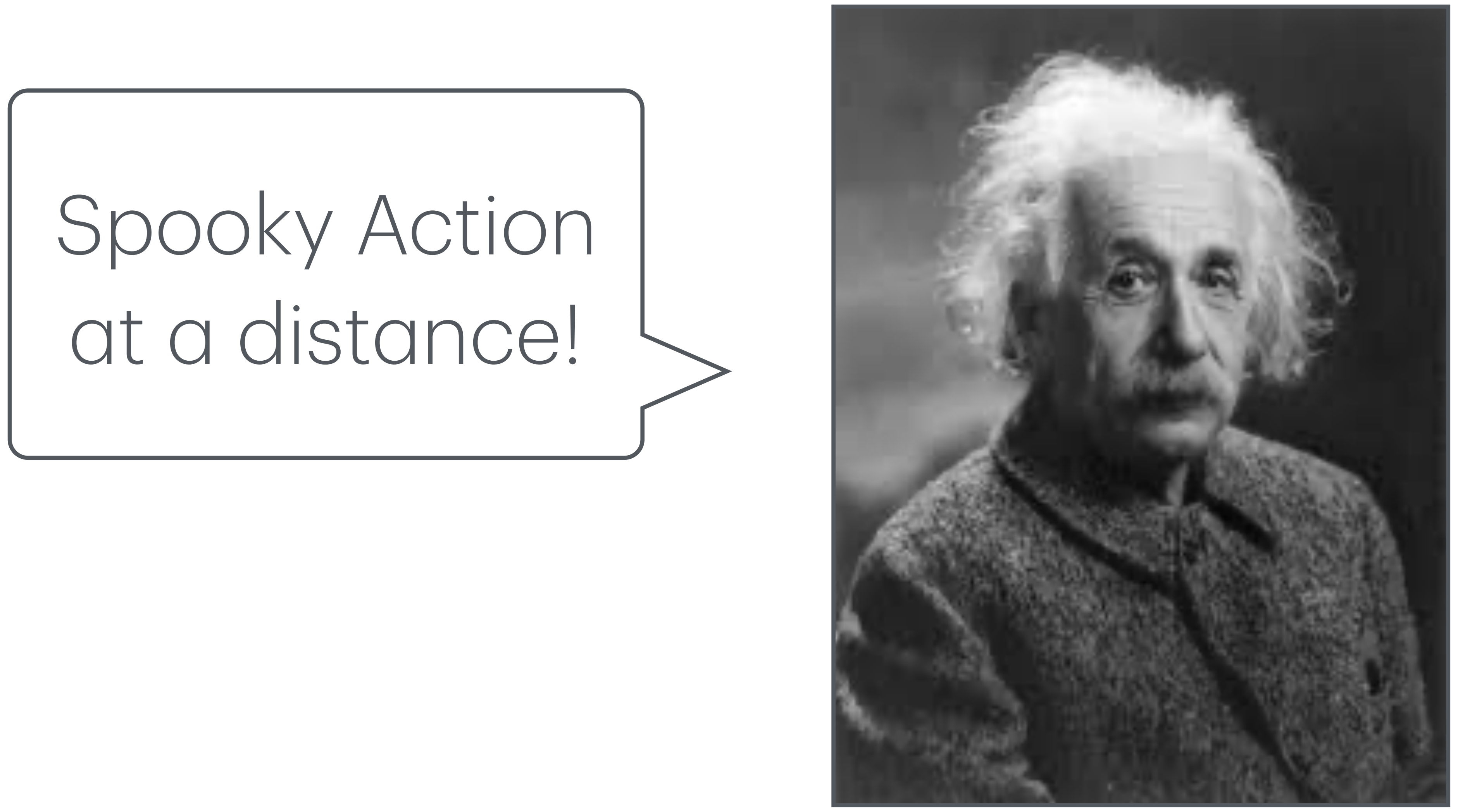
- Measuring the qubits in the computational basis yields:
  - With prob 1/2 Alice obtains 0 and Bob obtains 0
  - With prob 1/2 Alice obtains 1 and Bob obtains 1
- Perfect correlation without communication!

The EPR Paradox

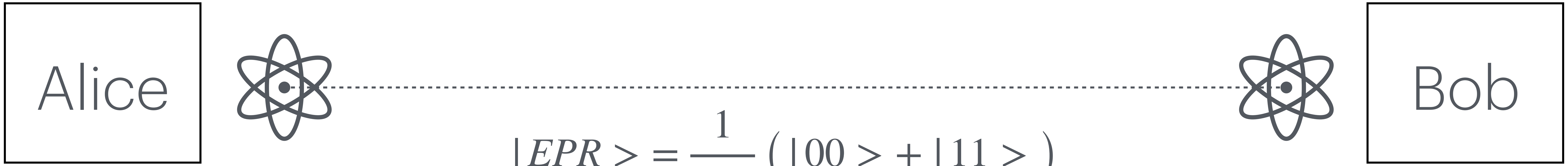


$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

- Measuring the qubits in the computational basis yields:
  - With prob 1/2 Alice obtains 0 and Bob obtains 0
  - With prob 1/2 Alice obtains 1 and Bob obtains 1
- Perfect correlation without communication!

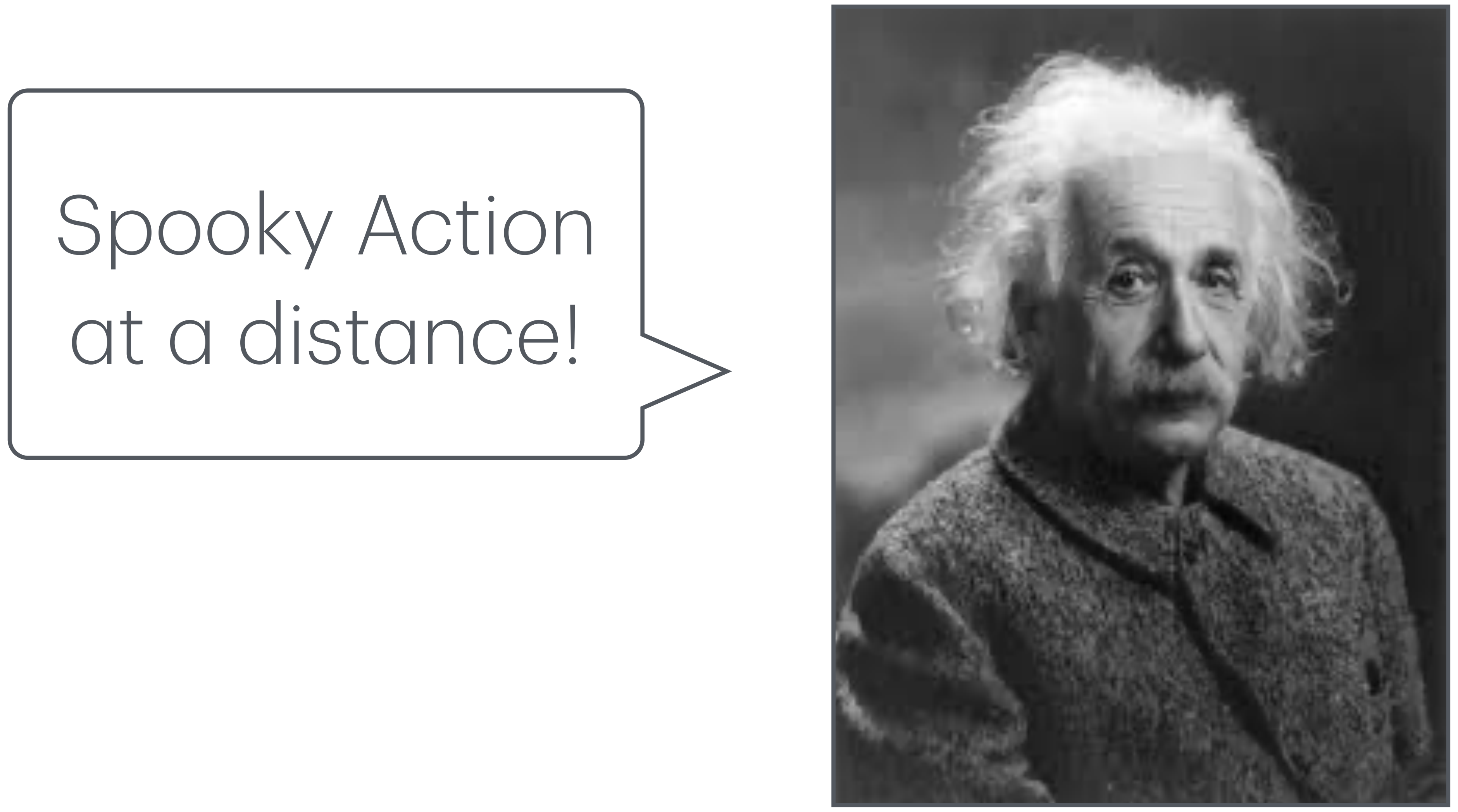


The EPR Paradox

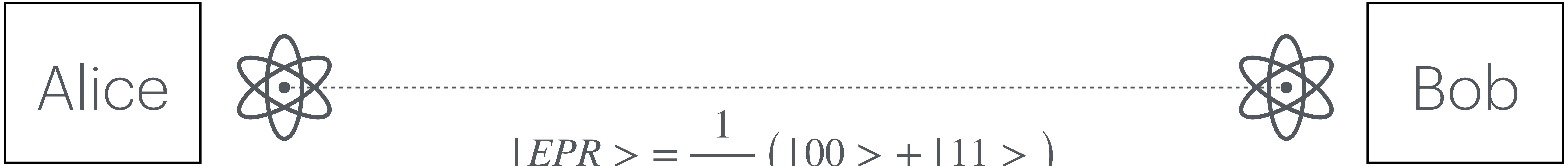


$$|EPR> = \frac{1}{\sqrt{2}} \left(|00> + |11> \right)$$

- Measuring the qubits in the computational basis yields:
  - With prob 1/2 Alice obtains 0 and Bob obtains 0
  - With prob 1/2 Alice obtains 1 and Bob obtains 1
- Perfect correlation without communication!
  - (Cannot be used to transmit information)

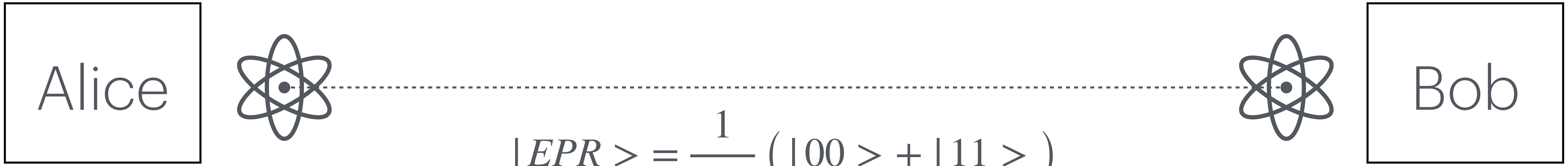


The EPR Paradox



$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

The EPR Paradox



$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

Quantum Mechanics

The EPR Paradox

Alice

Bob

$$|EPR> = \frac{1}{\sqrt{2}} \left(|00> + |11> \right)$$

Quantum Mechanics

Local Hidden Variables

Alice

Bob

00 with prob $1/2$ and 11 with prob $1/2$

The EPR Paradox

Alice

Bob

$$|EPR> = \frac{1}{\sqrt{2}}\left(|00> + |11>\right)$$

Quantum Mechanics

Local Hidden Variables

Alice

Bob

00 with prob $1/2$ and 11 with prob $1/2$

- PROBLEM: The probabilities are identical in both cases!

Testing Quantum Mechanics

Testing Quantum Mechanics

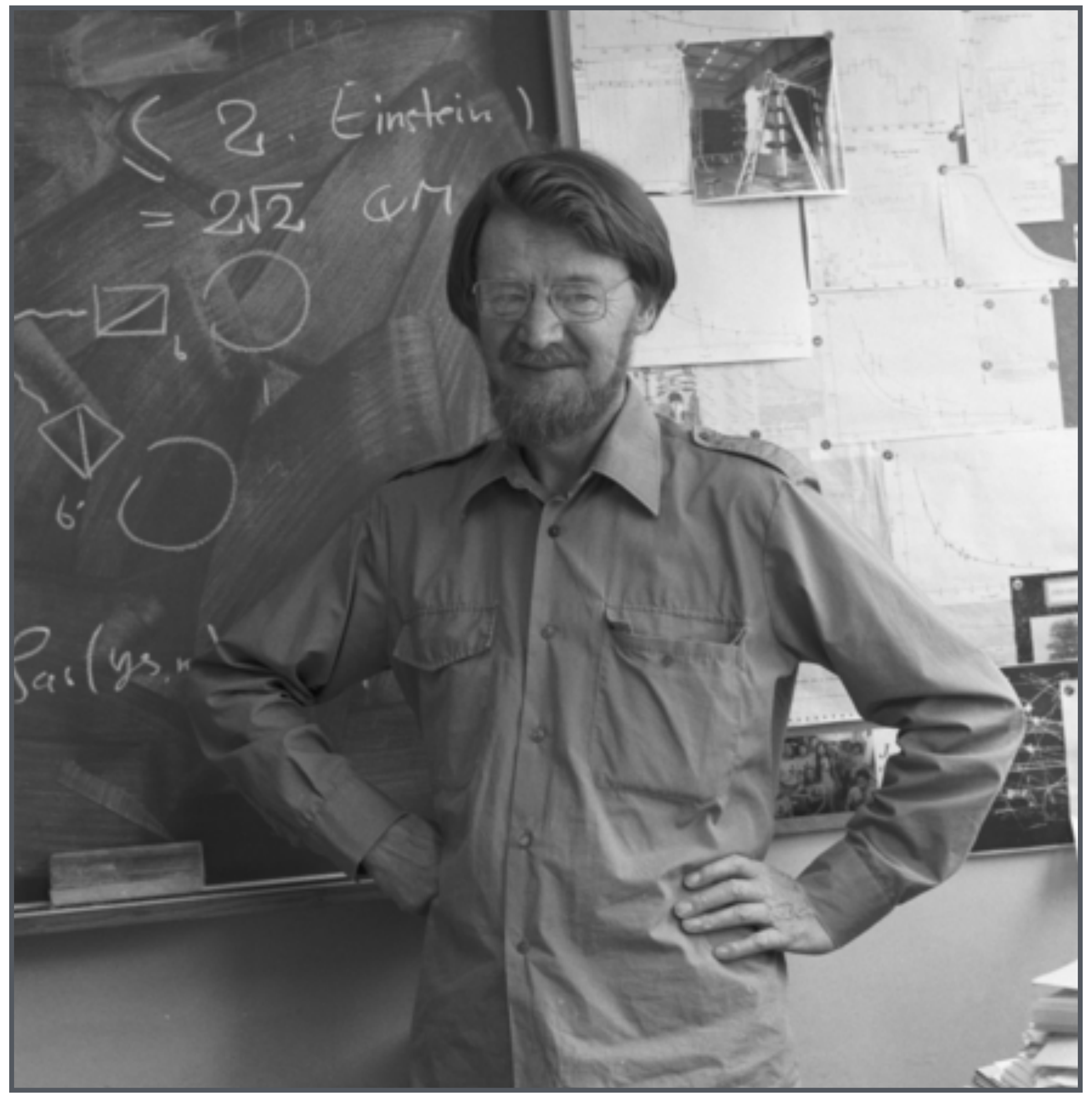
- Turns out, you can actually tell these two scenarios apart!

Testing Quantum Mechanics

- Turns out, you can actually tell these two scenarios apart!
  - The catch is to measure the state in a different basis

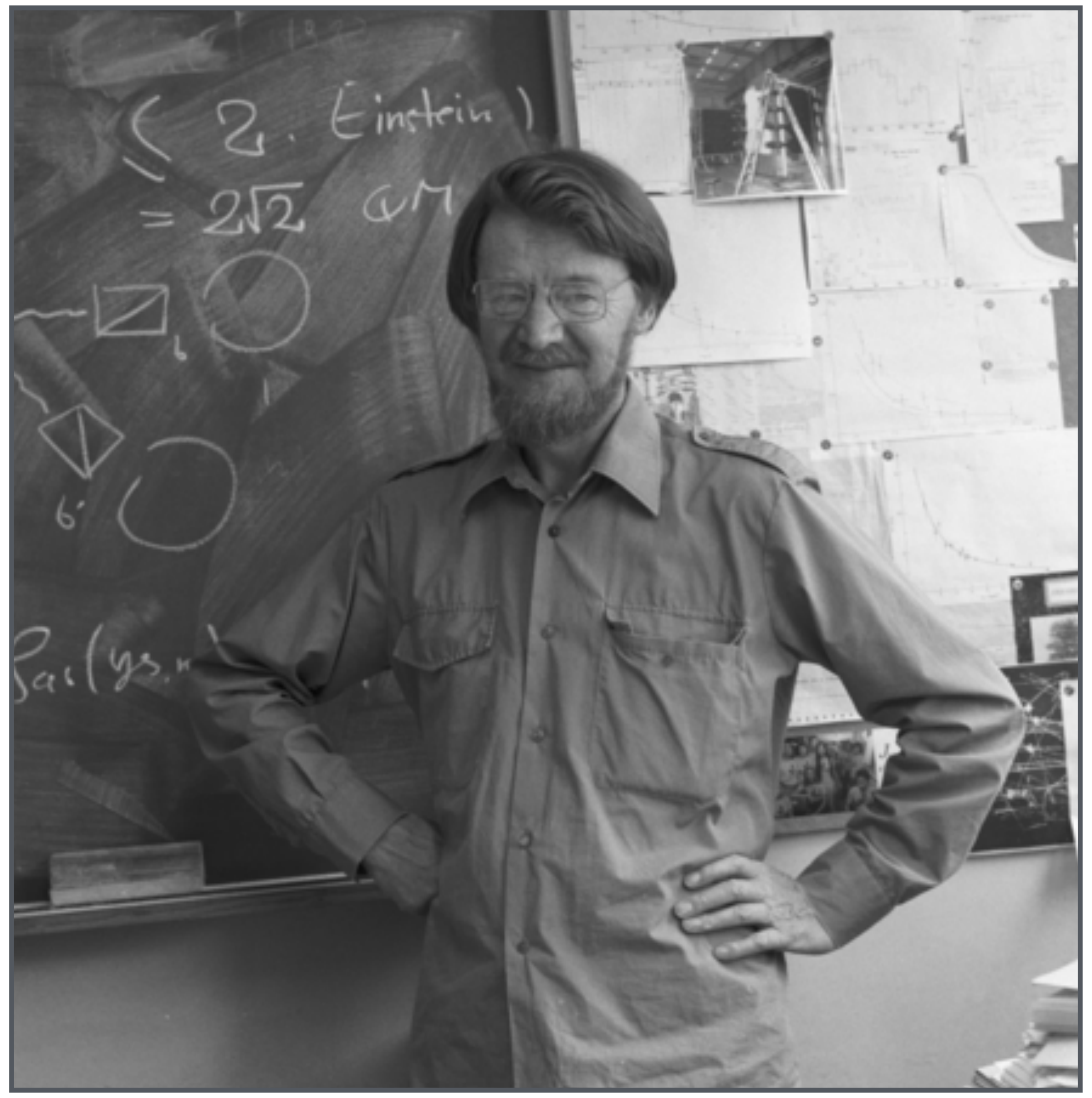
Testing Quantum Mechanics

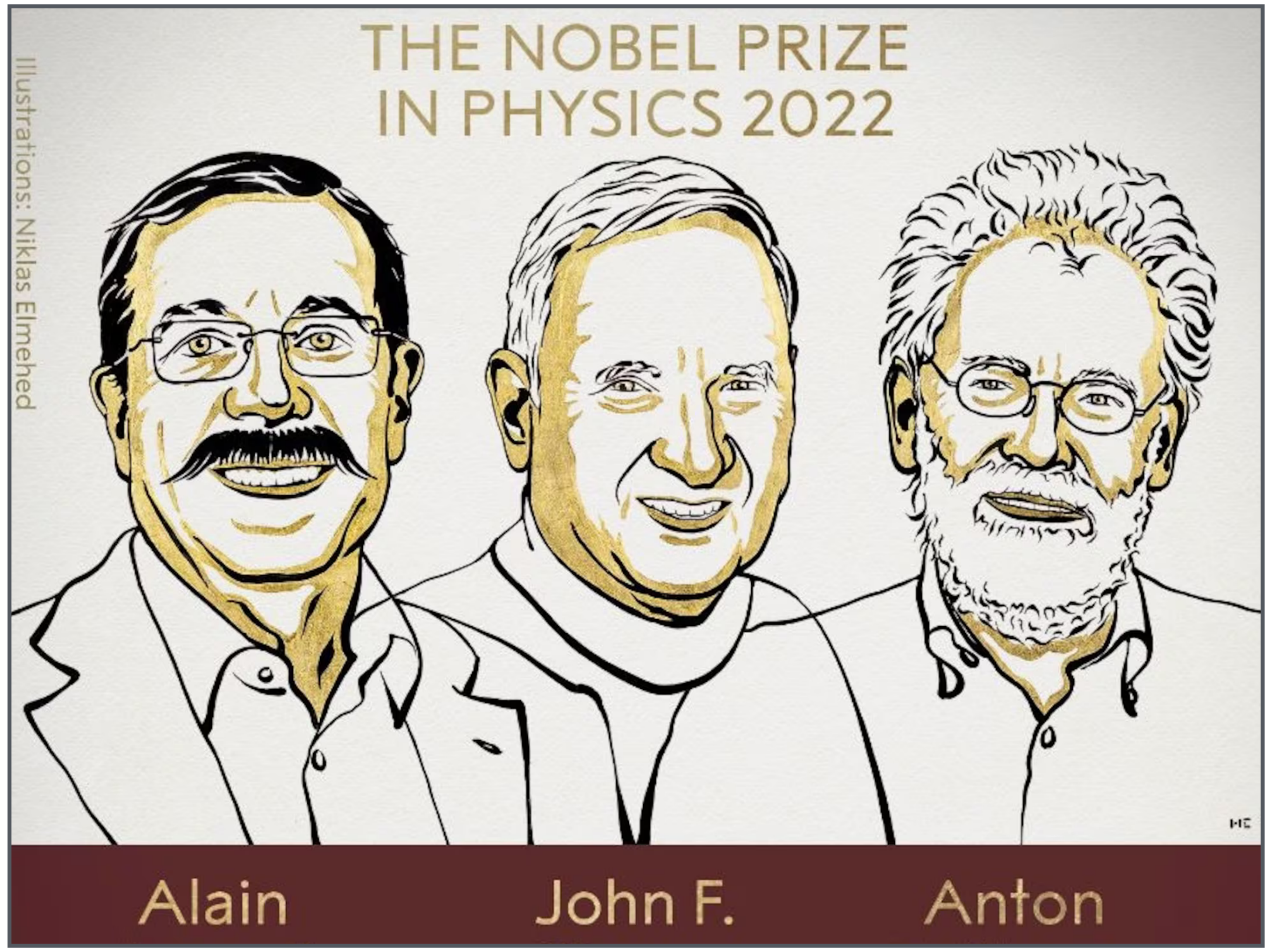
- Turns out, you can actually tell these two scenarios apart!
    - The catch is to measure the state in a different basis



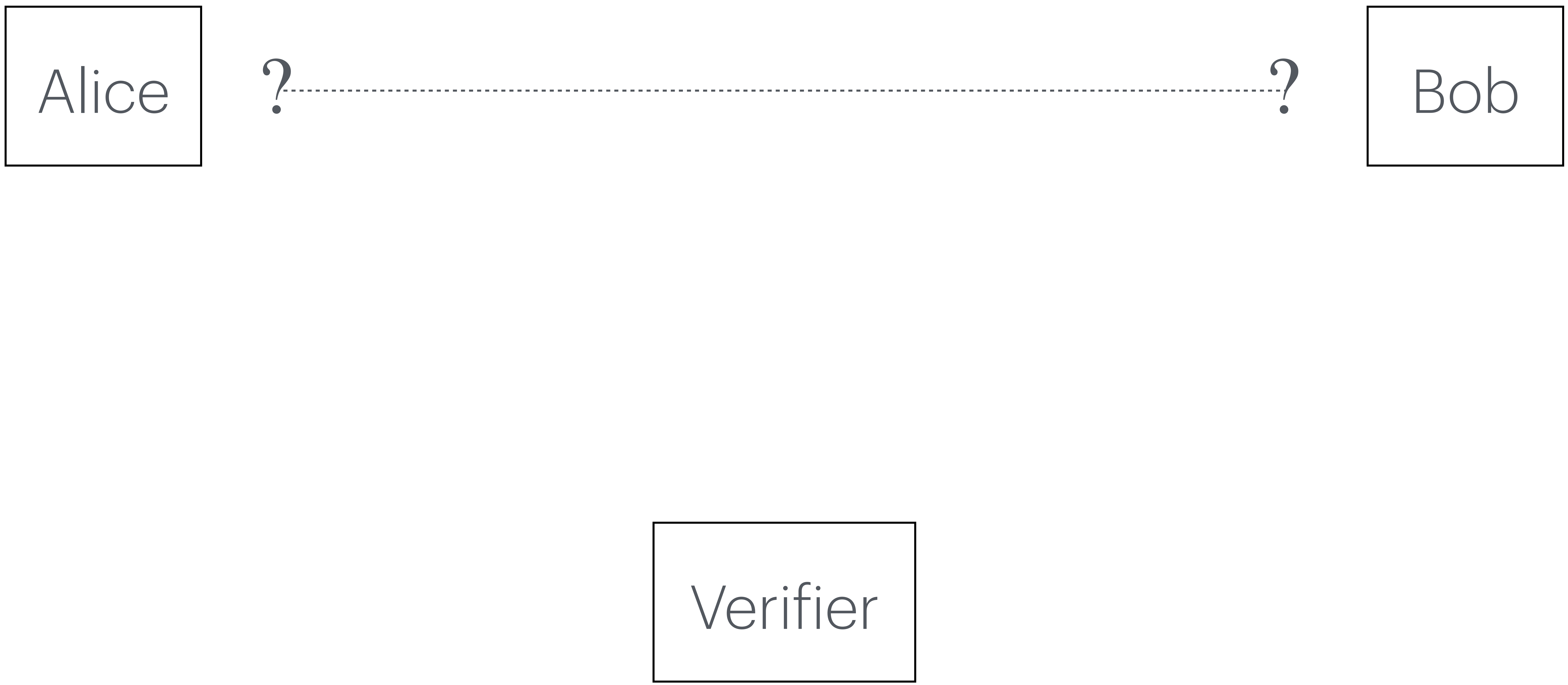
Testing Quantum Mechanics

- Turns out, you can actually tell these two scenarios apart!
  - The catch is to measure the state in a different basis

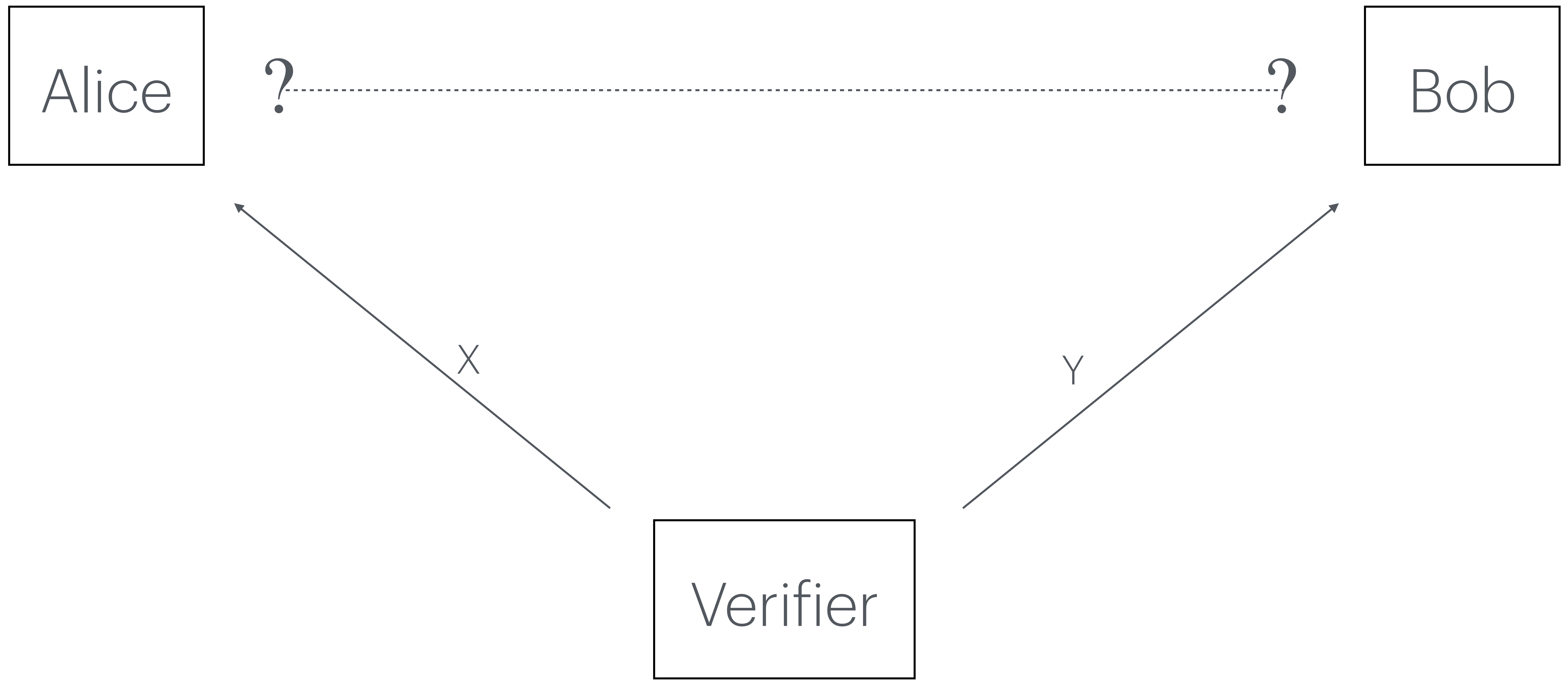




The CHSH Game

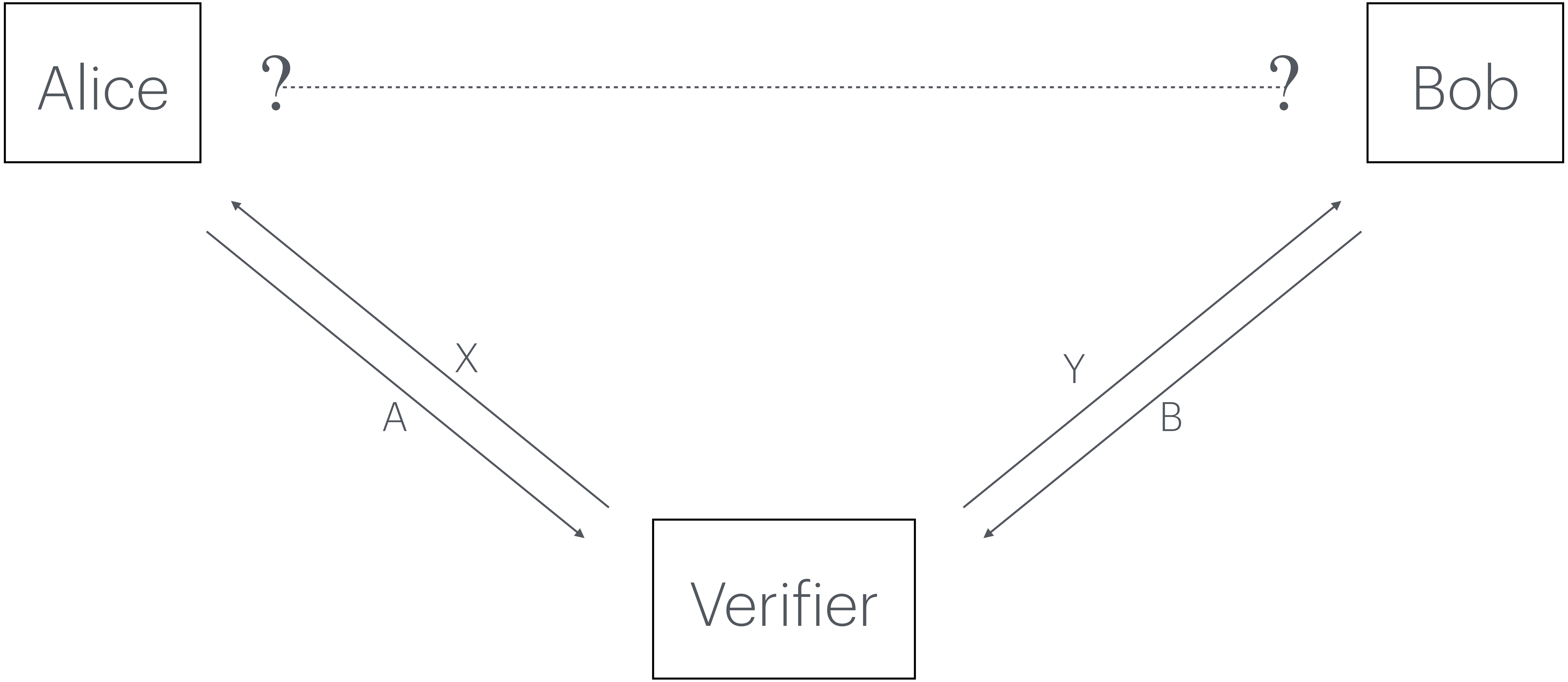


The CHSH Game



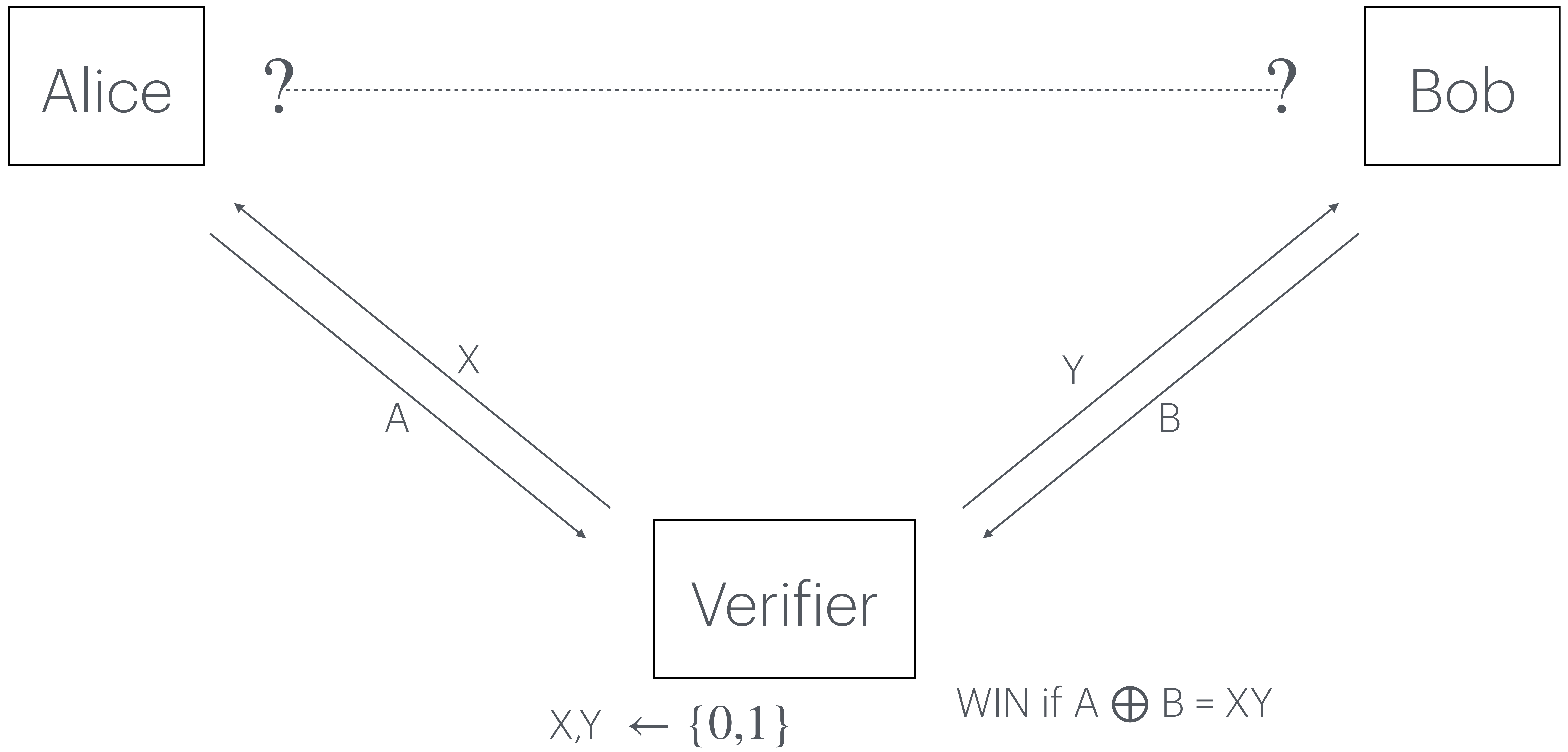
X,Y $\leftarrow \{0,1\}$

The CHSH Game



X,Y $\leftarrow \{0,1\}$

The CHSH Game



The CHSH Game

The CHSH Game

- It can be shown that for any classical strategy (where Alice and Bob share classical random variables) the best success rate is 75%

The CHSH Game

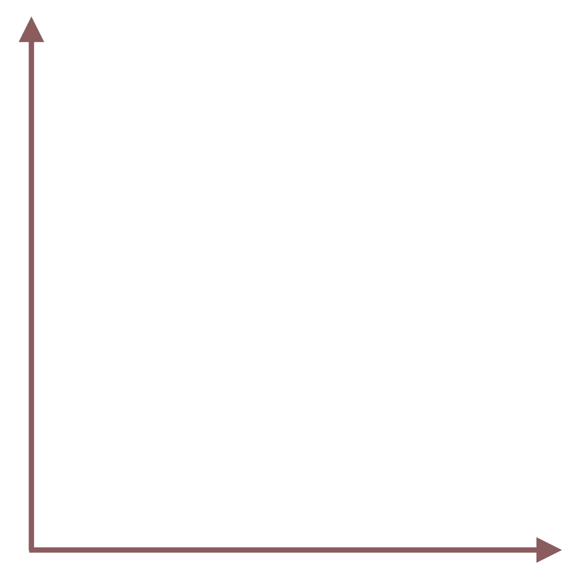
- It can be shown that for any classical strategy (where Alice and Bob share classical random variables) the best success rate is 75%
- On the other hand, if Alice and Bob share an EPR pair, they can win the game ~85% of the times with the following strategy:

The CHSH Game

- It can be shown that for any classical strategy (where Alice and Bob share classical random variables) the best success rate is 75%

- On the other hand, if Alice and Bob share an EPR pair, they can win the game ~85% of the times with the following strategy:

  - If X = 0 Alice measures her qubit in the computational basis



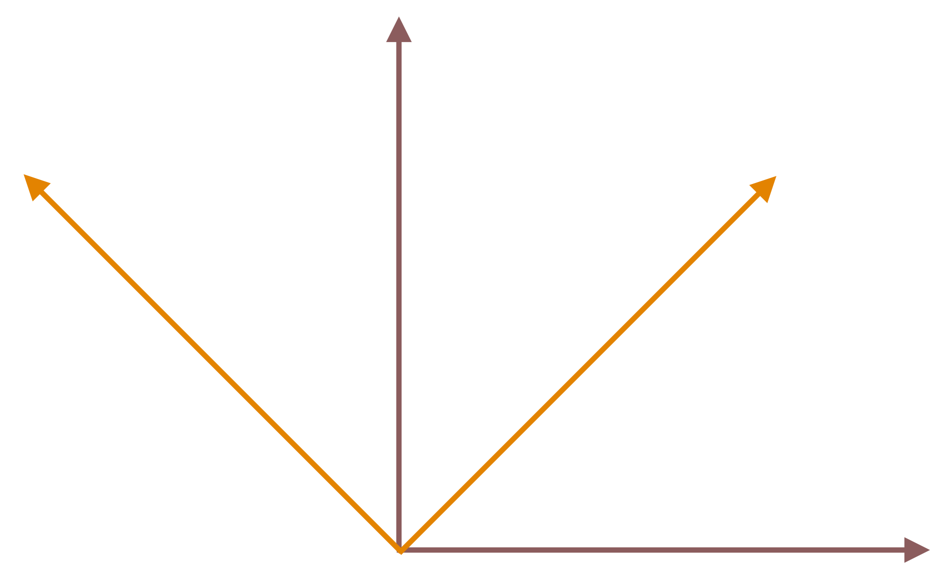
The CHSH Game

- It can be shown that for any classical strategy (where Alice and Bob share classical random variables) the best success rate is 75%

- On the other hand, if Alice and Bob share an EPR pair, they can win the game ~85% of the times with the following strategy:

  - If X = 0 Alice measures her qubit in the computational basis

  - If X = 1 Alice measures her qubit in the $|+>, |->$ basis



The CHSH Game

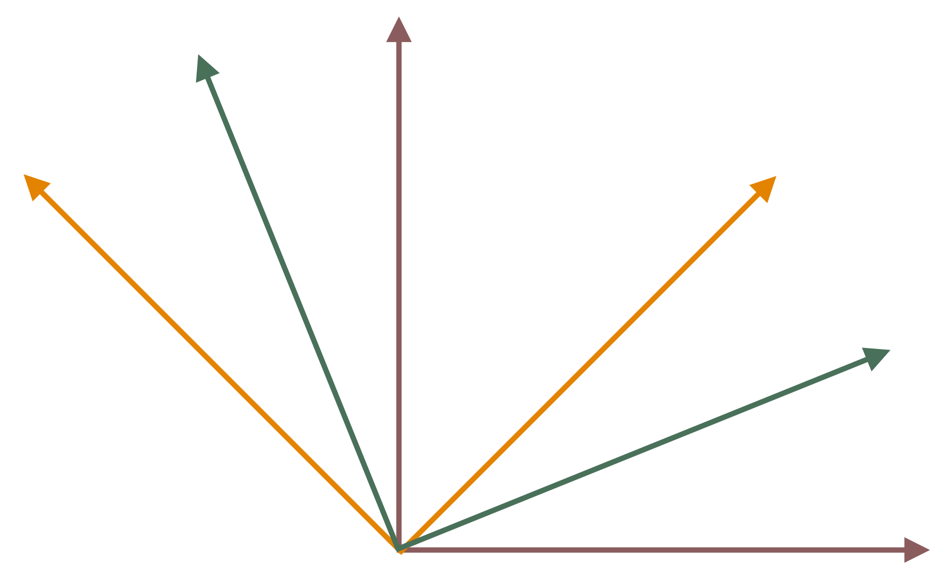
- It can be shown that for any classical strategy (where Alice and Bob share classical random variables) the best success rate is 75%

- On the other hand, if Alice and Bob share an EPR pair, they can win the game ~85% of the times with the following strategy:

  - If X = 0 Alice measures her qubit in the computational basis

  - If X = 1 Alice measures her qubit in the $|+>, |->$ basis

  - If Y = 0 Bob measures his qubit in the comp. basis rotated by $\pi/8$



The CHSH Game

- It can be shown that for any classical strategy (where Alice and Bob share classical random variables) the best success rate is 75%

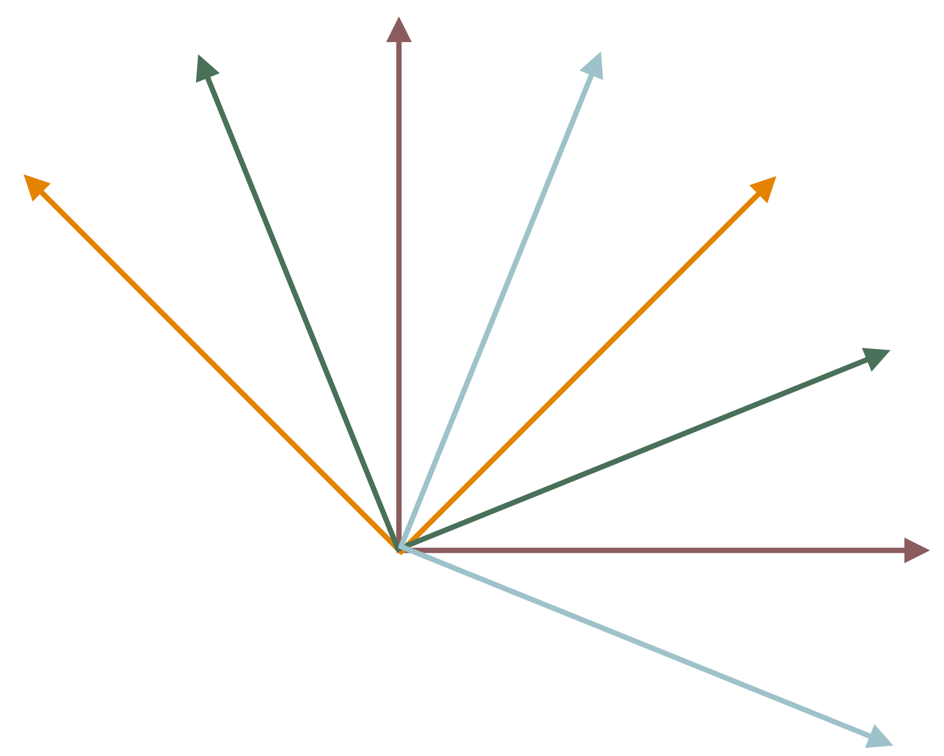
- On the other hand, if Alice and Bob share an EPR pair, they can win the game ~85% of the times with the following strategy:

  - If X = 0 Alice measures her qubit in the computational basis

  - If X = 1 Alice measures her qubit in the $|+>,|->$ basis

  - If Y = 0 Bob measures his qubit in the comp. basis rotated by $\pi/8$

  - If Y = 1 Bob measures his qubit in the comp. basis rotated by $-\pi/8$



Thank you!