

Entanglement and Quantum Information

Stephen A. Fenner¹

¹University of South Carolina
fenner.sa@gmail.com

Graduate Seminar, Fall 2009

Outline

- 1 Classical and quantum information
 - Basics
 - Quantum teleportation

- 2 Quantum channels

Outline

- 1 Classical and quantum information
 - Basics
 - Quantum teleportation
- 2 Quantum channels

One bit and one qubit

A *classical bit* can take on the possible values 0 or 1. That is, the state of the bit at any given time is either 0 or 1.

A *quantum bit* (or *qubit*) can take on the value 0 or 1 or *any linear superposition of these two*.

For $b \in \{0, 1\}$, we write $|b\rangle$ for the bit value b .

The state of a qubit is a vector sum:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where the complex coefficients α and β satisfy

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

α and β are called *probability amplitudes*, and $|\alpha|^2 + |\beta|^2$ is the *norm* of the vector $|\psi\rangle$.

A (pure) quantum state is always a vector of norm 1.

One bit and one qubit

A *classical bit* can take on the possible values 0 or 1. That is, the state of the bit at any given time is either 0 or 1.

A *quantum bit* (or *qubit*) can take on the value 0 or 1 or *any linear superposition of these two*.

For $b \in \{0, 1\}$, we write $|b\rangle$ for the bit value b .

The state of a qubit is a vector sum:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where the complex coefficients α and β satisfy

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

α and β are called *probability amplitudes*, and $|\alpha|^2 + |\beta|^2$ is the *norm* of the vector $|\psi\rangle$.

A (pure) quantum state is always a vector of norm 1.

One bit and one qubit

A *classical bit* can take on the possible values 0 or 1. That is, the state of the bit at any given time is either 0 or 1.

A *quantum bit* (or *qubit*) can take on the value 0 or 1 or *any linear superposition of these two*.

For $b \in \{0, 1\}$, we write $|b\rangle$ for the bit value b .

The state of a qubit is a vector sum:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where the complex coefficients α and β satisfy

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

α and β are called *probability amplitudes*, and $|\alpha|^2 + |\beta|^2$ is the *norm* of the vector $|\psi\rangle$.

A (pure) quantum state is always a vector of norm 1.

One bit and one qubit

A *classical bit* can take on the possible values 0 or 1. That is, the state of the bit at any given time is either 0 or 1.

A *quantum bit* (or *qubit*) can take on the value 0 or 1 or *any linear superposition of these two*.

For $b \in \{0, 1\}$, we write $|b\rangle$ for the bit value b .

The state of a qubit is a vector sum:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where the complex coefficients α and β satisfy

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

α and β are called *probability amplitudes*, and $|\alpha|^2 + |\beta|^2$ is the *norm* of the vector $|\psi\rangle$.

A (pure) quantum state is always a vector of norm 1.

One bit and one qubit

A *classical bit* can take on the possible values 0 or 1. That is, the state of the bit at any given time is either 0 or 1.

A *quantum bit* (or *qubit*) can take on the value 0 or 1 or *any linear superposition of these two*.

For $b \in \{0, 1\}$, we write $|b\rangle$ for the bit value b .

The state of a qubit is a vector sum:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where the complex coefficients α and β satisfy

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

α and β are called *probability amplitudes*, and $|\alpha|^2 + |\beta|^2$ is the *norm* of the vector $|\psi\rangle$.

A (pure) quantum state is always a vector of norm 1.

One bit and one qubit

A *classical bit* can take on the possible values 0 or 1. That is, the state of the bit at any given time is either 0 or 1.

A *quantum bit* (or *qubit*) can take on the value 0 or 1 or *any linear superposition of these two*.

For $b \in \{0, 1\}$, we write $|b\rangle$ for the bit value b .

The state of a qubit is a vector sum:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where the complex coefficients α and β satisfy

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

α and β are called *probability amplitudes*, and $|\alpha|^2 + |\beta|^2$ is the *norm* of the vector $|\psi\rangle$.

A (pure) quantum state is always a vector of norm 1.

Measuring a qubit

We can measure the bit value of a qubit in state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

We get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.

After the measurement, the state of the qubit *collapses* to the state reflecting the result of the measurement.

For example, if the result of the measurement is 1, then the state changes to $|1\rangle$.

A subsequent measurement will yield the same value with certainty.

Measuring a qubit

We can measure the bit value of a qubit in state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

We get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.
After the measurement, the state of the qubit *collapses* to the state reflecting the result of the measurement.

For example, if the result of the measurement is 1, then the state changes to $|1\rangle$.

A subsequent measurement will yield the same value with certainty.

Measuring a qubit

We can measure the bit value of a qubit in state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

We get 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.
After the measurement, the state of the qubit *collapses* to the state reflecting the result of the measurement.

For example, if the result of the measurement is 1, then the state changes to $|1\rangle$.

A subsequent measurement will yield the same value with certainty.

Transforming a qubit

One can act on a qubit without measuring it.

A *single-qubit quantum gate* is any linear transformation G that preserves the norm:

$$G : \alpha|0\rangle + \beta|1\rangle \mapsto \gamma|0\rangle + \delta|1\rangle$$

so that $|\gamma|^2 + |\delta|^2 = 1$.

Since G is linear, we only need to give $G|0\rangle$ and $G|1\rangle$ to specify G completely.

Transforming a qubit

One can act on a qubit without measuring it.

A *single-qubit quantum gate* is any linear transformation G that preserves the norm:

$$G : \alpha|0\rangle + \beta|1\rangle \mapsto \gamma|0\rangle + \delta|1\rangle$$

so that $|\gamma|^2 + |\delta|^2 = 1$.

Since G is linear, we only need to give $G|0\rangle$ and $G|1\rangle$ to specify G completely.

Transforming a qubit

One can act on a qubit without measuring it.

A *single-qubit quantum gate* is any linear transformation G that preserves the norm:

$$G : \alpha|0\rangle + \beta|1\rangle \mapsto \gamma|0\rangle + \delta|1\rangle$$

so that $|\gamma|^2 + |\delta|^2 = 1$.

Since G is linear, we only need to give $G|0\rangle$ and $G|1\rangle$ to specify G completely.

The X and Z gates

The X gate flips the value of the bit:

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

In general,

$$X : \alpha|0\rangle + \beta|1\rangle \mapsto \beta|0\rangle + \alpha|1\rangle.$$

X is the *bit-flip* gate (classically, the NOT gate).

The Z gate has no classical analogue:

$$\begin{aligned}Z|0\rangle &= |0\rangle, \\Z|1\rangle &= -|1\rangle.\end{aligned}$$

In general,

$$Z : \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle - \beta|1\rangle.$$

Z is the *phase-flip* gate.

The X and Z gates

The X *gate* flips the value of the bit:

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

In general,

$$X : \alpha|0\rangle + \beta|1\rangle \mapsto \beta|0\rangle + \alpha|1\rangle.$$

X is the *bit-flip* gate (classically, the NOT gate).

The Z *gate* has no classical analogue:

$$\begin{aligned}Z|0\rangle &= |0\rangle, \\Z|1\rangle &= -|1\rangle.\end{aligned}$$

In general,

$$Z : \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle - \beta|1\rangle.$$

Z is the *phase-flip* gate.

The X and Z gates

The X gate flips the value of the bit:

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

$$X|1\rangle = |0\rangle.$$

In general,

$$X : \alpha|0\rangle + \beta|1\rangle \mapsto \beta|0\rangle + \alpha|1\rangle.$$

X is the *bit-flip* gate (classically, the NOT gate).

The Z gate has no classical analogue:

$$Z|0\rangle = |0\rangle,$$

$$Z|1\rangle = -|1\rangle.$$

In general,

$$Z : \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle - \beta|1\rangle.$$

Z is the *phase-flip* gate.

The X and Z gates

The X gate flips the value of the bit:

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

In general,

$$X : \alpha|0\rangle + \beta|1\rangle \mapsto \beta|0\rangle + \alpha|1\rangle.$$

X is the *bit-flip* gate (classically, the NOT gate).

The Z gate has no classical analogue:

$$\begin{aligned}Z|0\rangle &= |0\rangle, \\Z|1\rangle &= -|1\rangle.\end{aligned}$$

In general,

$$Z : \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle - \beta|1\rangle.$$

Z is the *phase-flip* gate.

The X and Z gates

The X gate flips the value of the bit:

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

In general,

$$X : \alpha|0\rangle + \beta|1\rangle \mapsto \beta|0\rangle + \alpha|1\rangle.$$

X is the *bit-flip* gate (classically, the NOT gate).

The Z gate has no classical analogue:

$$\begin{aligned}Z|0\rangle &= |0\rangle, \\Z|1\rangle &= -|1\rangle.\end{aligned}$$

In general,

$$Z : \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle - \beta|1\rangle.$$

Z is the *phase-flip* gate.

Implementing a qubit

Qubits can be implemented any number of ways:

- Electron spin: $|0\rangle = |\uparrow\rangle = |\text{spin-up}\rangle$;
 $|1\rangle = |\downarrow\rangle = |\text{spin-down}\rangle$.
- Photon polarization: $|0\rangle = |\leftrightarrow\rangle = |\text{horizontal}\rangle$;
 $|1\rangle = |\updownarrow\rangle = |\text{vertical}\rangle$.
- Nuclear spin
- Vibrational modes of a trapped ion
- Position of a particle in a quantum dot
- etc.

Implementing a qubit

Qubits can be implemented any number of ways:

- Electron spin: $|0\rangle = |\uparrow\rangle = |\text{spin-up}\rangle$;
 $|1\rangle = |\downarrow\rangle = |\text{spin-down}\rangle$.
- Photon polarization: $|0\rangle = |\leftrightarrow\rangle = |\text{horizontal}\rangle$;
 $|1\rangle = |\updownarrow\rangle = |\text{vertical}\rangle$.
- Nuclear spin
- Vibrational modes of a trapped ion
- Position of a particle in a quantum dot
- etc.

Implementing a qubit

Qubits can be implemented any number of ways:

- Electron spin: $|0\rangle = |\uparrow\rangle = |\text{spin-up}\rangle$;
 $|1\rangle = |\downarrow\rangle = |\text{spin-down}\rangle$.
- Photon polarization: $|0\rangle = |\leftrightarrow\rangle = |\text{horizontal}\rangle$;
 $|1\rangle = |\updownarrow\rangle = |\text{vertical}\rangle$.
- Nuclear spin
- Vibrational modes of a trapped ion
- Position of a particle in a quantum dot
- etc.

Implementing a qubit

Qubits can be implemented any number of ways:

- Electron spin: $|0\rangle = |\uparrow\rangle = |\text{spin-up}\rangle$;
 $|1\rangle = |\downarrow\rangle = |\text{spin-down}\rangle$.
- Photon polarization: $|0\rangle = |\leftrightarrow\rangle = |\text{horizontal}\rangle$;
 $|1\rangle = |\updownarrow\rangle = |\text{vertical}\rangle$.
- Nuclear spin
- Vibrational modes of a trapped ion
- Position of a particle in a quantum dot
- etc.

Implementing a qubit

Qubits can be implemented any number of ways:

- Electron spin: $|0\rangle = |\uparrow\rangle = |\text{spin-up}\rangle$;
 $|1\rangle = |\downarrow\rangle = |\text{spin-down}\rangle$.
- Photon polarization: $|0\rangle = |\leftrightarrow\rangle = |\text{horizontal}\rangle$;
 $|1\rangle = |\updownarrow\rangle = |\text{vertical}\rangle$.
- Nuclear spin
- Vibrational modes of a trapped ion
- Position of a particle in a quantum dot
- etc.

Implementing a qubit

Qubits can be implemented any number of ways:

- Electron spin: $|0\rangle = |\uparrow\rangle = |\text{spin-up}\rangle$;
 $|1\rangle = |\downarrow\rangle = |\text{spin-down}\rangle$.
- Photon polarization: $|0\rangle = |\leftrightarrow\rangle = |\text{horizontal}\rangle$;
 $|1\rangle = |\updownarrow\rangle = |\text{vertical}\rangle$.
- Nuclear spin
- Vibrational modes of a trapped ion
- Position of a particle in a quantum dot
- etc.

Implementing a qubit

Qubits can be implemented any number of ways:

- Electron spin: $|0\rangle = |\uparrow\rangle = |\text{spin-up}\rangle$;
 $|1\rangle = |\downarrow\rangle = |\text{spin-down}\rangle$.
- Photon polarization: $|0\rangle = |\leftrightarrow\rangle = |\text{horizontal}\rangle$;
 $|1\rangle = |\updownarrow\rangle = |\text{vertical}\rangle$.
- Nuclear spin
- Vibrational modes of a trapped ion
- Position of a particle in a quantum dot
- etc.

Two qubits

Classically, a pair of bits can be in any of four possible combinations: 00, 01, 10, 11.

Quantally, a pair of qubits can be in any linear superposition of these four possibilities:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

such that

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

Two qubits

Classically, a pair of bits can be in any of four possible combinations: 00, 01, 10, 11.

Quantally, a pair of qubits can be in any linear superposition of these four possibilities:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

such that

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

Two qubits

Classically, a pair of bits can be in any of four possible combinations: 00, 01, 10, 11.

Quantally, a pair of qubits can be in any linear superposition of these four possibilities:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

such that

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

For example, if Alice's qubit is in the state

$$|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2},$$

and Bob's qubit is in the state

$$|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2},$$

then the pair is in the state

$$|+\rangle|-\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

This is an example of a *product state*.

For example, if Alice's qubit is in the state

$$|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2},$$

and Bob's qubit is in the state

$$|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2},$$

then the pair is in the state

$$|+\rangle|-\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

This is an example of a *product state*.

For example, if Alice's qubit is in the state

$$|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2},$$

and Bob's qubit is in the state

$$|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2},$$

then the pair is in the state

$$|+\rangle|-\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

This is an example of a *product state*.

Entanglement

Some 2-qubit states are *not* product states.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

cannot be written as the product of two single-qubit states.

In this case, we say that the two qubits are *entangled*.

If Alice and Bob each measure their respective qubits in this state, then each will get 0 or 1 with equal probability, but . . . the results will always be *equal* (perfectly correlated).

Entanglement

Some 2-qubit states are *not* product states.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

cannot be written as the product of two single-qubit states.

In this case, we say that the two qubits are *entangled*.

If Alice and Bob each measure their respective qubits in this state, then each will get 0 or 1 with equal probability, but ... the results will always be *equal* (perfectly correlated).

Entanglement

Some 2-qubit states are *not* product states.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

cannot be written as the product of two single-qubit states. In this case, we say that the two qubits are *entangled*. If Alice and Bob each measure their respective qubits in this state, then each will get 0 or 1 with equal probability, but . . . the results will always be *equal* (perfectly correlated).

Entanglement

Some 2-qubit states are *not* product states.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

cannot be written as the product of two single-qubit states. In this case, we say that the two qubits are *entangled*. If Alice and Bob each measure their respective qubits in this state, then each will get 0 or 1 with equal probability, but . . . the results will always be *equal* (perfectly correlated).

The EPR paradox

Einstein, Podolski, and Rosen (EPR) used entanglement to try to disprove quantum mechanics by arguing that entanglement is impossible. (“Spooky action at a distance.”)

Later, Bell suggested an experiment to test the presence of entanglement. (It has been confirmed repeatedly.)

The state $|\Phi^+\rangle$ is called an *EPR pair*. It is also one of four possible *Bell states*:

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2},$$

$$|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2},$$

$$|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2},$$

$$|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}.$$

The EPR paradox

Einstein, Podolski, and Rosen (EPR) used entanglement to try to disprove quantum mechanics by arguing that entanglement is impossible. (“Spooky action at a distance.”)

Later, Bell suggested an experiment to test the presence of entanglement. (It has been confirmed repeatedly.)

The state $|\Phi^+\rangle$ is called an *EPR pair*. It is also one of four possible *Bell states*:

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2},$$

$$|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2},$$

$$|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2},$$

$$|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}.$$

The EPR paradox

Einstein, Podolski, and Rosen (EPR) used entanglement to try to disprove quantum mechanics by arguing that entanglement is impossible. (“Spooky action at a distance.”)

Later, Bell suggested an experiment to test the presence of entanglement. (It has been confirmed repeatedly.)

The state $|\Phi^+\rangle$ is called an *EPR pair*. It is also one of four possible *Bell states*:

$$|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2},$$

$$|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2},$$

$$|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2},$$

$$|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}.$$

Uses of entanglement

Entanglement is useful in quantum information.

- Quantum secret sharing
- Quantum teleportation
- Collaborative quantum games
- Superadditivity of quantum channel capacity

Uses of entanglement

Entanglement is useful in quantum information.

- Quantum secret sharing
- Quantum teleportation
- Collaborative quantum games
- Superadditivity of quantum channel capacity

Uses of entanglement

Entanglement is useful in quantum information.

- Quantum secret sharing
- **Quantum teleportation**
- Collaborative quantum games
- Superadditivity of quantum channel capacity

Uses of entanglement

Entanglement is useful in quantum information.

- Quantum secret sharing
- **Quantum teleportation**
- Collaborative quantum games
- Superadditivity of quantum channel capacity

Uses of entanglement

Entanglement is useful in quantum information.

- Quantum secret sharing
- **Quantum teleportation**
- Collaborative quantum games
- **Superadditivity of quantum channel capacity**

Outline

- 1 Classical and quantum information
 - Basics
 - Quantum teleportation
- 2 Quantum channels

Quantum teleportation

Alice has some a quantum state $|\psi\rangle$, which she wants to send to Bob.

But she can only communicate with Bob classically (e.g., over the phone).

Worse, Alice does not necessarily know what $|\psi\rangle$ is.
A long time ago, Alice and Bob shared an EPR pair

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

Alice keeping the first bit and Bob the second.

Alice can now send $|p\rangle$ to Bob, consuming the EPR pair in the process.

Quantum teleportation

Alice has some a quantum state $|\psi\rangle$, which she wants to send to Bob.

But she can only communicate with Bob classically (e.g., over the phone).

Worse, Alice does not necessarily know what $|\psi\rangle$ is.
A long time ago, Alice and Bob shared an EPR pair

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

Alice keeping the first bit and Bob the second.

Alice can now send $|p\rangle$ to Bob, consuming the EPR pair in the process.

Quantum teleportation

Alice has some a quantum state $|\psi\rangle$, which she wants to send to Bob.

But she can only communicate with Bob classically (e.g., over the phone).

Worse, Alice does not necessarily know what $|\psi\rangle$ is.

A long time ago, Alice and Bob shared an EPR pair

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

Alice keeping the first bit and Bob the second.

Alice can now send $|p\rangle$ to Bob, consuming the EPR pair in the process.

Quantum teleportation

Alice has some a quantum state $|\psi\rangle$, which she wants to send to Bob.

But she can only communicate with Bob classically (e.g., over the phone).

Worse, Alice does not necessarily know what $|\psi\rangle$ is.

A long time ago, Alice and Bob shared an EPR pair

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

Alice keeping the first bit and Bob the second.

Alice can now send $|p\rangle$ to Bob, consuming the EPR pair in the process.

Quantum teleportation

Alice has some a quantum state $|\psi\rangle$, which she wants to send to Bob.

But she can only communicate with Bob classically (e.g., over the phone).

Worse, Alice does not necessarily know what $|\psi\rangle$ is.

A long time ago, Alice and Bob shared an EPR pair

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

Alice keeping the first bit and Bob the second.

Alice can now send $|p\rangle$ to Bob, consuming the EPR pair in the process.

The teleportation protocol

The 3-qubit system:

- 1 Alice's state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to send to Bob,
- 2 Alice's share of the EPR pair $|\Phi^+\rangle$,
- 3 Bob's share of the EPR pair $|\Phi^+\rangle$.

Step 1 (Alice) Alice applies to her two qubits the transformation B^* :

$$\begin{aligned} |\Phi^+\rangle &\mapsto |00\rangle, \\ |\Phi^-\rangle &\mapsto |01\rangle, \\ |\Psi^+\rangle &\mapsto |10\rangle, \\ |\Psi^-\rangle &\mapsto |11\rangle. \end{aligned}$$

This is a norm-preserving map.

Step 2 (Alice) Alice measures the values of her two qubits, giving the four possible combinations 00, 01, 10, 11 (with equal probability).

The teleportation protocol

The 3-qubit system:

- 1 Alice's state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to send to Bob,
- 2 Alice's share of the EPR pair $|\Phi^+\rangle$,
- 3 Bob's share of the EPR pair $|\Phi^+\rangle$.

Step 1 (Alice) Alice applies to her two qubits the transformation B^* :

$$|\Phi^+\rangle \mapsto |00\rangle,$$

$$|\Phi^-\rangle \mapsto |01\rangle,$$

$$|\Psi^+\rangle \mapsto |10\rangle,$$

$$|\Psi^-\rangle \mapsto |11\rangle.$$

This is a norm-preserving map.

Step 2 (Alice) Alice measures the values of her two qubits, giving the four possible combinations 00, 01, 10, 11 (with equal probability).

The teleportation protocol

The 3-qubit system:

- 1 Alice's state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to send to Bob,
- 2 Alice's share of the EPR pair $|\Phi^+\rangle$,
- 3 Bob's share of the EPR pair $|\Phi^+\rangle$.

Step 1 (Alice) Alice applies to her two qubits the transformation B^* :

$$|\Phi^+\rangle \mapsto |00\rangle,$$

$$|\Phi^-\rangle \mapsto |01\rangle,$$

$$|\Psi^+\rangle \mapsto |10\rangle,$$

$$|\Psi^-\rangle \mapsto |11\rangle.$$

This is a norm-preserving map.

Step 2 (Alice) Alice measures the values of her two qubits, giving the four possible combinations 00, 01, 10, 11 (with equal probability).

The protocol (cont.)

- Step 2 (Alice)** Alice measures the values of her two qubits, giving the four possible combinations 00, 01, 10, 11 (with equal probability).
- Step 3 (Alice & Bob) Alice tells Bob (over the phone) what her two measurement results were.
- Step 4 (Bob) If the second value was 1, then Bob applies X to his qubit (otherwise Bob does nothing).
- Step 5 (Bob) If the first value was 1, then Bob applies Z to his qubit (otherwise Bob does nothing).

The protocol (cont.)

- Step 2 (Alice)** Alice measures the values of her two qubits, giving the four possible combinations 00, 01, 10, 11 (with equal probability).
- Step 3 (Alice & Bob)** Alice tells Bob (over the phone) what her two measurement results were.
- Step 4 (Bob)** If the second value was 1, then Bob applies X to his qubit (otherwise Bob does nothing).
- Step 5 (Bob)** If the first value was 1, then Bob applies Z to his qubit (otherwise Bob does nothing).

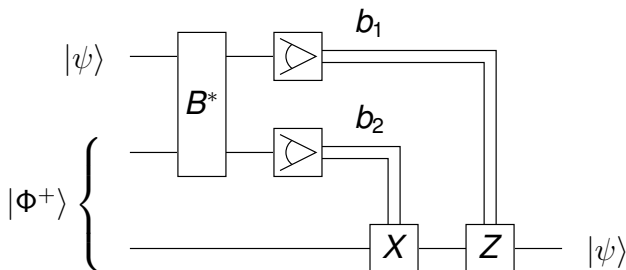
The protocol (cont.)

- Step 2 (Alice)** Alice measures the values of her two qubits, giving the four possible combinations 00, 01, 10, 11 (with equal probability).
- Step 3 (Alice & Bob)** Alice tells Bob (over the phone) what her two measurement results were.
- Step 4 (Bob)** If the second value was 1, then Bob applies X to his qubit (otherwise Bob does nothing).
- Step 5 (Bob)** If the first value was 1, then Bob applies Z to his qubit (otherwise Bob does nothing).

The protocol (cont.)

- Step 2 (Alice)** Alice measures the values of her two qubits, giving the four possible combinations 00, 01, 10, 11 (with equal probability).
- Step 3 (Alice & Bob)** Alice tells Bob (over the phone) what her two measurement results were.
- Step 4 (Bob)** If the second value was 1, then Bob applies X to his qubit (otherwise Bob does nothing).
- Step 5 (Bob)** If the first value was 1, then Bob applies Z to his qubit (otherwise Bob does nothing).

The protocol (cont.)

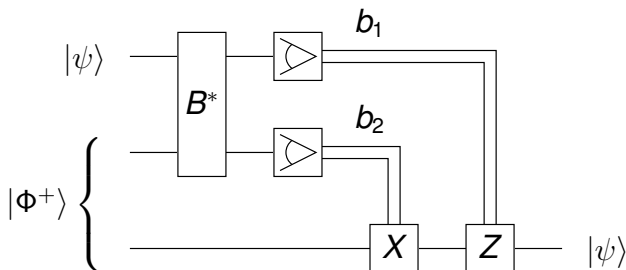


Afterwards, Bob's qubit is in state $|\psi\rangle$.

Alice's copy of $|\psi\rangle$ is destroyed. (Quantum states cannot be cloned!)

The entanglement is consumed.

The protocol (cont.)

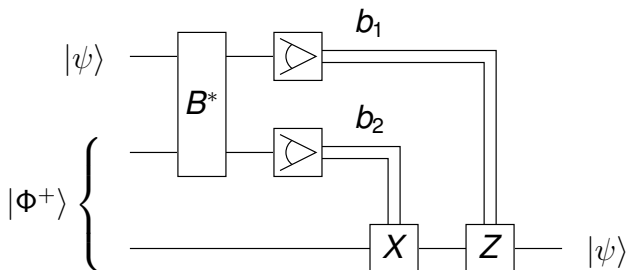


Afterwards, Bob's qubit is in state $|\psi\rangle$.

Alice's copy of $|\psi\rangle$ is destroyed. (Quantum states cannot be cloned!)

The entanglement is consumed.

The protocol (cont.)

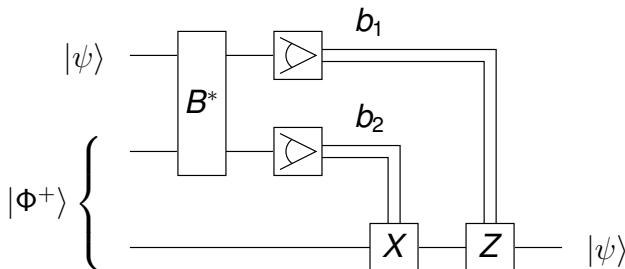


Afterwards, Bob's qubit is in state $|\psi\rangle$.

Alice's copy of $|\psi\rangle$ is destroyed. (Quantum states cannot be cloned!)

The entanglement is consumed.

The protocol (cont.)



Afterwards, Bob's qubit is in state $|\psi\rangle$.

Alice's copy of $|\psi\rangle$ is destroyed. (Quantum states cannot be cloned!)

The entanglement is consumed.

Quantum states as operators

Definition

For any matrix A with complex entries, define A^* to be the conjugate transpose of A (replace each entry with its complex conjugate, then take the transpose). A^* is called the *adjoint* of A .

Think of $|\psi\rangle$ as a column vector ($n \times 1$ matrix). Its adjoint is a row vector denoted by $\langle\psi|$.

Then the matrix product $\rho = |\psi\rangle\langle\psi|$ is an $n \times n$ matrix (operator) which we use to denote the state (rather than $|\psi\rangle$ itself).

This is a *pure state*, *i.e.*, it is completely described.

Quantum states as operators

Definition

For any matrix A with complex entries, define A^* to be the conjugate transpose of A (replace each entry with its complex conjugate, then take the transpose). A^* is called the *adjoint* of A .

Think of $|\psi\rangle$ as a column vector ($n \times 1$ matrix). Its adjoint is a row vector denoted by $\langle\psi|$.

Then the matrix product $\rho = |\psi\rangle\langle\psi|$ is an $n \times n$ matrix (operator) which we use to denote the state (rather than $|\psi\rangle$ itself).

This is a *pure state*, *i.e.*, it is completely described.

Quantum states as operators

Definition

For any matrix A with complex entries, define A^* to be the conjugate transpose of A (replace each entry with its complex conjugate, then take the transpose). A^* is called the *adjoint* of A .

Think of $|\psi\rangle$ as a column vector ($n \times 1$ matrix). Its adjoint is a row vector denoted by $\langle\psi|$.

Then the matrix product $\rho = |\psi\rangle\langle\psi|$ is an $n \times n$ matrix (operator) which we use to denote the state (rather than $|\psi\rangle$ itself).

This is a *pure state*, *i.e.*, it is completely described.

Quantum states as operators

Definition

For any matrix A with complex entries, define A^* to be the conjugate transpose of A (replace each entry with its complex conjugate, then take the transpose). A^* is called the *adjoint* of A .

Think of $|\psi\rangle$ as a column vector ($n \times 1$ matrix). Its adjoint is a row vector denoted by $\langle\psi|$.

Then the matrix product $\rho = |\psi\rangle\langle\psi|$ is an $n \times n$ matrix (operator) which we use to denote the state (rather than $|\psi\rangle$ itself).

This is a *pure state*, *i.e.*, it is completely described.

Mixed states

Often, we don't know a quantum state exactly (impure), but we still need to work with it.

Let $\rho_1, \rho_2, \dots, \rho_k$ be pure states. Suppose Alice rolls dice and flips coins in her lab and then produces state ρ_i with probability q_i , where $\sum_{i=1}^k q_i = 1$.

Then we say that she produces the state

$$\rho = q_1\rho_1 + q_2\rho_2 + \dots + q_k\rho_k.$$

This ρ is a **convex sum** of the pure states ρ_1, \dots, ρ_k .

Definition

A **quantum state** is any convex sum of pure states.

If the sum involves more than one pure state, then we say that the state is **mixed**.

Mixed states

Often, we don't know a quantum state exactly (impure), but we still need to work with it.

Let $\rho_1, \rho_2, \dots, \rho_k$ be pure states. Suppose Alice rolls dice and flips coins in her lab and then produces state ρ_i with probability q_i , where $\sum_{i=1}^k q_i = 1$.

Then we say that she produces the state

$$\rho = q_1\rho_1 + q_2\rho_2 + \dots + q_k\rho_k.$$

This ρ is a **convex sum** of the pure states ρ_1, \dots, ρ_k .

Definition

A **quantum state** is any convex sum of pure states.

If the sum involves more than one pure state, then we say that the state is **mixed**.

Mixed states

Often, we don't know a quantum state exactly (impure), but we still need to work with it.

Let $\rho_1, \rho_2, \dots, \rho_k$ be pure states. Suppose Alice rolls dice and flips coins in her lab and then produces state ρ_i with probability q_i , where $\sum_{i=1}^k q_i = 1$.

Then we say that she produces the state

$$\rho = q_1\rho_1 + q_2\rho_2 + \dots + q_k\rho_k.$$

This ρ is a **convex sum** of the pure states ρ_1, \dots, ρ_k .

Definition

A *quantum state* is any convex sum of pure states.

If the sum involves more than one pure state, then we say that the state is **mixed**.

Mixed states

Often, we don't know a quantum state exactly (impure), but we still need to work with it.

Let $\rho_1, \rho_2, \dots, \rho_k$ be pure states. Suppose Alice rolls dice and flips coins in her lab and then produces state ρ_i with probability q_i , where $\sum_{i=1}^k q_i = 1$.

Then we say that she produces the state

$$\rho = q_1\rho_1 + q_2\rho_2 + \dots + q_k\rho_k.$$

This ρ is a **convex sum** of the pure states ρ_1, \dots, ρ_k .

Definition

A **quantum state** is any convex sum of pure states.

If the sum involves more than one pure state, then we say that the state is **mixed**.

Mixed states

Often, we don't know a quantum state exactly (impure), but we still need to work with it.

Let $\rho_1, \rho_2, \dots, \rho_k$ be pure states. Suppose Alice rolls dice and flips coins in her lab and then produces state ρ_i with probability q_i , where $\sum_{i=1}^k q_i = 1$.

Then we say that she produces the state

$$\rho = q_1\rho_1 + q_2\rho_2 + \dots + q_k\rho_k.$$

This ρ is a **convex sum** of the pure states ρ_1, \dots, ρ_k .

Definition

A **quantum state** is any convex sum of pure states.

If the sum involves more than one pure state, then we say that the state is **mixed**.

Properties of quantum states

Recall that a quantum state is a certain $n \times n$ matrix.

If ρ is any quantum state, then it satisfies two essential properties:

Positivity ρ is a positive operator, *i.e.*, $\langle \psi | \rho | \psi \rangle \geq 0$ for every column vector $|\psi\rangle$.

Unit trace $\text{Tr}(\rho) = 1$.

One can show that an operator is a quantum state if and only if it has the two properties above.

Properties of quantum states

Recall that a quantum state is a certain $n \times n$ matrix.
If ρ is any quantum state, then it satisfies two essential properties:

Positivity ρ is a positive operator, *i.e.*, $\langle \psi | \rho | \psi \rangle \geq 0$ for every column vector $|\psi\rangle$.

Unit trace $\text{Tr}(\rho) = 1$.

One can show that an operator is a quantum state if and only if it has the two properties above.

Properties of quantum states

Recall that a quantum state is a certain $n \times n$ matrix.
If ρ is any quantum state, then it satisfies two essential properties:

Positivity ρ is a positive operator, *i.e.*, $\langle \psi | \rho | \psi \rangle \geq 0$ for every column vector $|\psi\rangle$.

Unit trace $\text{Tr}(\rho) = 1$.

One can show that an operator is a quantum state if and only if it has the two properties above.

Entropy

Entropy is a measure of uncertainty.

Classically, if $p = p_1, \dots, p_k$ is a probability distribution, then its **Shannon entropy** (in bits) is defined as

$$H(p) = - \sum_{i=1}^k p_i \log_2 p_i.$$

Analogously, the uncertainty of a mixed state ρ is given by its **von Neumann entropy**:

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho).$$

Pure states have von Neumann entropy 0. Mixed states have positive von Neumann entropy.

Entropy

Entropy is a measure of uncertainty.

Classically, if $p = p_1, \dots, p_k$ is a probability distribution, then its **Shannon entropy** (in bits) is defined as

$$H(p) = - \sum_{i=1}^k p_i \log_2 p_i.$$

Analogously, the uncertainty of a mixed state ρ is given by its **von Neumann entropy**:

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho).$$

Pure states have von Neumann entropy 0. Mixed states have positive von Neumann entropy.

Entropy

Entropy is a measure of uncertainty.

Classically, if $p = p_1, \dots, p_k$ is a probability distribution, then its **Shannon entropy** (in bits) is defined as

$$H(p) = - \sum_{i=1}^k p_i \log_2 p_i.$$

Analogously, the uncertainty of a mixed state ρ is given by its **von Neumann entropy**:

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho).$$

Pure states have von Neumann entropy 0. Mixed states have positive von Neumann entropy.

Entropy

Entropy is a measure of uncertainty.

Classically, if $p = p_1, \dots, p_k$ is a probability distribution, then its **Shannon entropy** (in bits) is defined as

$$H(p) = - \sum_{i=1}^k p_i \log_2 p_i.$$

Analogously, the uncertainty of a mixed state ρ is given by its **von Neumann entropy**:

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho).$$

Pure states have von Neumann entropy 0. Mixed states have positive von Neumann entropy.

Quantum channels

A **quantum channel** is a certain linear operator that maps states in one system to states in another system (or the same system).

If \mathcal{E} is a quantum channel and ρ is a quantum state, then $\mathcal{E}(\rho)$ is a quantum state (maybe in another system).

Quantum channels can transmit information via quantum states.

Techniques of (classical) information theory (due to Shannon) can be adapted to study quantum channels.

Quantum channels

A **quantum channel** is a certain linear operator that maps states in one system to states in another system (or the same system).

If \mathcal{E} is a quantum channel and ρ is a quantum state, then $\mathcal{E}(\rho)$ is a quantum state (maybe in another system).

Quantum channels can transmit information via quantum states.

Techniques of (classical) information theory (due to Shannon) can be adapted to study quantum channels.

Quantum channels

A **quantum channel** is a certain linear operator that maps states in one system to states in another system (or the same system).

If \mathcal{E} is a quantum channel and ρ is a quantum state, then $\mathcal{E}(\rho)$ is a quantum state (maybe in another system).

Quantum channels can transmit information via quantum states.

Techniques of (classical) information theory (due to Shannon) can be adapted to study quantum channels.

Quantum channels

A **quantum channel** is a certain linear operator that maps states in one system to states in another system (or the same system).

If \mathcal{E} is a quantum channel and ρ is a quantum state, then $\mathcal{E}(\rho)$ is a quantum state (maybe in another system).

Quantum channels can transmit information via quantum states.

Techniques of (classical) information theory (due to Shannon) can be adapted to study quantum channels.

Quantum channel capacity

The **capacity** of a noisy channel \mathcal{E} to transmit information is given in terms of entropies.

Classically, the capacity of a channel from Alice to Bob is the maximum mutual information achievable by Alice tweaking her source distribution.

Quantally, given a source distribution on quantum states ρ_1, \dots, ρ_k with probabilities q_1, \dots, q_k respectively, the mutual information is given by

$$\chi = S\left(\sum_i q_i \mathcal{E}(\rho_i)\right) - \sum_i q_i S(\mathcal{E}(\rho_i)).$$

The capacity is then the biggest value of χ obtainable by varying the ρ_i and q_i .

Quantum channel capacity

The **capacity** of a noisy channel \mathcal{E} to transmit information is given in terms of entropies.

Classically, the capacity of a channel from Alice to Bob is the maximum mutual information achievable by Alice tweaking her source distribution.

Quantally, given a source distribution on quantum states ρ_1, \dots, ρ_k with probabilities q_1, \dots, q_k respectively, the mutual information is given by

$$\chi = S\left(\sum_i q_i \mathcal{E}(\rho_i)\right) - \sum_i q_i S(\mathcal{E}(\rho_i)).$$

The capacity is then the biggest value of χ obtainable by varying the ρ_i and q_i .

Quantum channel capacity

The **capacity** of a noisy channel \mathcal{E} to transmit information is given in terms of entropies.

Classically, the capacity of a channel from Alice to Bob is the maximum mutual information achievable by Alice tweaking her source distribution.

Quantally, given a source distribution on quantum states ρ_1, \dots, ρ_k with probabilities q_1, \dots, q_k respectively, the mutual information is given by

$$\chi = S\left(\sum_i q_i \mathcal{E}(\rho_i)\right) - \sum_i q_i S(\mathcal{E}(\rho_i)).$$

The capacity is then the biggest value of χ obtainable by varying the ρ_i and q_i .

Quantum channel capacity

The **capacity** of a noisy channel \mathcal{E} to transmit information is given in terms of entropies.

Classically, the capacity of a channel from Alice to Bob is the maximum mutual information achievable by Alice tweaking her source distribution.

Quantally, given a source distribution on quantum states ρ_1, \dots, ρ_k with probabilities q_1, \dots, q_k respectively, the mutual information is given by

$$\chi = S\left(\sum_i q_i \mathcal{E}(\rho_i)\right) - \sum_i q_i S(\mathcal{E}(\rho_i)).$$

The capacity is then the biggest value of χ obtainable by varying the ρ_i and q_i .

Additivity

Classically, when combining noisy channels (or separate uses of the same channel), the capacities add.

Conjecture (Additivity Conjecture)

The same is true for quantum channels.

Peter Shor showed that the Additivity Conjecture is equivalent to several other important conjectures in quantum information theory. If true, it would make computing quantum channel capacities **easy**.

Hastings (2009): The Additivity Conjecture is **FALSE**.

Basic reason: Input states to different channels may be **entangled**.

Additivity

Classically, when combining noisy channels (or separate uses of the same channel), the capacities add.

Conjecture (Additivity Conjecture)

The same is true for quantum channels.

Peter Shor showed that the Additivity Conjecture is equivalent to several other important conjectures in quantum information theory. If true, it would make computing quantum channel capacities **easy**.

Hastings (2009): The Additivity Conjecture is **FALSE**.

Basic reason: Input states to different channels may be **entangled**.

Additivity

Classically, when combining noisy channels (or separate uses of the same channel), the capacities add.

Conjecture (Additivity Conjecture)

The same is true for quantum channels.

Peter Shor showed that the Additivity Conjecture is equivalent to several other important conjectures in quantum information theory. If true, it would make computing quantum channel capacities **easy**.

Hastings (2009): The Additivity Conjecture is **FALSE**.

Basic reason: Input states to different channels may be **entangled**.

Additivity

Classically, when combining noisy channels (or separate uses of the same channel), the capacities add.

Conjecture (Additivity Conjecture)

The same is true for quantum channels.

Peter Shor showed that the Additivity Conjecture is equivalent to several other important conjectures in quantum information theory. If true, it would make computing quantum channel capacities **easy**.

Hastings (2009): The Additivity Conjecture is **FALSE**.

Basic reason: Input states to different channels may be **entangled**.

Additivity

Classically, when combining noisy channels (or separate uses of the same channel), the capacities add.

Conjecture (Additivity Conjecture)

The same is true for quantum channels.

Peter Shor showed that the Additivity Conjecture is equivalent to several other important conjectures in quantum information theory. If true, it would make computing quantum channel capacities **easy**.

Hastings (2009): The Additivity Conjecture is **FALSE**.

Basic reason: Input states to different channels may be **entangled**.

Questions?