Mathematical Foundations of Quantum Information

John Watrous
Department of Computer Science
University of Calgary

Overview

So far, we have been using a simple mathematical framework for discussing quantum information:

quantum state ↔ unit vector in a Hilbert space

evolution ↔ unitary operators

measurement ↔ projections

In many situations that arise when studying quantum information, this framework is either inconvenient or inadequate…

Overview

We extend this formalism by considering a different way of representing quantum states:

quantum state ↔ a **matrix** (or **operator**) acting on a Hilbert space

This extension has various advantages over the simpler formalism (in many situations) as we will see…

"Ket" vectors

Suppose we have a superposition on n qubits:

known as a "ket"

$$|\psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle \longleftrightarrow \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{bmatrix}$$

Let $\mathcal{H}$ be a space corresponding to n qubits…
$|\psi\rangle$ is a unit vector in $\mathcal{H}$.

Terminology: $|\psi\rangle$ is a **pure state**.

“Bra” Vectors

The corresponding “bra”:

$$\langle \psi | = \sum_{x=0}^{2^n-1} \overline{\alpha_x} \langle x | \longleftrightarrow \left(\overline{\alpha_0} \quad \overline{\alpha_1} \quad \cdots \quad \overline{\alpha_{2^n-1}} \right)$$

The names come from the fact that a “bra” plus a “ket” form a “bracket”:

$$\text{if } |\phi\rangle = \sum_{x=0}^{2^n-1} \beta_x |x\rangle \quad \text{then} \quad \langle \phi | \psi \rangle = \sum_{x=0}^{2^n-1} \overline{\beta_x} \alpha_x$$

Density Matrices

The **density matrix** corresponding to $|\psi\rangle$ is:

$$|\psi\rangle\langle\psi| \longleftrightarrow \begin{bmatrix} \alpha_0\overline{\alpha_0} & \alpha_0\overline{\alpha_1} & \cdots & \alpha_0\overline{\alpha_{2^n-1}} \\ \alpha_1\overline{\alpha_0} & \alpha_1\overline{\alpha_1} & \cdots & \alpha_1\overline{\alpha_{2^n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{2^n-1}\overline{\alpha_0} & \alpha_{2^n-1}\overline{\alpha_1} & \cdots & \alpha_{2^n-1}\overline{\alpha_{2^n-1}} \end{bmatrix}$$

$$\mathrm{Tr}\left(|\psi\rangle\langle\psi|\right) = \sum_x \alpha_x\overline{\alpha_x} = \sum_x |\alpha_x|^2 = 1$$

Density Matrices

Now suppose we have a collection of pure states:

$$\left\{ \left|\square_1\right\rangle, \left|\square_2\right\rangle, \mathrm{K}\ , \left|\square_k\right\rangle \right\}$$

and we imagine randomly choosing a state; choose $\left|\square_j\right\rangle$ with probability p_j for each $j=1,\ldots,k$.

$$\xcancel{\square_{j=1}^{k} p_j \left|\square_j\right\rangle}$$

doesn’t make sense… the p_j values are probabilities not amplitudes.

Density Matrices

Now suppose we have a collection of pure states:

$$\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle\}$$

and we imagine randomly choosing a state; choose $|\psi_j\rangle$ with probability p_j for each $j=1,\ldots,k$.

For density matrices it works:

$$\sum_{j=1}^{k} p_j |\psi_j\rangle\langle\psi_j|$$

this is called a **mixture** (or ensemble)

Examples

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \longleftrightarrow \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$|+\rangle\langle+| \quad \longleftrightarrow \quad \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \quad \longleftrightarrow \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

$$|-\rangle\langle-| \quad \longleftrightarrow \quad \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

Examples

Suppose we randomly choose one of $|+\rangle$ and $|-\rangle$ each with probability 1/2.

Resulting density matrix:

$$\frac{1}{2}|+\rangle\langle+| \;+\; \frac{1}{2}|-\rangle\langle-| \quad\longleftrightarrow\quad \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

↕ **equal ?**

Same thing with states $|0\rangle$ and $|1\rangle$:

$$\frac{1}{2}|0\rangle\langle0| \;+\; \frac{1}{2}|1\rangle\langle1| \quad\longleftrightarrow\quad \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Mixtures vs. density matrices

It is not an accident that different mixtures can give the same density matrix…

…two mixtures can be distinguished if and only if they yield different density matrices.

Density matrices describe **mixed states**. For instance,

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

describes a mixed state. It is equal to

$$\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|\square\rangle\langle \square|$$

Facts about density matrices

- Every density matrix has trace equal to 1:

$$\mathrm{Tr}\left(\sum_{j=1}^{k} p_j \left|\psi_j\right\rangle\left\langle\psi_j\right|\right) = \sum_{j=1}^{k} p_j \,\mathrm{Tr}\left(\left|\psi_j\right\rangle\left\langle\psi_j\right|\right) = \sum_{j=1}^{k} p_j = 1$$

- Every density matrix is **positive semidefinite** (Hermitian, with all eigenvalues nonnegative.)

Implies that every density matrix ρ comes from a mixture of orthogonal pure states:

$$\rho = \sum_{j=1}^{m} q_j \left|\phi_j\right\rangle\left\langle\phi_j\right|$$

where $\left\{\left|\phi_1\right\rangle, \ldots, \left|\phi_m\right\rangle\right\}$ is an orthonormal set.

Quantum Transformations

The class of physically realizable transformations is easily characterized:

$$T : \rho \mapsto \sum_{j=1}^{k} A_j \rho A_j^{\dagger}$$

provided $\sum_{j=1}^{k} A_j^{\dagger} A_j = I$.

Equivalently, T is completely positive and trace preserving.

Measurements

Any collection $\{E_1, \ldots, E_k\}$ of matrices satisfying

$$\sum_{j=1}^{k} E_j^\dagger E_j = I$$

defines a measurement.

If ρ is measured, the outcome j results with probability

$$p_j = \mathrm{Tr}\left(E_j \rho E_j^\dagger\right)$$

and the state becomes

$$\frac{1}{p_j} E_j \rho E_j^\dagger$$

corrected
(incorrect during talk)

Relation to simpler model

Note: from an **algorithmic** point of view, there is nothing to be gained from these more general transformations and measurements…

…can simulate general transformations and measurements with unitary gates and projective measurements.

Fidelity and Trace-Distance

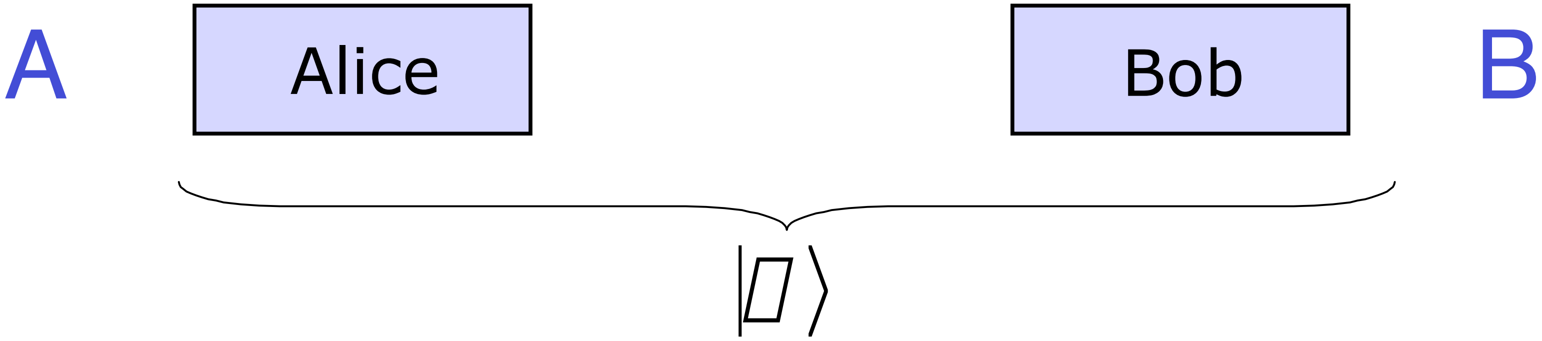
Natural notions of closeness between mixed states exist:

Fidelity: $F(\square,\square) = \mathrm{Tr}\sqrt{\sqrt{\square}\,\square\,\sqrt{\square}}$

Trace distance: $\left\|\square\square\square\right\|_{\mathrm{tr}} = \mathrm{Tr}\left|\square\square\square\right|$

Bipartite Systems

Suppose Alice and Bob share some state $|\psi\rangle$…



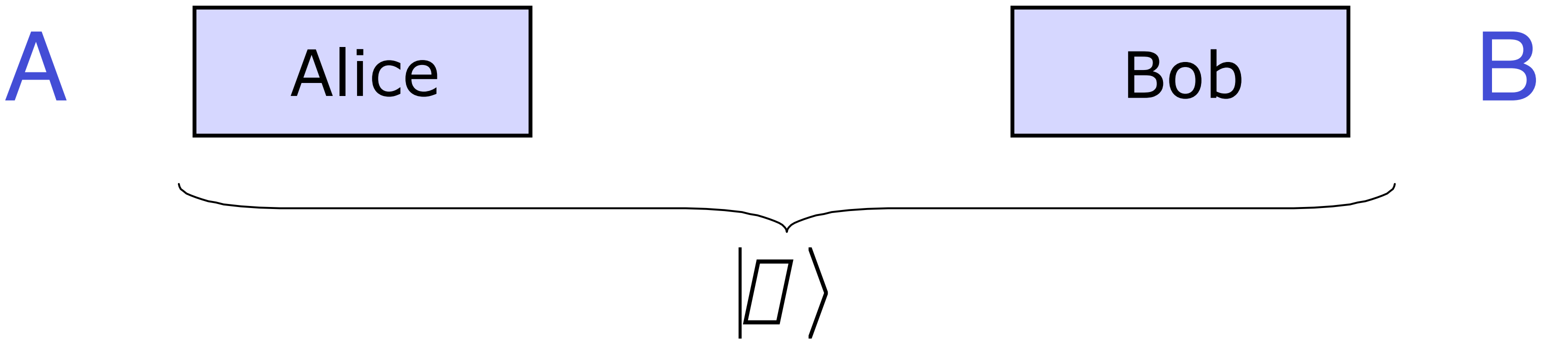
…but Bob decides to leave town.

What is Alice left with? Answer: a mixed state.

Combined state: $|\psi\rangle \in A \otimes B$

Bipartite Systems

Suppose Alice and Bob share some state $|\psi\rangle$…



A

Alice

Bob

B

$|\psi\rangle$

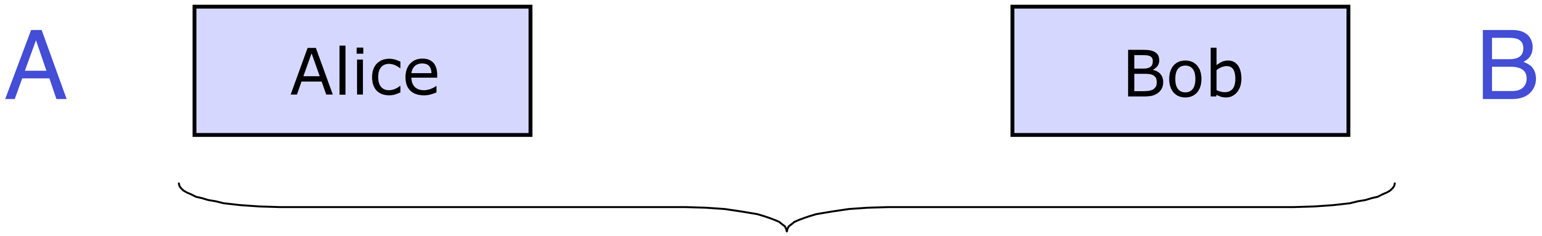
…but Bob decides to leave town.

What is Alice left with? Answer: a mixed state.

Alice’s state (after Bob leaves town):

Partial trace → $\mathrm{Tr}_B \, |\psi\rangle\langle\psi|$

Partial Trace


A

Alice

Bob

B

$$|\square\rangle$$

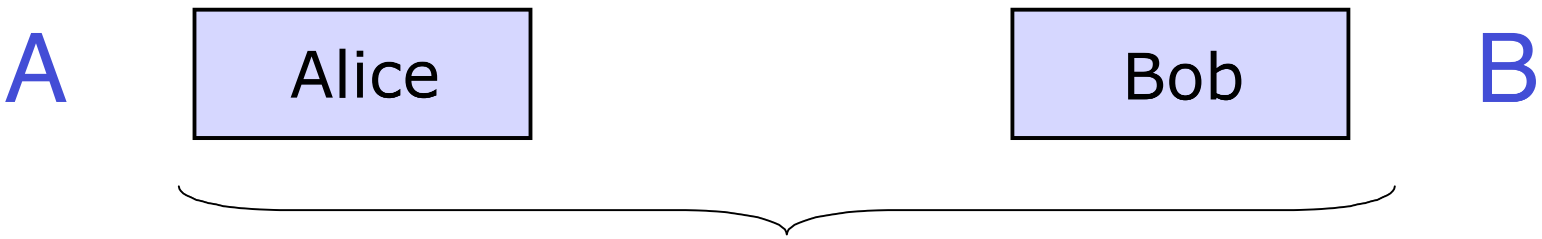
$$\mathrm{Tr}_{\mathrm{B}}\,|\square\rangle\langle\square| = \mathop{\square}_{j} \left(I \quad \langle j|\right)|\square\rangle\langle\square|\left(I \quad |j\rangle\right)$$

or

$$\mathrm{Tr}_{\mathrm{B}}\ A \quad \mathrm{B} = \left(\mathrm{Tr}\,B\right)A$$

(and extend to all matrices by linearity)

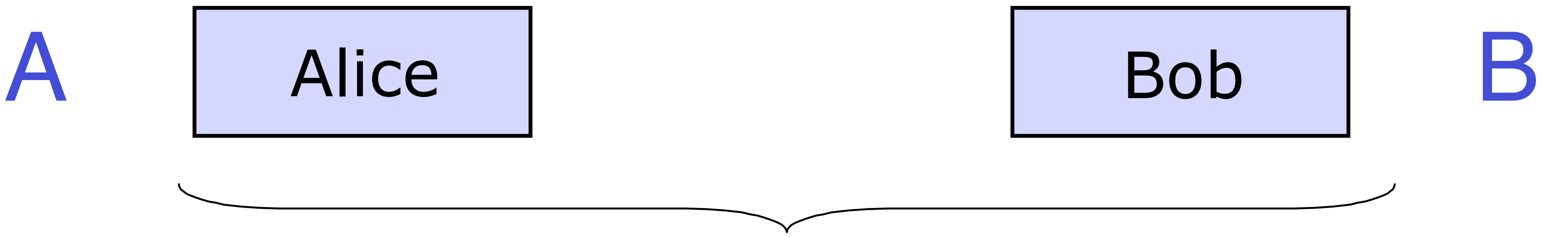
Example



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

$$\begin{aligned}\mathrm{Tr}_{\mathrm{B}}\, |\Phi^+\rangle\langle\Phi^+| &= \left(I \quad \langle 0|\right)|\Phi^+\rangle\langle\Phi^+|\left(I \quad |0\rangle\right) \\ &\quad + \left(I \quad \langle 1|\right)|\Phi^+\rangle\langle\Phi^+|\left(I \quad |1\rangle\right) \\ &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\end{aligned}$$

Example



$$\left|\Box^{\Box}\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle\left|0\right\rangle \Box \frac{1}{\sqrt{2}}\left|1\right\rangle\left|1\right\rangle$$

$$\mathrm{Tr}_{B}\left|\Box^{\Box}\right\rangle\left\langle\Box^{\Box}\right| = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| + \frac{1}{2}\left|1\right\rangle\left\langle 1\right|$$

Bell Basis

$$\left|\square^{+}\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle\left|1\right\rangle \qquad \left|\square^{\square}\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle\left|0\right\rangle \square \frac{1}{\sqrt{2}}\left|1\right\rangle\left|1\right\rangle$$

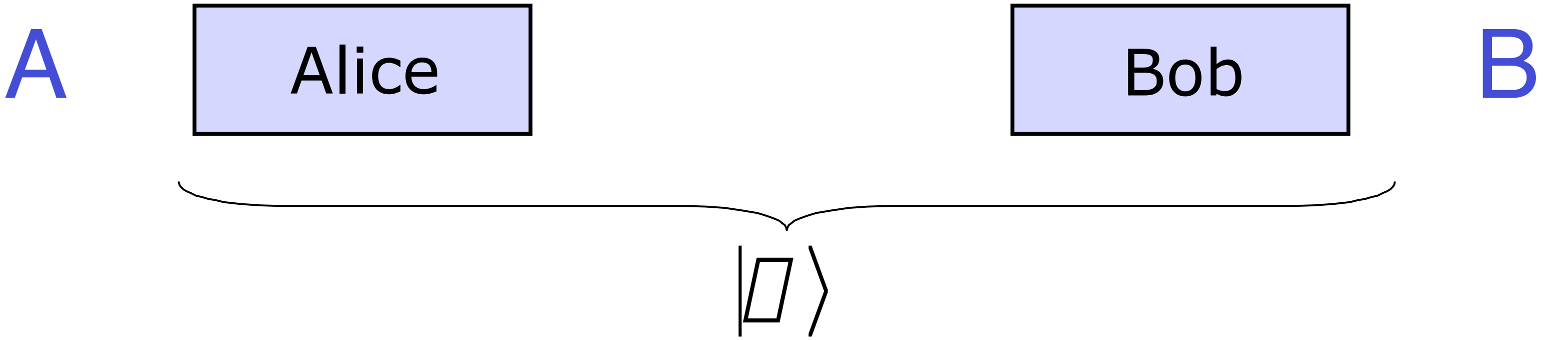
$$\left|\square^{+}\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle\left|1\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle\left|0\right\rangle \qquad \left|\square^{\square}\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle\left|1\right\rangle \square \frac{1}{\sqrt{2}}\left|1\right\rangle\left|0\right\rangle$$

They all look the same to Alice:

$$\mathrm{Tr}_{\mathrm{B}}\left|\square^{+}\right\rangle\left\langle\square^{+}\right| = \mathrm{Tr}_{\mathrm{B}}\left|\square^{\square}\right\rangle\left\langle\square^{\square}\right| = \mathrm{Tr}_{\mathrm{B}}\left|\square^{+}\right\rangle\left\langle\square^{+}\right| = \mathrm{Tr}_{\mathrm{B}}\left|\square^{\square}\right\rangle\left\langle\square^{\square}\right|$$

$$= \frac{1}{2}\left|0\right\rangle\left\langle 0\right| + \frac{1}{2}\left|1\right\rangle\left\langle 1\right|$$

Schmidt Decomposition



A Alice Bob B

$$|\square\rangle$$

Suppose we have orthonormal bases for A and B:

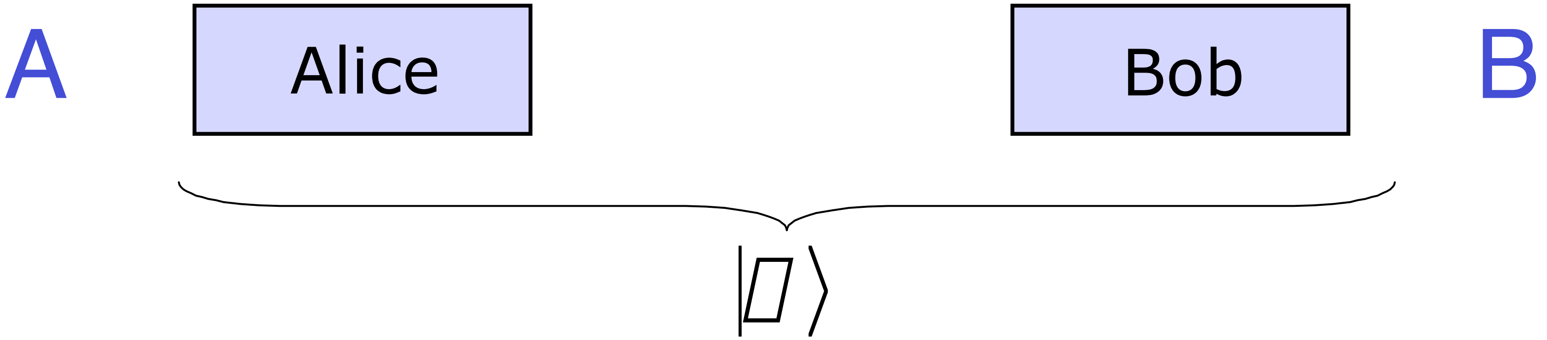
A: $\{|\square_1\rangle, \mathrm{K}\ , |\square_n\rangle\ \}$ B: $\{|\square_1\rangle, \mathrm{K}\ , |\square_m\rangle\ \}$

It is possible to write

$$|\square\rangle = \mathop{\square}\limits_{j=1}^{n} \mathop{\square}\limits_{k=1}^{m} \square_{j,k} |\square_j\rangle |\square_k\rangle$$

for some choice of complex numbers $\{\square_{j,k}\ \}$.

Schmidt Decomposition



The **Schmidt decomposition** says that there exist particular choices of orthonormal bases

A: $\{|\square_1\rangle, \mathrm{K}\ , |\square_n\rangle\}$ B: $\{|\square_1\rangle, \mathrm{K}\ , |\square_m\rangle\}$

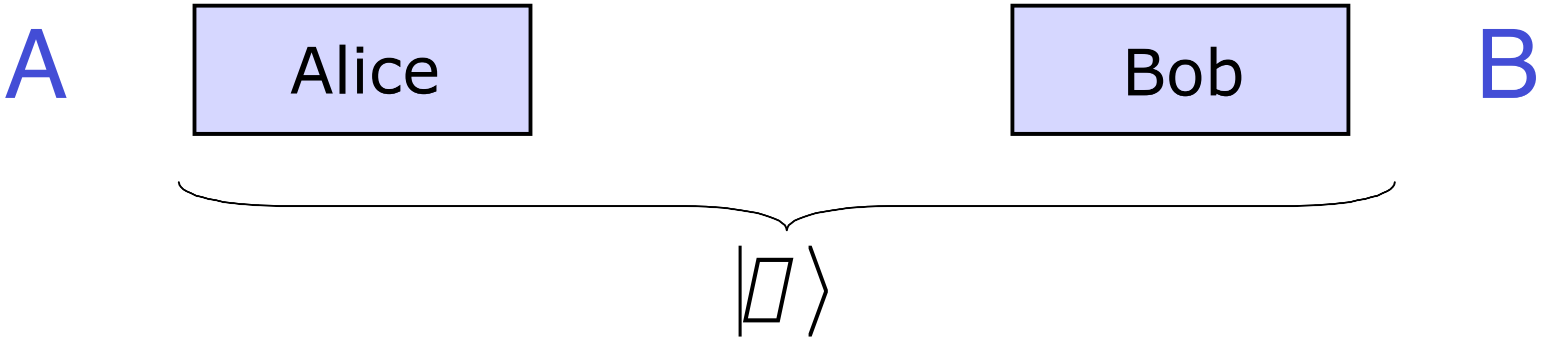
eigenvectors of $\mathrm{Tr}_{\mathrm{B}}\,|\square\rangle\langle\square|$

(depending on $|\square\rangle$) such that

$$|\square\rangle = \sum_{j=1}^{\min(n,m)} \sqrt{p_j}\,|\square_j\rangle|\square_j\rangle$$

for some choice of $\{p_j\}$. No cross terms!

Schmidt Decomposition



The **Schmidt decomposition** says that there exist particular choices of orthonormal bases

A: $\{|\alpha_1\rangle, \ldots, |\alpha_n\rangle\}$ B: $\{|\beta_1\rangle, \ldots, |\beta_m\rangle\}$

(depending on $|\psi\rangle$) such that

$$|\psi\rangle = \sum_{j=1}^{\min(n,m)} \sqrt{p_j}\, |\alpha_j\rangle|\beta_j\rangle$$

eigenvectors of $\mathrm{Tr}_A |\psi\rangle\langle\psi|$

for some choice of $\{p_j\}$. No cross terms!

Schmidt Decomposition

Several interesting facts follow. For instance…

The (nonzero) eigenvalues of the reduced states

$$\mathrm{Tr}_{\mathrm{A}} \left|\square\right\rangle\left\langle\square\right| \qquad \text{and} \qquad \mathrm{Tr}_{\mathrm{B}} \left|\square\right\rangle\left\langle\square\right|$$

are the same.

$$\left|\square\right\rangle = \mathop{\square}_{j=1}^{\min(n,m)} \sqrt{p_j}\, \left|\square_j\right\rangle\left|\square_j\right\rangle$$

$$\mathrm{Tr}_{\mathrm{B}} \left|\square\right\rangle\left\langle\square\right| = \mathop{\square}_{j} p_j \left|\square_j\right\rangle\left\langle\square_j\right| \qquad \mathrm{Tr}_{\mathrm{A}} \left|\square\right\rangle\left\langle\square\right| = \mathop{\square}_{j} p_j \left|\square_j\right\rangle\left\langle\square_j\right|$$

Purifications

The previous fact is often used in conjunction with the fact that every mixed state has a **purification**:

Given a mixed state ρ, there is an orthonormal basis $\{|\phi_1\rangle,\ldots,|\phi_n\rangle\}$ such that

$$\rho = \sum_{j=1}^{n} p_j |\phi_j\rangle\langle\phi_j|$$

Let

$$|\psi\rangle = \sum_{j=1}^{n} \sqrt{p_j}\, |\phi_j\rangle|\phi_j\rangle \in \mathrm{A} \otimes \mathrm{B}$$

Then

$$\mathrm{Tr}_{\mathrm{B}} |\psi\rangle\langle\psi| = \sum_{j} p_j |\phi_j\rangle\langle\phi_j| = \rho$$

Schmidt Decomposition

Another interesting consequence of the Schmidt decomposition…

Suppose $|\square\rangle$ and $|\square\rangle$ are bipartite quantum states

$$|\square\rangle, |\square\rangle \;\square\; A \quad B$$

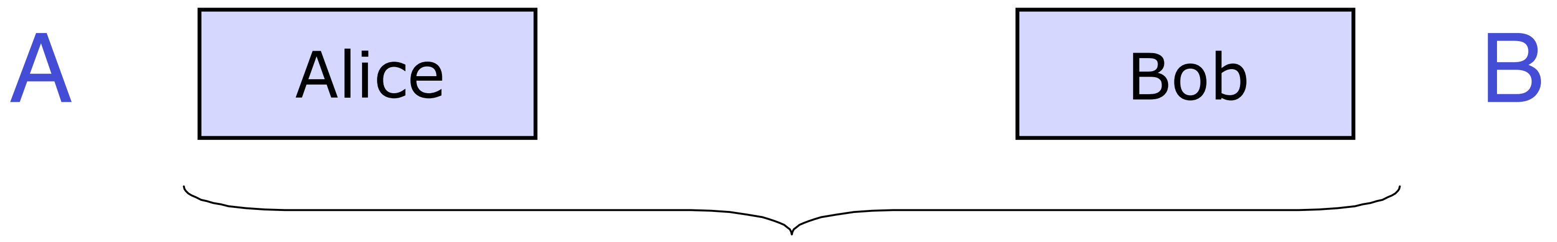
that look the same to Alice:

$$\mathrm{Tr}_B |\square\rangle\langle\square| = \mathrm{Tr}_B |\square\rangle\langle\square|$$

Then there exists a unitary operator U acting only on B such that

$$(I \quad U)|\square\rangle = |\square\rangle$$

Schmidt Decomposition



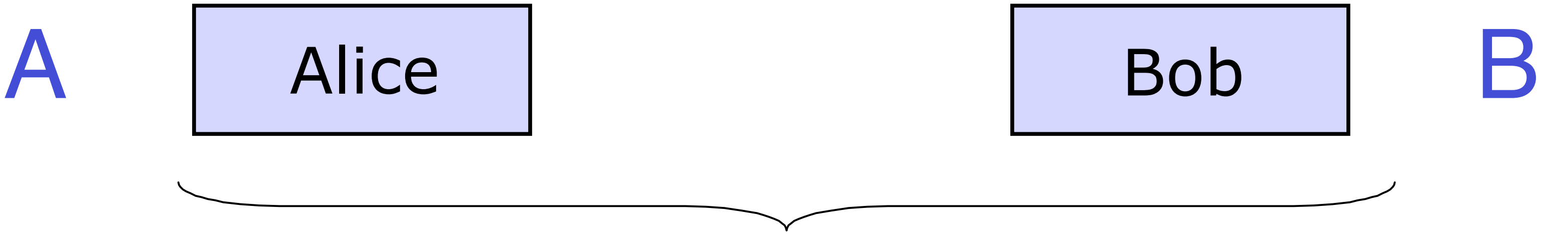
$|\square\rangle$ a $|\square\rangle$

Suppose now that Bob doesn’t leave town, but instead decides he wants to change the state he shares with Alice to some other (pure) state.

What are his choices? He can change the state to **any** state $|\square\rangle$ for which

$$\mathrm{Tr}_B\, |\square\rangle\langle\square| = \mathrm{Tr}_B\, |\square\rangle\langle\square|$$

Superdense Coding



A

Alice

Bob

B

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

In superdense coding Alice and Bob share an entangled state…

…suppose Bob wants to communicate 2 classical bits to Alice by sending only one qubit.

Superdense Coding

A Alice Bob B

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle}$$

Encoding:

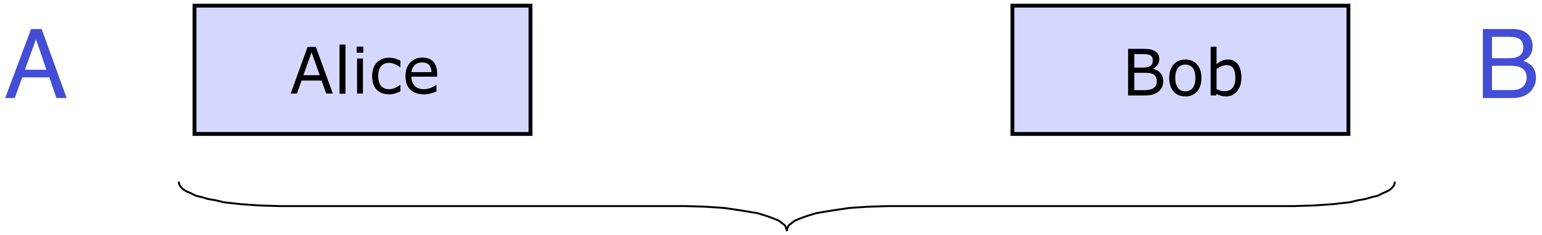
$$00 \longrightarrow \left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

$$01 \longrightarrow \left|\Phi^{-}\right\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

$$10 \longrightarrow \left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

$$11 \longrightarrow \left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle$$

Superdense Coding



$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

All Bell states look the same to Alice…

$$\mathrm{Tr_B}\left|\Phi^+\right\rangle\left\langle\Phi^+\right| = \mathrm{Tr_B}\left|\Phi^-\right\rangle\left\langle\Phi^-\right| = \mathrm{Tr_B}\left|\Psi^+\right\rangle\left\langle\Psi^+\right| = \mathrm{Tr_B}\left|\Psi^-\right\rangle\left\langle\Psi^-\right|$$

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

…so Bob can convert between them as he chooses.

Bit Commitment

The same principle can be used to show that an interesting task—**bit commitment**—is impossible.

Bit commitment works as follows:

Alice has a bit $b \in \{0,1\}$ and she wants to commit to this bit…

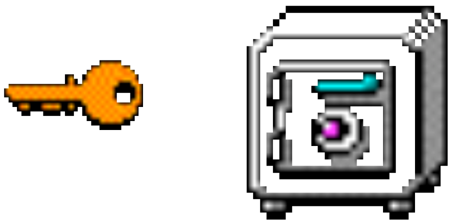
…but she doesn't want Bob to know the bit until later when she decides to reveal it.

Two requirements: **binding** and **concealing**.

Bit Commitment

We can imagine implementing bit commitment in the following way:

1. When Alice wants to commit her bit a, she writes a on a piece of paper, locks it in a safe, and sends the safe to Bob. (Alice keeps the key.)



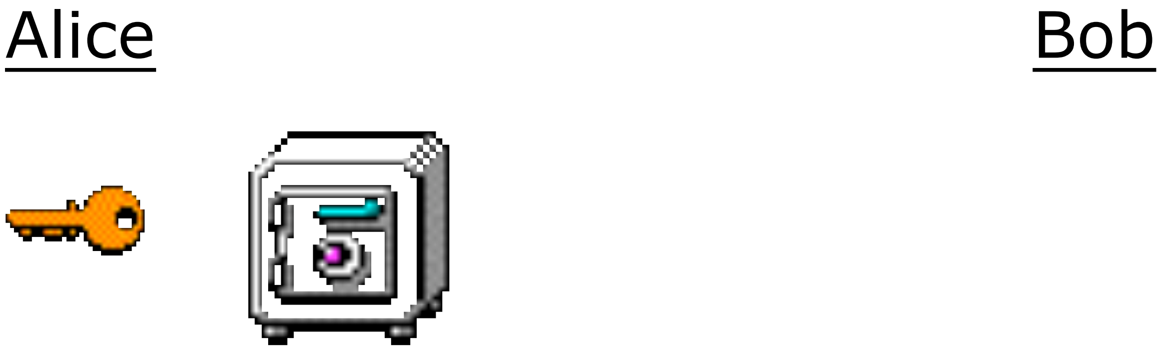
Alice

Bob

Bit Commitment

We can imagine implementing bit commitment in the following way:

1. When Alice wants to commit her bit a, she writes a on a piece of paper, locks it in a safe, and sends the safe to Bob. (Alice keeps the key.)



Alice

Bob

Bit Commitment

2. When Alice wants to reveal her bit, she sends Bob the key.

Bit Commitment

2. When Alice wants to reveal her bit, she sends Bob the key.

Bit Commitment

Information-theoretically secure bit commitment is impossible classically.

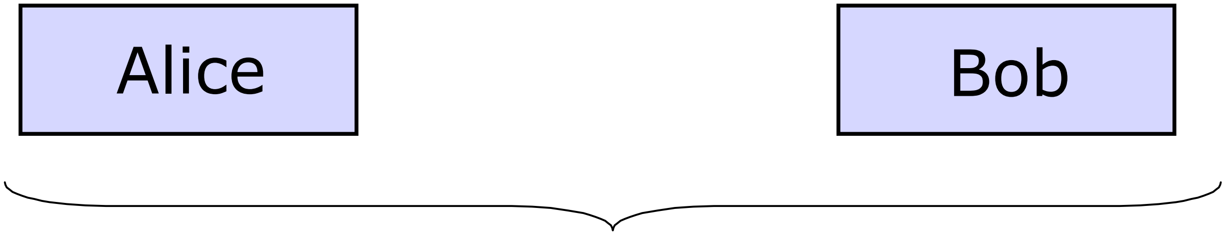
Quantum bit commitment schemes were proposed in the early 1990's… they were originally thought to be secure.

But it turns out that they were not secure after all…

…moreover, we now know that quantum bit commitment is impossible using <u>any</u> scheme.

Impossibility of Bit Commitment

Suppose we have a scheme where Alice sends Bob half of some entangled state:



$$b = 0 \Rightarrow \quad \text{state} = |\psi_0\rangle$$

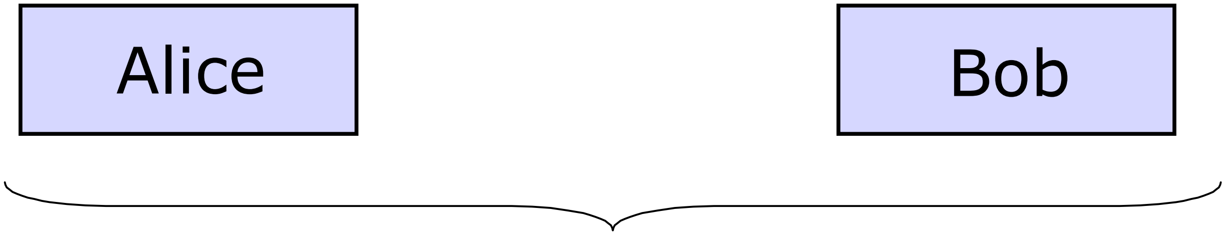
$$b = 1 \Rightarrow \quad \text{state} = |\psi_1\rangle$$

If the scheme is perfectly concealing, Bob cannot distinguish the two states:

$$\mathrm{Tr}_\mathrm{A} |\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_\mathrm{A} |\psi_1\rangle\langle\psi_1|$$

Impossibility of Bit Commitment

Suppose we have a scheme where Alice sends Bob half of some entangled state:



Alice

Bob

$$b = 0 \;\square\; \text{state} = |\square_0\rangle$$

$$b = 1 \;\square\; \text{state} = |\square_1\rangle$$

This gives Alice the freedom to change her mind:

$$(U \quad I)|\square_0\rangle = |\square_1\rangle \quad \text{(for some } U\text{)}$$

so the scheme cannot be binding.

Entanglement

The notion of **entanglement** has been mentioned several times so far this week.

Archetypal example of an entangled quantum state:

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

Entanglement is useful for various tasks:

- teleportation
- superdense coding
- quantum communication protocols
- quantum computation?

Entanglement is (arguably) not well understood…

Entanglement

What is entanglement?

Given a pure state of a bipartite system:

$$|\psi\rangle \in A \otimes B$$

We say that $|\psi\rangle$ is a **product state** if

$$|\psi\rangle = |\phi\rangle|\chi\rangle$$

for $|\phi\rangle \in A$ and $|\chi\rangle \in B$.

If $|\psi\rangle$ is not a product state, then it is **entangled**.

Entanglement

Mixed state case: ρ is **separable** if

$$\rho = \sum_{j=1}^{k} p_j \alpha_j \otimes \beta_j$$

for $\alpha_1, \ldots, \alpha_k$ and $\beta_1, \ldots, \beta_k$ mixed states of the first and second system, respectively.

If ρ is not separable, then it is **entangled**.

(Given a density matrix ρ, it is a very difficult computational problem to test whether it is entangled.)

Entanglement

For example, the following state is not entangled:

$$|1\rangle|1\rangle$$

Which one is more entangled?

while this state is entangled:

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

So is this state:

$$\sqrt{10^{-9}}|0\rangle|0\rangle+\sqrt{1-10^{-9}}|1\rangle|1\rangle$$

Measures of Entanglement

There are many ways to measure entanglement.

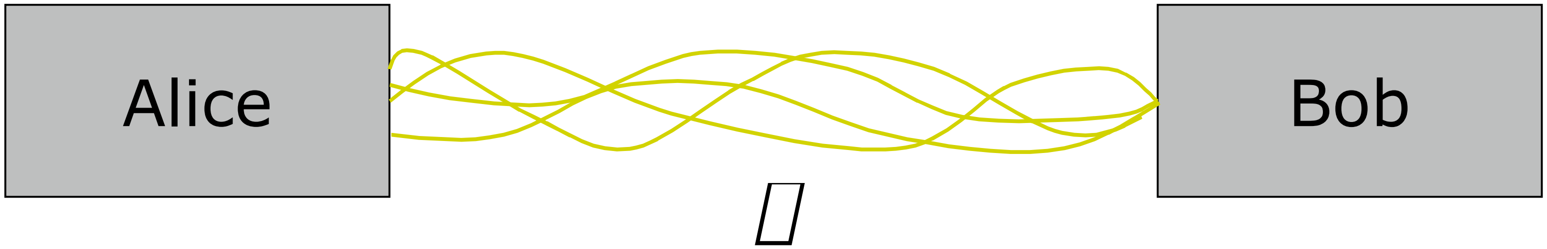
Two natural measures:

how much does it cost to create?

- **Entanglement cost.**
- **Distillable entanglement.**

how much can you get out of it?

Local quantum operations
+
classical communication



Alice and Bob share some entangled state ▯.

Any transformation they can perform on ▯ that does not require them to send quantum information is said to be an **LOCC transformation**.

Entanglement Cost

Suppose Alice and Bob want to share N copies of $\square$ (where N is very large), but they only share copies of $\left|\square^{+}\right\rangle$.

It is always possible for them to convert kN copies of $\left|\square^{+}\right\rangle$ into N copies of $\square$ (approximately) via some LOCC transformation for some k.

The **entanglement cost** of $\square$ is the infimum over all values of k for which this is possible.

$E_C(\square)$ = entanglement cost of $\square$

Distillable Entanglement

Distillable entanglement is essentially the opposite…

Suppose Alice and Bob share N copies of ρ (where N is very large), and they want copies of $\left|\Phi^{+}\right\rangle$.

The **distillable entanglement** of ρ is the supremum over all values of k for which they can extract kN copies of $\left|\Phi^{+}\right\rangle$ from N copies of ρ.

$E_D(\rho)$ = distillable entanglement of ρ

The von Neumann Entropy

In the case of pure states, these quantities are always equal:

$$E_C\left(\left|\square\right\rangle\right) = E_D\left(\left|\square\right\rangle\right) \overset{\text{def}}{=} E\left(\left|\square\right\rangle\right)$$

and this quantity is given by the von Neumann entropy of Alice’s (or Bob’s) reduced state:

$$E\left(\left|\square\right\rangle\right) = S\left(\mathrm{Tr}_{\mathrm{A}}\left|\square\right\rangle\left\langle\square\right|\right) = S\left(\mathrm{Tr}_{\mathrm{B}}\left|\square\right\rangle\left\langle\square\right|\right)$$

where

$$S(\square) = \square\mathrm{Tr}(\square\log\square)$$

The von Neumann Entropy

Proof starts by looking at the Schmidt decomposition of $|\square\rangle$:

$$|\square\rangle = \mathop{\square}_{j=1}^{m} \sqrt{p_j}\, |\square_j\rangle |\square_j\rangle$$

A large number of copies N of this state behaves in a very similar way to N independent samples from a random source with respect to the bases

$$\left\{|\square_1\rangle, \mathrm{K}\ , |\square_m\rangle\right\} \quad \text{and} \quad \left\{|\square_1\rangle, \mathrm{K}\ , |\square_m\rangle\right\}$$

Distillation and formation are very similar in spirit to compression and decompression…

Mixed state entanglement

Things become much more complicated (and more interesting) for mixed states… for instance:

- The task of testing whether a given density matrix is entangled or separable is **NP-hard** (with respect to Cook reductions).

- There exist states ρ for which

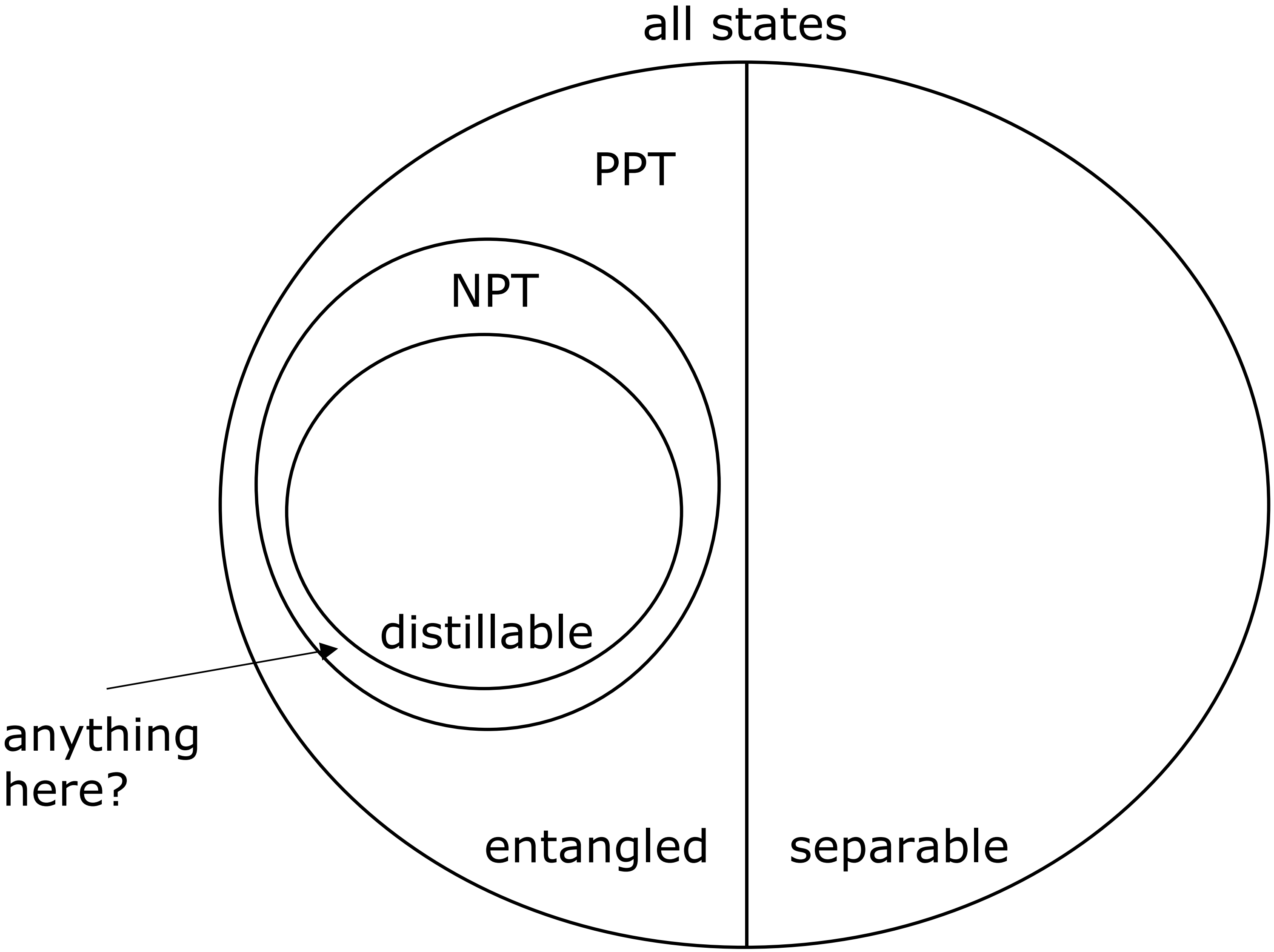
$$0 < E_D(\rho) < E_C(\rho)$$

- There exist <u>entangled</u> states ρ for which

$$E_D(\rho) = 0$$

(“bound entangled” states).

Diagram of bipartite states



Example

Is this state distillable?

$$\rho = \frac{1}{15}\sum_{j,k=0}^{2}\left(2\,|j\rangle\langle j| \otimes |k\rangle\langle k| - |j\rangle\langle k| \otimes |k\rangle\langle j|\right)$$

(It is an NPT state, and is conjectured to be undistillable.)

Conclusion

The purpose of this talk has been to give an introduction to the mathematical foundations of quantum information.

There are many other interesting topics in quantum information theory. For example:

- many other aspects of entanglement (such as multiparty entanglement)
- quantum channel capacities, additivity questions.
- quantum error correction