Summer School 2012, Aug. 8-18, Miyako

量子情報基礎

Masato Koashi, Univ. of Tokyo

1. Basic rules of quantum mechanics
2. State of subsystems
3. Qubits
4. Power of ancilla system
5. Communication resources
6. Quantum error correcting codes

1. Basic rules of quantum mechanics

How to describe the states of an ideally controlled system?

How to describe changes in an ideally controlled system?

How to describe measurements on an ideally controlled system?

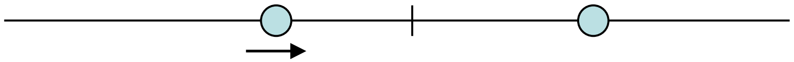
How to treat composite systems?

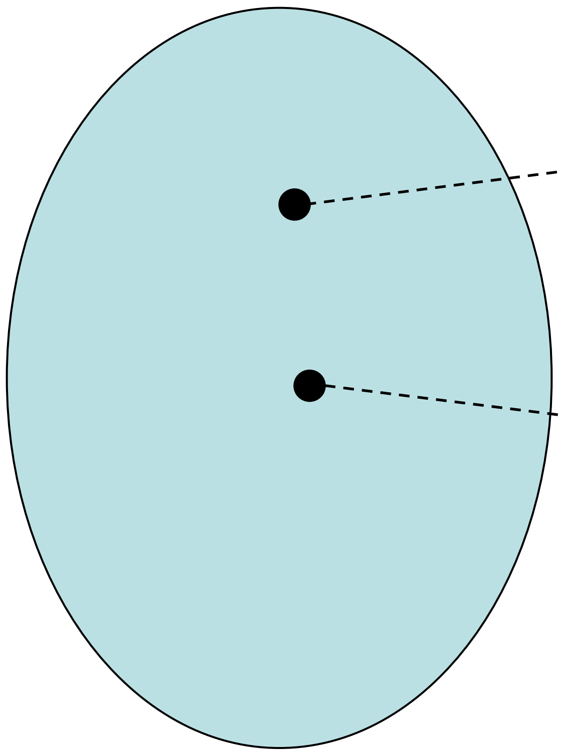
How to describe the states of an ideally controlled system?

(Basic rule I)

Example of a classical system

A particle on a 1D line





It is at 3.4 cm to the right of the origin and stands still.

It is at 2.3 cm to the left of the origin and moves to the right at 0.3 cm/sec.

Set of all the states

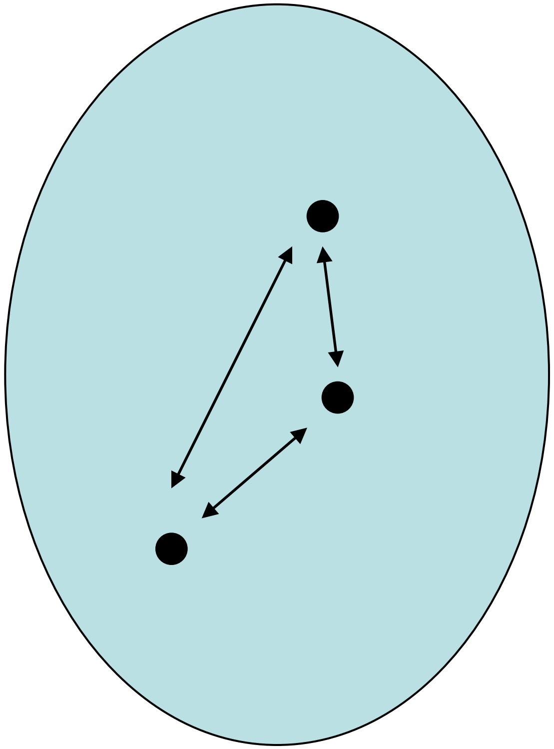
Is there any common structure in the set?

Relation between a pair of states?

Closeness?

How to describe the states of an ideally controlled system?

(Basic rule I)



Set of all the states

Quantum system

State A and State B may not be perfectly distinguishable.

Distinguishablity: Can be operationally defined.

Applicable to *any* system

Common structure

A quantity representing the distiguishablity is assigned to every pair of states.

Hilbert space

- Linear space over $\mathbb{C}$
- Inner product (a, b)
- Complete in the norm $||a|| \equiv \sqrt{(a, a)}$

$\mathbb{C}$: set of complex numbers

How to describe the states of an ideally controlled system?

(Basic rule I)

A physical system $\leftrightarrow$ a **Hilbert space** $\mathcal{H}$

A state $\leftrightarrow$ a **ray** in the Hilbert space
Usually, we use a normalized vector ϕ satisfying
$(\phi,\phi)=1$ as a representative of the ray.
(not unique: $\phi, -\phi, i\phi, \ldots$)

Distinguishability —— Inner product $\quad (\phi,\phi)=(\psi,\psi)=1$

$|(\phi,\psi)|=0$ Perfectly distinguishable

$0<|(\phi,\psi)|<1$ Partially distinguishable

$|(\phi,\psi)|=1$ Completely indistinguishable (the same state)

Dirac notation

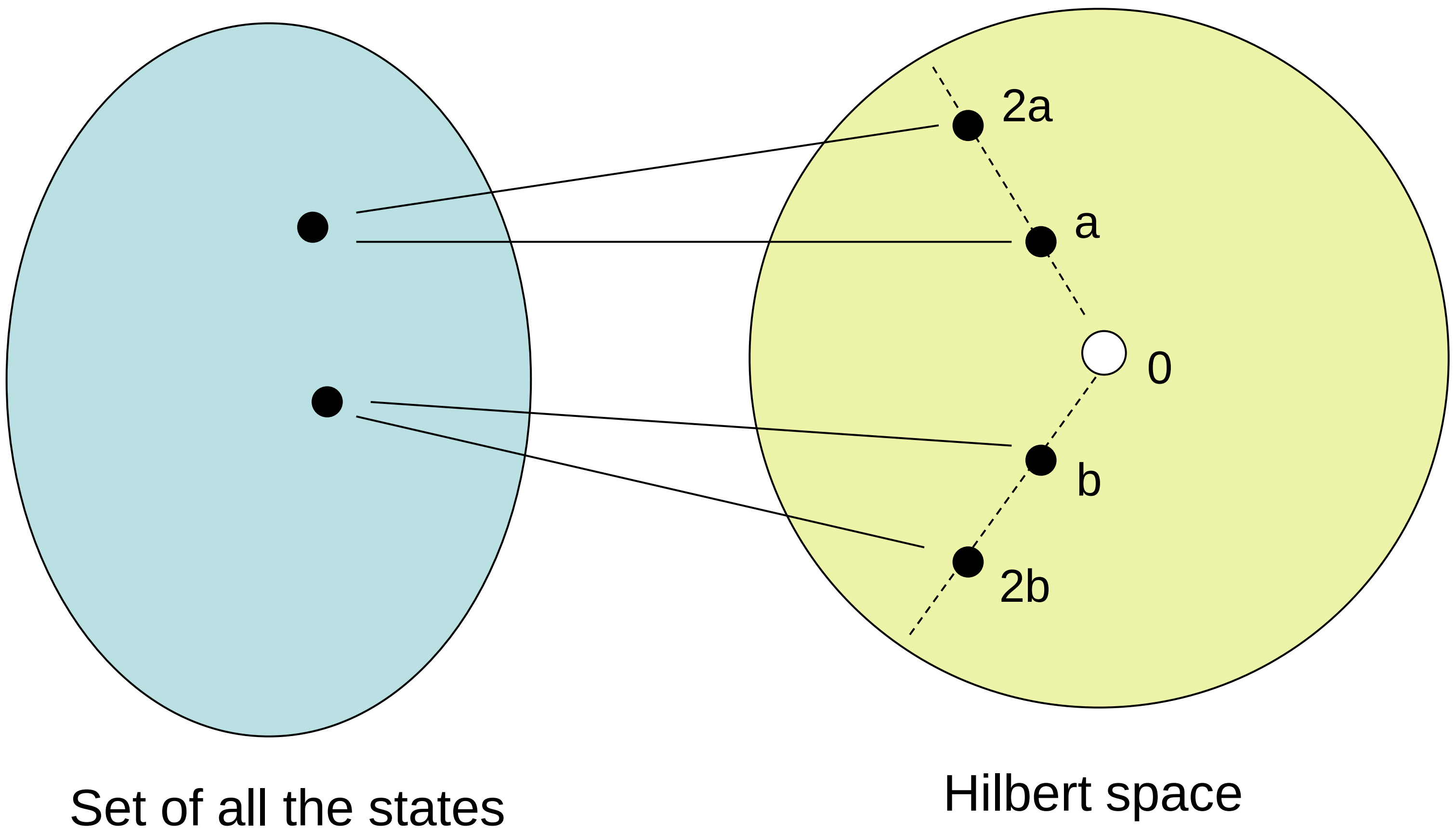
'ket' $|\phi\rangle$ — vector $\phi\in\mathcal{H}$.

'bra' $\langle\phi|$ — linear functional $(\phi,\cdot):\mathcal{H}\to\mathbb{C}$.

$\langle\phi|\psi\rangle$ — (ϕ,ψ)

How to describe the states of an ideally controlled system?

(Basic rule I)



A state $\leftrightarrow$ a **ray** in the Hilbert space

ray including vector $a \neq 0$ is

$\{\alpha a | \alpha \in \mathbb{C}, \alpha \neq 0\}$.

How to describe changes in an ideally controlled system?

(Basic rule II)

Reversible evolution

A unitary operator $\hat{U}$:

$|\phi_{\text{out}}\rangle = \hat{U}|\phi_{\text{in}}\rangle$

Inner products are preserved by unitary operations.

Distinguishability should never be improved by any operation.

↓

Distinguishability should be unchanged by any reversible operation.

↓

Inner products will be preserved in any reversible operation.

Infinitesimal change

$$|\phi(t_2)\rangle = \hat{U}(t_2, t_1)|\phi(t_1)\rangle$$

$$|\phi(t+dt)\rangle = \hat{U}(t+dt, t)|\phi(t)\rangle$$

$$\hat{U}(t+dt, t) \cong \hat{1} - (i/\hbar)\hat{H}(t)dt$$

Self-adjoint operator $\hat{H}(t)$:
Hamiltonian of the system

Schrödinger equation:

$$i\hbar\frac{d}{dt}|\phi(t)\rangle = \hat{H}(t)|\phi(t)\rangle$$

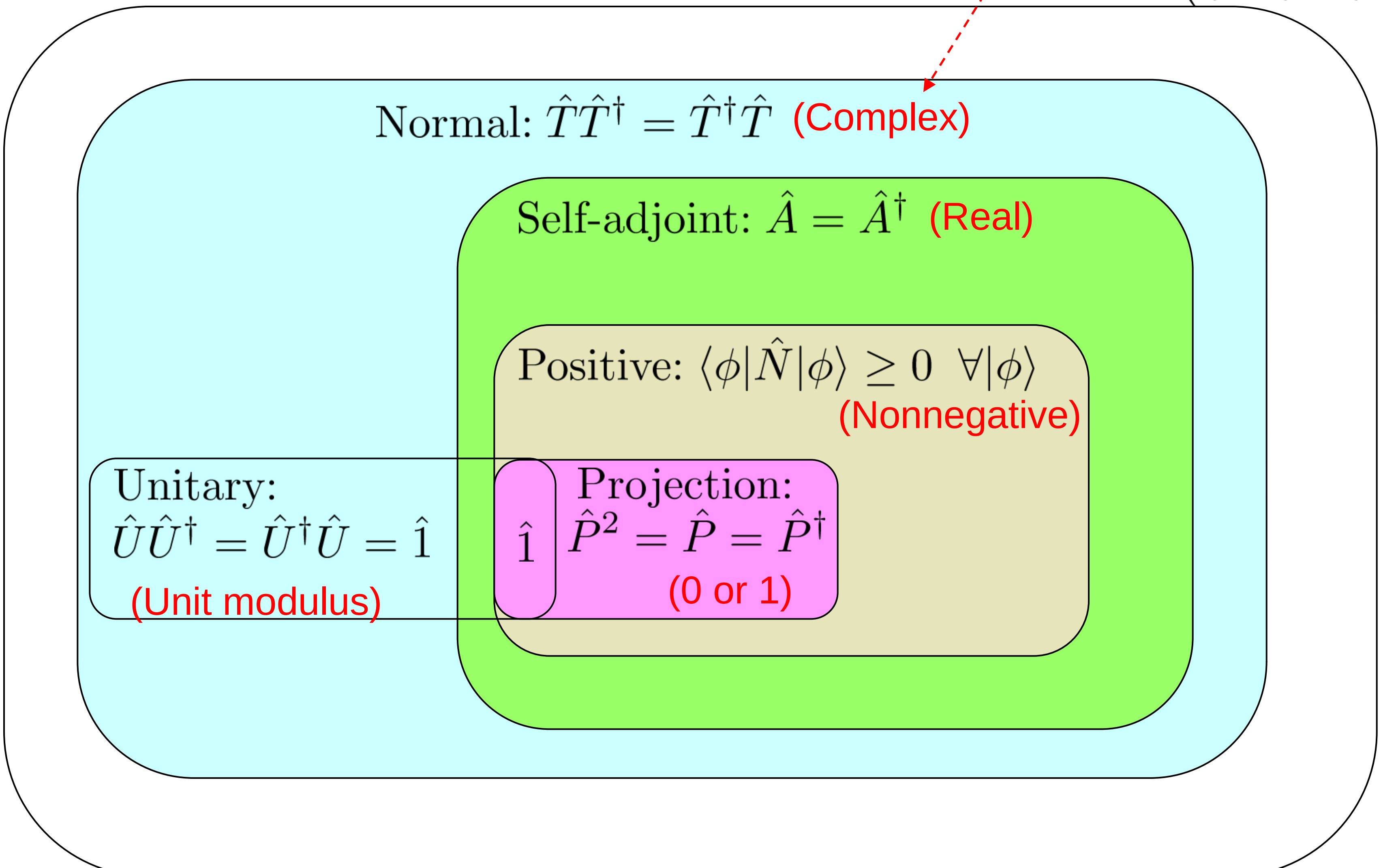
Classes of linear operators: $\mathcal{H} \to \mathcal{H}$

$\hat{T}$ is normal $\leftrightarrow$ $\hat{T}$ is diagonalizable.

An orthonormal basis

$$\hat{T} = \sum_j \lambda_j |u_j\rangle\langle u_j| = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \ddots \end{pmatrix}$$

Eigenvalues



How to describe measurements on an ideally controlled system?

(Basic rule III)

An ideal measurement with outcome $j = 1, \ldots, d$

For every j,

(1) There exists an input state $|a_j\rangle$ that produces outcome j with probability 1.

(2) ~~Any other state produces outcome j with probability 0.~~

(3) The number of outcomes d is maximal.

$\downarrow$

$\{|a_j\rangle\}_{j=1,\cdots,d}$ is an orthonormal basis of $\mathcal{H}$.

$$d = \dim \mathcal{H}.$$

Note: This is not the unique way of defining the 'best' measurement. We'll see later.

How to describe measurements on an ideally controlled system?

(Basic rule III)

Orthogonal measurement on an orthonormal basis $\{|a_j\rangle\}_{j=1,\cdots,d}$
(von Neumann measurement, projection measurement)

Input state $|\phi\rangle = \sum_j |a_j\rangle\langle a_j|\phi\rangle$

Closure relation

$\sum_j |a_j\rangle\langle a_j| = \hat{1}$

Probability of outcome j

$$P(j) = |\langle a_j|\phi\rangle|^2$$

Measurement of an observable

Self-adjoint operator $\hat{A}$

$$\hat{A} = \sum_j \lambda_j |a_j\rangle\langle a_j|$$

Measurement on $\{|a_j\rangle\}_{j=1,\cdots,d}$ Assign $j \to \lambda_j$

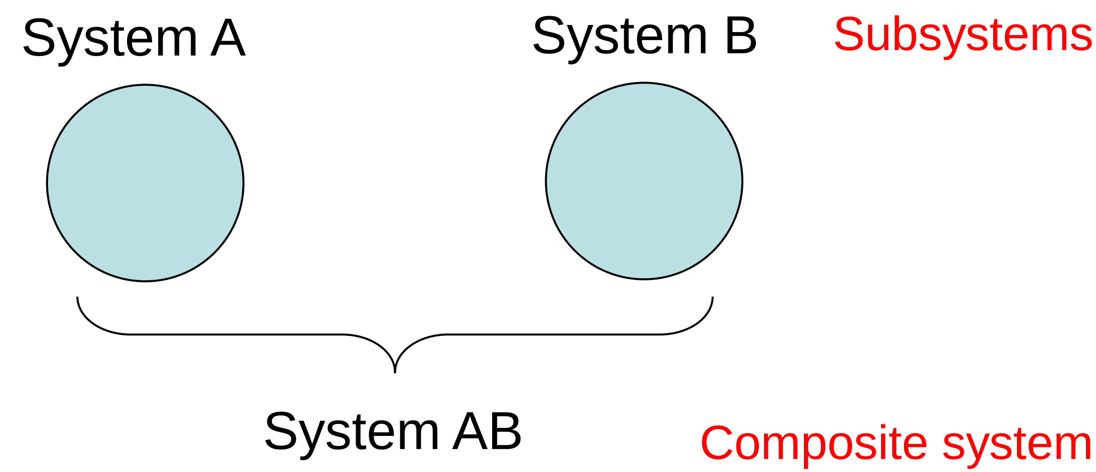
$$\langle\hat{A}\rangle \equiv \sum_j P(j)\lambda_j = \sum_j \langle\phi|a_j\rangle\langle a_j|\phi\rangle\lambda_j = \langle\phi|\hat{A}|\phi\rangle$$

How to treat composite systems?

(Basic rule IV)

We know how to describe each of the systems A and B.

How to describe AB as a single system?



System A: Hilbert space $\mathcal{H}_A$ Basis $\{|a_i\rangle\}_{i=1,\cdots,d_A}$

System B: Hilbert space $\mathcal{H}_B$ Basis $\{|b_j\rangle\}_{j=1,\cdots,d_B}$

Composite system AB:

Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$

Tensor product

Basis

$\{|a_i\rangle \otimes |b_j\rangle\}_{i=1,\cdots,d_A;j=1,\cdots,d_B}$

$$\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = \dim \mathcal{H}_A \dim \mathcal{H}_B$$

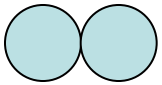
How to treat composite systems?

(Basic rule IV)

When system A and system B are independently accessed …

	State preparation	Unitary evolution	Orthogonal measurement
System A	$\vert\phi\rangle_A$	$\hat{U}_A$	$\{\vert a_i\rangle_A\}_{i=1,\cdots,d_A}$
System B	$\vert\psi\rangle_B$	$\hat{V}_B$	$\{\vert b_j\rangle_B\}_{j=1,\cdots,d_B}$
System AB	$\vert\phi\rangle_A \otimes \vert\psi\rangle_B$	$\hat{U}_A \otimes \hat{V}_B$	$\{\vert a_i\rangle_A \otimes \vert b_j\rangle_B\}_{i=1,\cdots,d_A}^{j=1,\cdots,d_B}$
	Separable states	Local unitary operations	Local measurements

When system A and system B are directly interacted …



State preparation	Unitary evolution	Orthogonal measurement
$\vert\Psi\rangle_{AB} \in \mathcal{H}_{AB}$	$\hat{U}_{AB} : \mathcal{H}_{AB} \to \mathcal{H}_{AB}$	$\{\vert\Psi_k\rangle_{AB}\}_{k=1,2,\ldots,d_A d_B}$
$\sum_k \alpha_k \vert\phi_k\rangle_A \otimes \vert\psi_k\rangle_B$		
Entangled states	Global unitary operations	Global measurements

2. State of a subsystem

Rule for a local measurement

State after discarding a subsystem (marginal state)

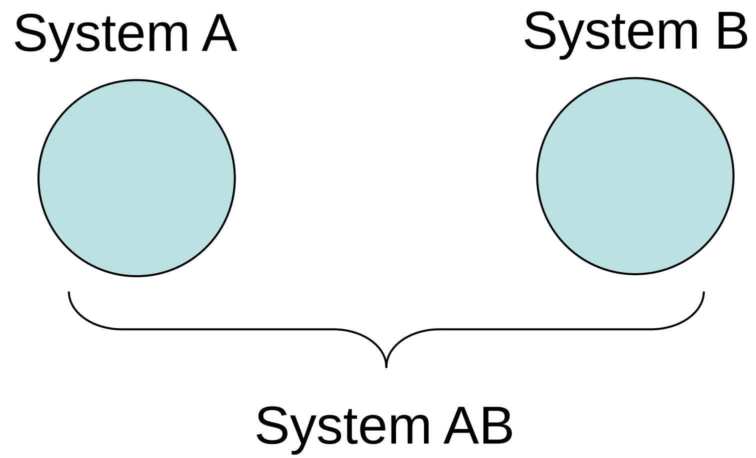
Density operator

- Properties of density operators
- Rules in terms of density operators

Why is the density operator sufficient for description ?

- Schmidt decomposition
- Pure states with the same marginal state
- Ensembles with the same density operator

Entanglement



state: $|\Phi\rangle_{AB}$

Suppose that the whole system (AB) is ideally controlled (prepared in a definite state).

Intuition in a 'classical' world:

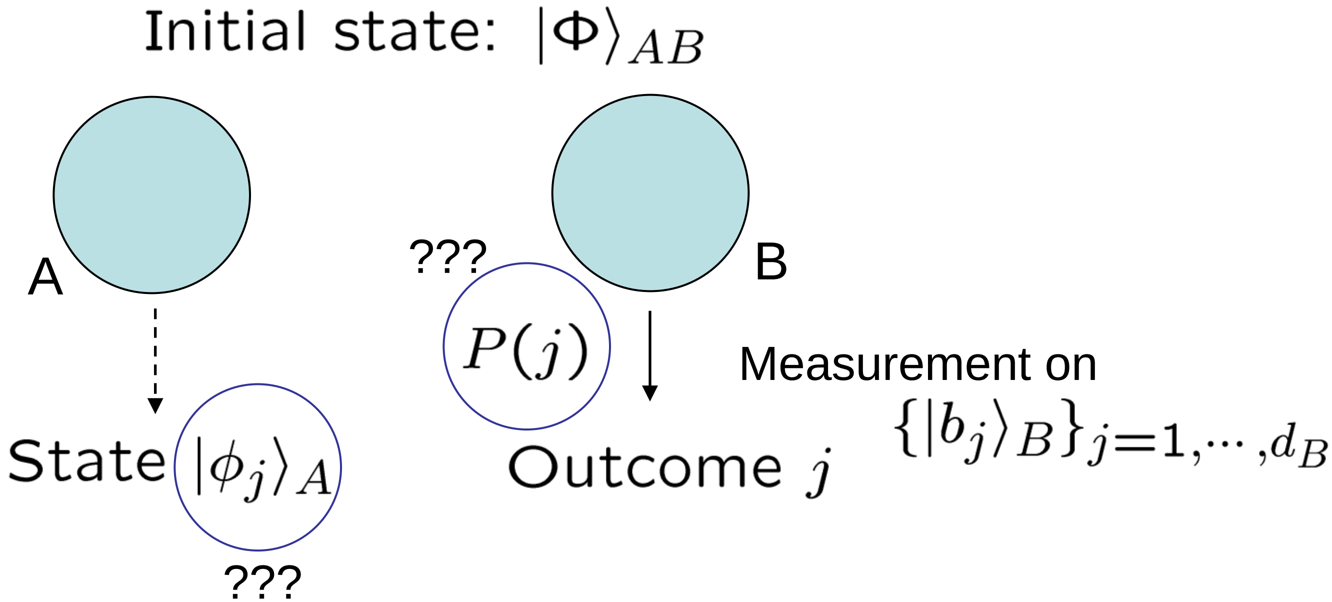
If the whole is under a good control, so are the parts.

But ….

It is not always possible to assign a state vector to subsystem A.

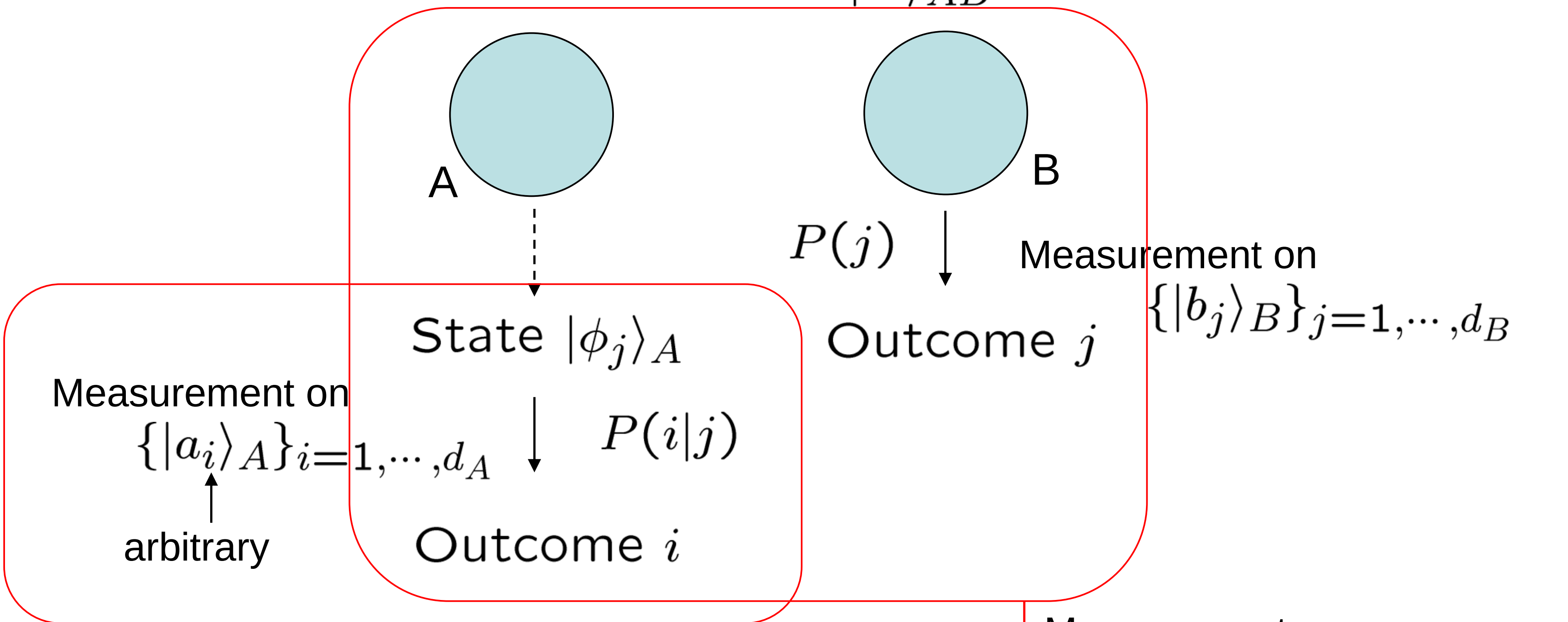
What is the state of subsystem A?

Rule for a local measurement



Rule for a local measurement

Initial state: $|\Phi\rangle_{AB}$



Measurement on $\{|a_i\rangle_A \otimes |b_j\rangle_B\}_{i=1,\cdots,d_A}^{j=1,\cdots,d_B}$

$$P(i|j) = |{}_A\langle a_i|\phi_j\rangle_A|^2$$

$$P(i,j) = \left|{}_A\langle a_i|{}_B\langle b_j||\Phi\rangle_{AB}\right|^2$$

$$P(i,j) = P(i|j)P(j) = |{}_A\langle a_i|\sqrt{P(j)}|\phi_j\rangle_A|^2$$

A remark on notations

$$ {}_A\langle a_i| \otimes {}_B\langle b_j||\Phi\rangle_{AB} $$

$$ = {}_A\langle a_i|\underbrace{(\hat{1}_A \otimes {}_B\langle b_j|)}|\Phi\rangle_{AB} $$

$$ \Big\downarrow \text{abbreviation} $$

$$ = {}_A\langle a_i| \; {}_B\langle b_j| \; |\Phi\rangle_{AB} $$

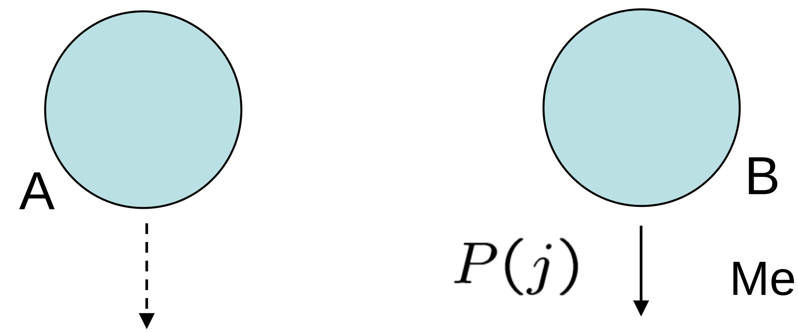
$$ \begin{matrix} {}_A\langle a_i| \\ {}_B\langle b_j| \end{matrix} \Big|\Phi\Big\rangle_{AB} $$

$$ \begin{matrix} {}_A\langle a_i| & \\ & {}_B\langle b_j| \end{matrix} \;\Big|\Phi\Big\rangle_{AB} $$

$$ \begin{aligned} {}_B\langle b_j| &: \mathcal{H}_B \to \mathbb{C} \\ \hat{1}_A &: \mathcal{H}_A \to \mathcal{H}_A \\ \hat{1}_A \otimes {}_B\langle b_j| &: \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \end{aligned} $$

Rule for a local measurement

Initial state: $|\Phi\rangle_{AB}$



Measurement on $\{|b_j\rangle_B\}_{j=1,\cdots,d_B}$

State $|\phi_j\rangle_A$

Outcome j

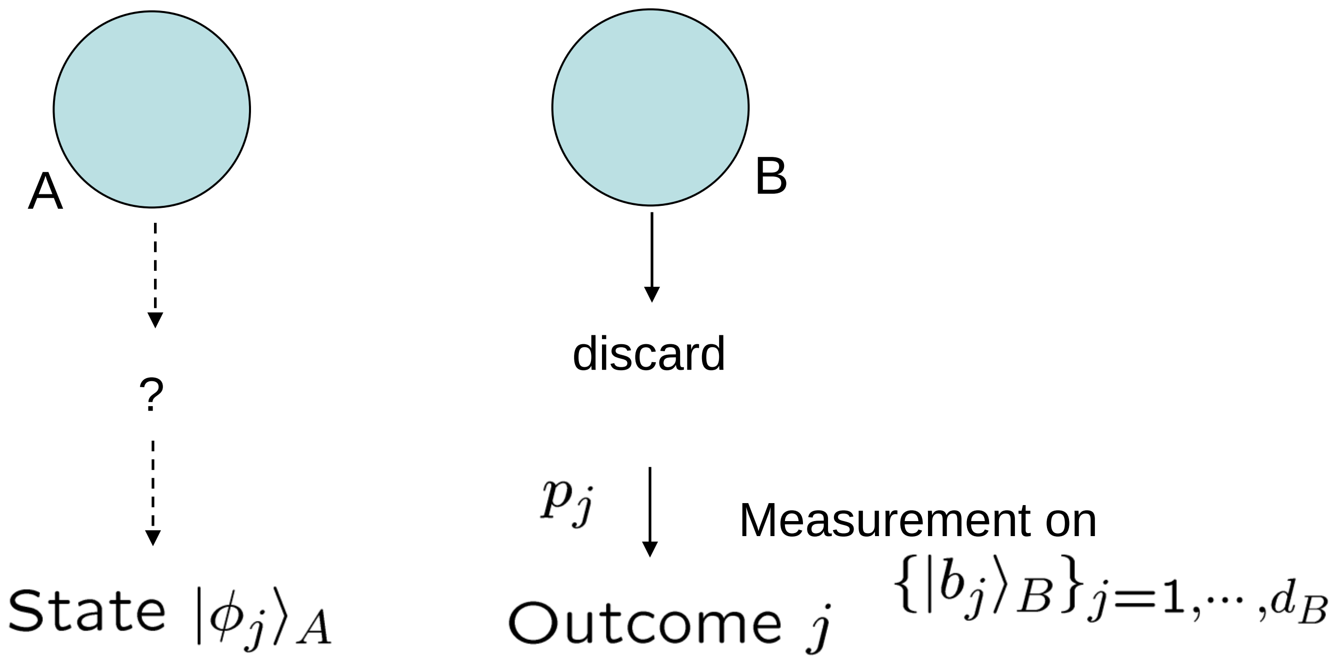
$$\boxed{\sqrt{P(j)}|\phi_j\rangle_A = {}_B\langle b_j||\Phi\rangle_{AB}}$$

$$P(j) = \|{}_B\langle b_j||\Phi\rangle_{AB}\|^2$$

$$|\phi_j\rangle_A = \frac{{}_B\langle b_j||\Phi\rangle_{AB}}{\|{}_B\langle b_j||\Phi\rangle_{AB}\|}$$

State after discarding a subsystem (marginal state)

Initial state: $|\Phi\rangle_{AB}$



State of system A: $|\phi_j\rangle_A$ with probability p_j $\longrightarrow$ $\{p_j, |\phi_j\rangle_A\}$

$$\sqrt{p_j}|\phi_j\rangle_A = {}_B\langle b_j||\Phi\rangle_{AB}$$

This description is correct, but dependence on the fictitious measurement is weird…

Example

$\{|0\rangle, |1\rangle\}$: an orthonormal basis

$\{|+\rangle, |-\rangle\}$: an orthonormal basis

$$|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

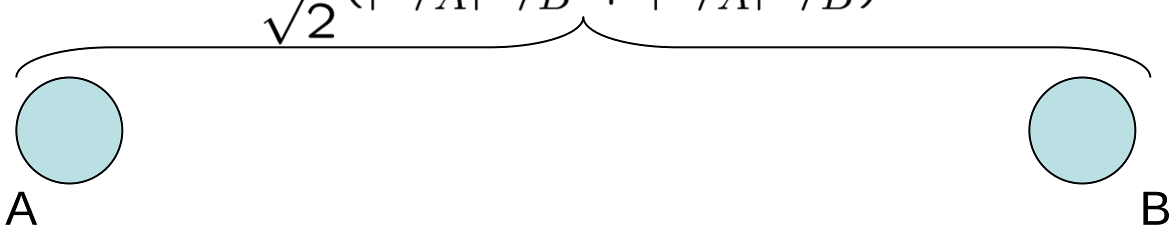
$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

measurement

50% 50%

$\{|0\rangle_A, |1\rangle_A\} \longleftarrow \{|0\rangle_B, |1\rangle_B\}$

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$



measurement

50% 50%

$\{|+\rangle_A, |-\rangle_A\} \longleftarrow \{|+\rangle_B, |-\rangle_B\}$

Alternative description: density operator

$\{p_j, |\phi_j\rangle_A\}$ $\quad$ $|\phi_j\rangle_A$ with probability p_j

$$\hat{\rho}_A \equiv \sum_j p_j |\phi_j\rangle_{AA}\langle\phi_j|$$

Cons

$$\left.\begin{array}{l}\{q_k, |\psi_k\rangle_A\} \\ \{p_j, |\phi_j\rangle_A\}\end{array}\right\} \rightarrow \text{Same } \hat{\rho}_A$$

Two different physical states could have the same density operator.
(The description could be insufficient.)

Pros

$$\sqrt{p_j}|\phi_j\rangle_A = {}_B\langle b_j||\Phi\rangle_{AB}$$

$$\hat{\rho}_A = \sum_j p_j |\phi_j\rangle_{AA}\langle\phi_j| = \sum_j \sqrt{p_j}|\phi_j\rangle_{AA}\langle\phi_j|\sqrt{p_j}$$

$$= \sum_j {}_B\langle b_j||\Phi\rangle\langle\Phi||b_j\rangle_B = \mathrm{Tr}_B(|\Phi\rangle\langle\Phi|)$$

Independent of the choice of the fictitious measurement

Example

$\{|0\rangle, |1\rangle\}$: an orthonormal basis

$\{|+\rangle, |-\rangle\}$: an orthonormal basis

$$|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

A

$$\boxed{\hat{\rho}_A = \frac{1}{2}|0\rangle_{AA}\langle 0| + \frac{1}{2}|1\rangle_{AA}\langle 1|}$$

B

50% 50%

$\{|0\rangle_A, |1\rangle_A\}$ ← measurement $\{|0\rangle_B, |1\rangle_B\}$

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

A

$$\boxed{\hat{\rho}_A = \frac{1}{2}|+\rangle_{AA}\langle +| + \frac{1}{2}|-\rangle_{AA}\langle -|}$$

B

50% 50%

$\{|+\rangle_A, |-\rangle_A\}$ ← measurement $\{|+\rangle_B, |-\rangle_B\}$

Properties of density operators

$$\hat{\rho} \equiv \sum_j p_j |\phi_j\rangle\langle\phi_j|$$

For any $|\psi\rangle$, $\langle\psi|\hat{\rho}|\psi\rangle = \sum_j p_j |\langle\psi|\phi_j\rangle|^2 \geq 0$ Positive

$$\mathrm{Tr}(\hat{\rho}) = \sum_j p_j \mathrm{Tr}(|\phi_j\rangle\langle\phi_j|)$$
$$= \sum_j p_j \langle\phi_j|\phi_j\rangle = \sum_j p_j = 1$$ Unit trace

Positive & Unit trace $\longrightarrow$ $\hat{\rho} = \sum_j \underbrace{p_j}_{\text{probability}} |\phi_j\rangle\langle\phi_j|$

This decomposition is by no means unique!

Pure state $\hat{\rho} = |\phi\rangle\langle\phi|$

Mixed state $\hat{\rho} = \sum_j p_j |\phi_j\rangle\langle\phi_j|$

Maximally mixed state: $\hat{\rho} = \frac{1}{d}\hat{1}$ $\quad (d = \dim \mathcal{H})$

(=The state after random unitary operation)

Range and kernel

Range and kernel of an operator $\hat{T} : \mathcal{H} \to \mathcal{H}$

$$\mathrm{Ran}\ \hat{T} \equiv \{\hat{T}|x\rangle \ \mid\ |x\rangle \in \mathcal{H}\}$$ (A subspace of $\mathcal{H}$)

$$\mathrm{Ker}\ \hat{T} \equiv \{|x\rangle \in \mathcal{H} \ \mid\ \hat{T}|x\rangle = 0\}$$ (A subspace of $\mathcal{H}$)

$$\mathrm{Rank}(\hat{T}) \equiv \dim \mathrm{Ran}\ \hat{T}$$

$\hat{\rho}$: positive operator $\quad \hat{\rho} = \sum_j p_j |\phi_j\rangle\langle\phi_j| \quad (p_j > 0)$

$\mathrm{Ran}\ \hat{\rho}$: Subspace spanned by $\{|\phi_j\rangle\}$

Subspace in which $\hat{\rho} > 0$

$\mathrm{Ker}\ \hat{\rho}$: Subspace orthogonal to $\mathrm{Ran}\ \hat{T}$

Subspace in which $\hat{\rho} = 0$

$$\mathcal{H} = (\mathrm{Ran}\ \hat{\rho}) \oplus (\mathrm{Ker}\ \hat{\rho})$$

$\mathrm{Rank}(\hat{\rho})$ Number of the nonzero eigenvalues of $\hat{\rho}$

Pure state $\quad \mathrm{Rank}(\hat{\rho}) = 1$

Mixed state $\quad \mathrm{Rank}(\hat{\rho}) \geq 2$

Rules in terms of density operators

Prepare $|\phi_j\rangle$ with probability p_j

$$\hat{\rho} \equiv \sum_j p_j |\phi_j\rangle\langle\phi_j|$$

Prepare $\hat{\rho}_j$ with probability p_j

$$\hat{\rho} = \sum_j p_j \hat{\rho}_j$$

Unitary evolution

$$|\phi_{\text{out}}\rangle = \hat{U}|\phi_{\text{in}}\rangle$$

Hint: $|\phi_{\text{out}}\rangle\langle\phi_{\text{out}}| = \hat{U}|\phi_{\text{in}}\rangle\langle\phi_{\text{in}}|\hat{U}^\dagger$

$$\hat{\rho}_{\text{out}} = \hat{U}\hat{\rho}_{\text{in}}\hat{U}^\dagger$$

Orthogonal measurement on basis $\{|a_j\rangle\}$

$$P(j) = |\langle a_j|\phi\rangle|^2$$

Hint: $P(j) = \langle a_j|\phi\rangle\langle\phi|a_j\rangle$

$$P(j) = \langle a_j|\hat{\rho}|a_j\rangle$$

Expectation value of an observable $\hat{A}$

$$\langle\hat{A}\rangle = \langle\phi|\hat{A}|\phi\rangle$$

$$\langle\hat{A}\rangle = \text{Tr}(\hat{A}\hat{\rho})$$

Hint: $\langle\hat{A}\rangle = \text{Tr}(\hat{A}|\phi\rangle\langle\phi|)$

Rules in terms of density operators

Independently prepared systems A and B

$$|\Psi\rangle_{AB} = |\phi\rangle_A \otimes |\psi\rangle_B \qquad \hat{\rho}_{AB} = \hat{\rho}_A \otimes \hat{\rho}_B$$

Local measurement on system B on basis $\{|b_j\rangle_B\}$

$$\sqrt{p_j}|\phi_j\rangle_A = {}_B\langle b_j||\Phi\rangle_{AB} \qquad p_j\hat{\rho}_A^{(j)} = {}_B\langle b_j|\hat{\rho}_{AB}|b_j\rangle_B$$

Discarding system B

$$\hat{\rho}_A = \mathsf{Tr}_B(|\Phi\rangle\langle\Phi|) \qquad \hat{\rho}_A = \mathsf{Tr}_B[\hat{\rho}_{AB}]$$

All the rules so far can be written in terms of density operators.

Which is the better description?

$\{p_j, |\phi_j\rangle\}$

This looks natural. The system is in one of the pure states, but we just don't know. Quantum mechanics may treat just the pure states, and leave mixed states to statistical mechanics or probability theory.

$\widehat{\rho} \equiv \sum_j p_j |\phi_j\rangle\langle\phi_j|$ *Best description*

All the rules so far can be written in terms of density operators.

Which description has one-to-one correspondence to physical states?

Theorem: Two states $\{p_j, |\phi_j\rangle\}$ and $\{q_k, |\psi_k\rangle\}$ with the same density operator are physically indistinguishable (hence are the same state).

Schmidt decomposition

Bipartite pure states have a very nice standard form.

Any orthonormal basis $\{|a_i\rangle_A\}$ $\{|b_j\rangle_B\}$

$$|\Phi\rangle_{AB} = \sum_{ij} \alpha_{ij} |a_i\rangle_A |b_j\rangle_B$$

We can always choose the two bases such that

$$|\Phi\rangle_{AB} = \sum_{i} \sqrt{p_i} |a_i\rangle_A |b_i\rangle_B$$

Schmidt decomposition

$\{|a_i\rangle_A\}$: Any basis that diagonalizes $\hat{\rho}_A \equiv \mathrm{Tr}_B |\Phi\rangle\langle\Phi| = \sum_i p_i |a_i\rangle_{AA}\langle a_i|$

Proof: $$|\Phi\rangle_{AB} = \sum_i |a_i\rangle_{AA}\langle a_i||\Phi\rangle_{AB} = \sum_i |a_i\rangle_A |\tilde{b}_i\rangle_B$$

$|\tilde{b}_i\rangle_B \equiv {}_A\langle a_i||\Phi\rangle_{AB}$

(unnormalized)

$$\begin{aligned}
{}_B\langle \tilde{b}_j|\tilde{b}_i\rangle_B &= {}_{AB}\langle\Phi||a_j\rangle_A \; {}_A\langle a_i||\Phi\rangle_{AB} \\
&= \mathrm{Tr}\left[{}_A\langle a_i||\Phi\rangle_{AB} \; {}_{AB}\langle\Phi||a_j\rangle_A\right] \\
&= {}_A\langle a_i|\mathrm{Tr}_B\left[|\Phi\rangle_{AB} \; {}_{AB}\langle\Phi|\right]|a_j\rangle_A \\
&= {}_A\langle a_i|\hat{\rho}_A|a_j\rangle_A = p_j \delta_{i,j}
\end{aligned}$$

$\sqrt{p_j}|b_j\rangle_B \equiv |\tilde{b}_j\rangle_B$

Entangled states and separable states

$|\phi\rangle_A \otimes |\psi\rangle_B$ $\sum_k \alpha_k |\phi_k\rangle_A \otimes |\psi_k\rangle_B$

Separable states Entangled states

Are there any procedure to distinguish between the two classes?

$\longrightarrow$ Schmidt decomposition $$|\Phi\rangle_{AB} = \sum_{i=1}^{s} \sqrt{p_i} |a_i\rangle_A |b_i\rangle_B$$

$$p_1 \geq p_2 \geq \cdots \geq p_s > 0$$

Schmidt number

Number of nonzero coefficients in Schmidt decomposition

= The rank of the marginal density operators

$\{p_j\}$: The eigenvalues of the marginal density operators (the same for A and B)

'Symmetry' between A and B

$\hat{\rho}_A, \hat{\rho}_B$ The same set of eigenvalues

$$s = \mathrm{Rank}(\hat{\rho}_A) = \mathrm{Rank}(\hat{\rho}_B)$$

Separable states Schmidt number = 1

$p_1 = 1$

Entangled states Schmidt number > 1

$p_1 \geq p_2 > 0$

Maximally entangled states (MES)

$$\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$$

Orthonormal bases $\{|k\rangle_A\}_{k=1,2,\ldots,d}$ $\{|k\rangle_B\}_{k=1,2,\ldots,d}$

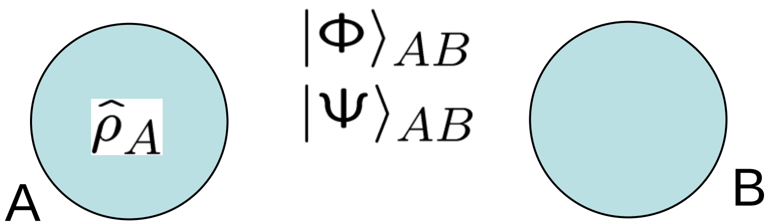
Maximally entangled state $$\sum_{k=1}^{d} \frac{1}{\sqrt{d}} |k\rangle_A \otimes |k\rangle_B$$

$$\hat{\rho}_A = \frac{1}{d}\hat{1}_A \quad \hat{\rho}_B = \frac{1}{d}\hat{1}_B$$

The marginal states are maximally mixed.

(MES with Schmidt number s : $\sum_{i=1}^{s} \frac{1}{\sqrt{s}} |k\rangle_A |k\rangle_B$)

Pure states with the same marginal state



$$\hat{\rho}_A = \mathrm{Tr}_B(|\Phi\rangle\langle\Phi|)$$
$$\hat{\rho}_A = \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|)$$

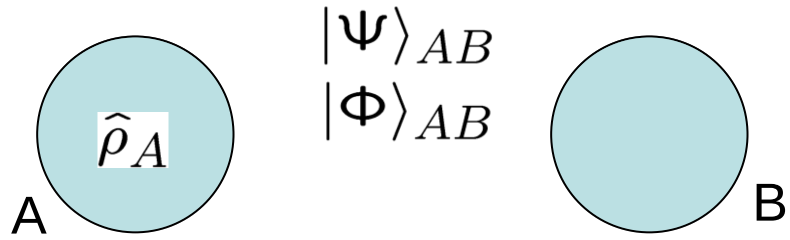
$|\Phi\rangle_{AB} \longrightarrow \hat{\rho}_A$ Marginal state (unique)

$\hat{\rho}_A \longrightarrow |\Phi\rangle_{AB}$, $\hat{\rho}_A \longrightarrow |\Psi\rangle_{AB}$ Purification
Pure extension (not unique)

$$\boxed{|\Phi\rangle_{AB} = (\hat{1}_A \otimes \hat{U}_B)|\Psi\rangle_{AB}}$$

Theorem: If $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ are purifications of the same state $\hat{\rho}_A$, state $|\Psi\rangle_{AB}$ can be physically converted to state $|\Phi\rangle_{AB}$ without touching system A.

Pure states with the same marginal state



$$\hat{\rho}_A = \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|) = \mathrm{Tr}_B(|\Phi\rangle\langle\Phi|)$$

Proof:

Orthonormal basis $\{|a_i\rangle_A\}$ that diagonalizes $\hat{\rho}_A$

Schmidt decomposition

$$|\Psi\rangle_{AB} = \sum_i \sqrt{p_i}|a_i\rangle_A|\mu_i\rangle_B$$

$$|\Phi\rangle_{AB} = \sum_i \sqrt{p_i}|a_i\rangle_A|\nu_i\rangle_B$$

$\{|\mu_i\rangle_B\}$ Orthonormal basis

$\{|\nu_i\rangle_B\}$ Orthonormal basis

$$|\nu_i\rangle_B = \hat{U}_B|\mu_i\rangle_B$$

unitary $\hat{U}_B = \sum_i |\nu_i\rangle_{BB}\langle\mu_i|$

$$|\Phi\rangle_{AB} = (\hat{1}_A \otimes \hat{U}_B)|\Psi\rangle_{AB}$$

Properties of MES (I): Local interconvertibility

All maximally entangled states have the same marginal state.

$$|\Theta\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |a_j\rangle_A |b_j\rangle_B \quad \Rightarrow \quad \rho_A = \frac{1}{d} \sum_{j=1}^{d} |a_j\rangle_{AA}\langle a_j| = \frac{1}{d} \hat{1}_A$$

$$|\Theta'\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |a'_j\rangle_A |b'_j\rangle_B \quad \Rightarrow \quad \rho_A = \frac{1}{d} \sum_{j=1}^{d} |a'_j\rangle_{AA}\langle a'_j| = \frac{1}{d} \hat{1}_A$$

$$|\Theta\rangle_{AB} = (\hat{1}_A \otimes \hat{U}_B)|\Theta'\rangle_{AB}$$

$$|\Theta\rangle_{AB} = (\hat{V}_A \otimes \hat{1}_B)|\Theta'\rangle_{AB}$$

They can be converted to one another by only accessing one of the subsystems.

Purification of $\hat{\rho}_A$ is not unique, but there is a simple way to write down all of them.

$$|\Phi\rangle_{AB} \equiv \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle_A |j\rangle_B$$

$|\Phi_\rho\rangle_{AB} \equiv \sqrt{d}(\sqrt{\hat{\rho}_A} \otimes \hat{1}_B)|\Phi\rangle_{AB}$ is a purification of $\hat{\rho}_A$

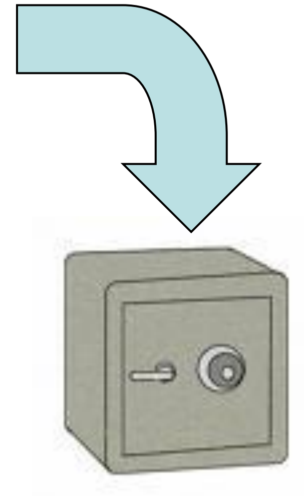
$$\mathrm{Tr}_B |\Phi_\rho\rangle\langle\Phi_\rho| = d\sqrt{\hat{\rho}_A}\left(\mathrm{Tr}_B|\Phi\rangle\langle\Phi|\right)\sqrt{\hat{\rho}_A} = \hat{\rho}_A$$

Any purification can be written as $\sqrt{d}(\sqrt{\hat{\rho}_A} \otimes \hat{U}_B)|\Phi\rangle_{AB}$

<u>Sealed move</u>　(封じ手)

Chess, Go, Shogi …

Bb5
4六銀



Let us call it a day and shall we start over tomorrow, with Bob's move.

While they are (suppose to be) sleeping...

- Alice should not learn the sealed move.
- Bob should not alter the sealed move.

Sealed move

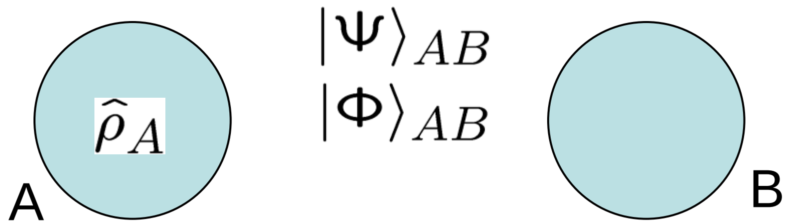
$|\Psi\rangle_{AB}$ Bb5 4六銀

$|\Phi\rangle_{AB}$ Pd5 3七角

- Alice should not learn the sealed move.
- Bob should not alter the sealed move.

If there is no reliable safe available …

(If there is no system out of both Alice's and Bob's reach …)



Alice has no knowledge

$\downarrow$

Bob can alter the states

$$\hat{\rho}_A = \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|) = \mathrm{Tr}_B(|\Phi\rangle\langle\Phi|)$$

$$\boxed{|\Phi\rangle_{AB} = (\hat{1}_A \otimes \hat{U}_B)|\Psi\rangle_{AB}}$$

Function of the "safe" cannot be realized.

Impossibility of unconditionally secure quantum bit commitment

(Lo, Mayers)

Ensembles with the same density operator

$\{p_j, |\phi_j\rangle_A\}$ $\qquad$ $|\phi_j\rangle_A$ with probability p_j

$\{q_k, |\psi_k\rangle_A\}$ $\qquad$ $|\psi_k\rangle_A$ with probability q_k

$$\hat{\rho}_A \equiv \sum_j p_j |\phi_j\rangle_{AA}\langle\phi_j| = \sum_k q_k |\psi_k\rangle_{AA}\langle\psi_k|$$

A scheme to realize the ensemble $\{p_j, |\phi_j\rangle_A\}$

Prepare system AB in state

$$|\Phi\rangle_{AB} \equiv \sum_j \sqrt{p_j}|\phi_j\rangle_A |b_j\rangle_B$$

$\{|b_j\rangle_B\}$ Orthonormal basis

$$\hat{\rho}_A = \mathrm{Tr}_B(|\Phi\rangle\langle\Phi|)$$

Measure system B on basis $\{|b_j\rangle_B\}$

$$\sqrt{p_j}|\phi_j\rangle_A = {}_B\langle b_j||\Phi\rangle_{AB}$$

$|\phi_j\rangle_A$ with probability p_j

Ensembles with the same density operator

Prepare system AB in state

$$|\Psi\rangle_{AB} \equiv \sum_k \sqrt{q_k}|\psi_k\rangle_A|b_k\rangle_B$$

Apply unitary operation $\widehat{U}_B$ to system B

$$|\Phi\rangle_{AB} \equiv \sum_j \sqrt{p_j}|\phi_j\rangle_A|b_j\rangle_B$$

Measure system B on basis $\{|b_j\rangle_B\}$

$|\phi_j\rangle_A$ with probability p_j

$\{p_j, |\phi_j\rangle_A\}$

$$|\Psi\rangle_{AB} \equiv \sum_k \sqrt{q_k}|\psi_k\rangle_A|b_k\rangle_B$$

Measure system B on basis $\{|b_k\rangle_B\}$

$|\psi_k\rangle_A$ with probability q_k

$\{q_k, |\psi_k\rangle_A\}$

$$\widehat{\rho}_A = \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|) = \mathrm{Tr}_B(|\Phi\rangle\langle\Phi|)$$

$$|\Phi\rangle_{AB} = (\widehat{1}_A \otimes \widehat{U}_B)|\Psi\rangle_{AB}$$

Example

Recipe I: $\{p_j, |\phi_j\rangle_A\}$ $p_0 = p_1 = \frac{1}{2},\ |\phi_0\rangle_A = |0\rangle_A, |\phi_1\rangle_A = |1\rangle_A$

Recipe II: $\{q_k, |\psi_k\rangle_A\}$ $q_0 = q_1 = \frac{1}{2},\ |\psi_0\rangle_A = |+\rangle_A, |\psi_1\rangle_A = |-\rangle_A$

$$\frac{1}{2}|0\rangle_{AA}\langle 0| + \frac{1}{2}|1\rangle_{AA}\langle 1| = \frac{1}{2}|+\rangle_{AA}\langle +| + \frac{1}{2}|-\rangle_{AA}\langle -| = \frac{1}{2}\hat{1}$$

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \xrightarrow[\{|0\rangle_B, |1\rangle_B\}]{\text{measurement}} \text{Recipe I:}$$

$$\Big\downarrow\ \hat{U} = |+\rangle_{BB}\langle 0| + |-\rangle_{BB}\langle 1|$$

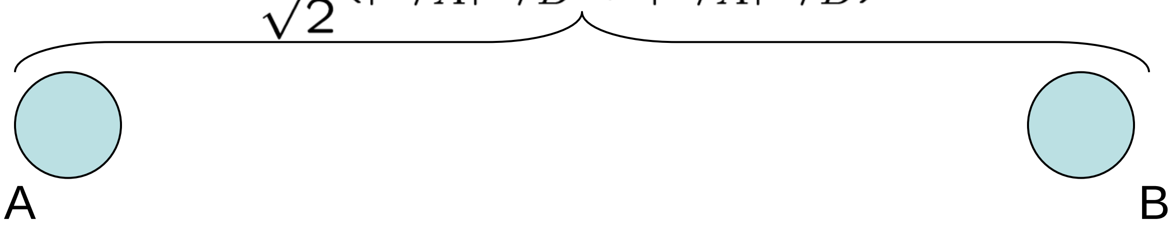
$$\frac{1}{\sqrt{2}}(|0\rangle_A|+\rangle_B + |1\rangle_A|-\rangle_B)$$

$$||$$

$$\frac{1}{\sqrt{2}}(|+\rangle_A|0\rangle_B + |-\rangle_A|1\rangle_B) \xrightarrow[\{|0\rangle_B, |1\rangle_B\}]{\text{measurement}} \text{Recipe II:}$$

Example

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$



B measurement

50% 50%

$\{|0\rangle_A, |1\rangle_A\}$ ⟵ - - - - - - $\{|0\rangle_B, |1\rangle_B\}$

(Recipe I)

50% 50%

$\{|+\rangle_A, |-\rangle_A\}$ ⟵ - - - - - - $\{|+\rangle_B, |-\rangle_B\}$

(Recipe II)

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \xrightarrow[\{|0\rangle_B, |1\rangle_B\}]{\text{measurement}} \text{Recipe I:}$$

$$\langle 0|\hat{U} = \langle +|$$
$$\langle 1|\hat{U} = \langle -|$$

$$\Big\downarrow \; \hat{U} = |+\rangle_{BB}\langle 0| \; + \; |-\rangle_{BB}\langle 1|$$

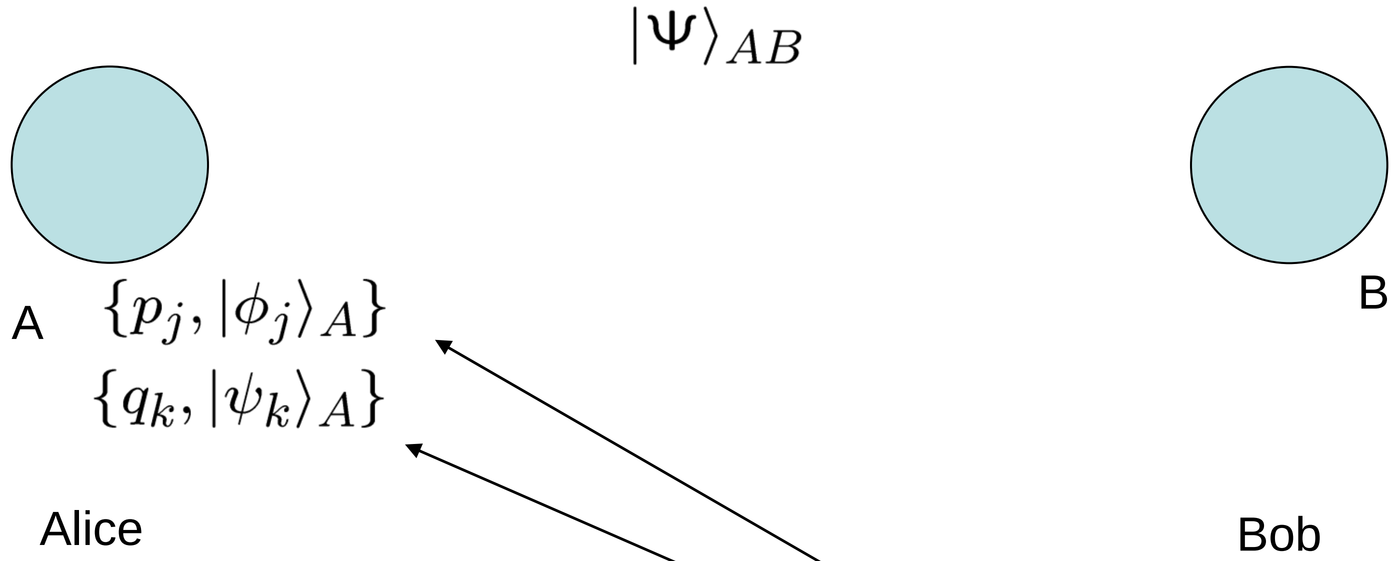
$$\frac{1}{\sqrt{2}}(|0\rangle_A|+\rangle_B + |1\rangle_A|-\rangle_B)$$

$$||$$

$$\frac{1}{\sqrt{2}}(|+\rangle_A|0\rangle_B + |-\rangle_A|1\rangle_B) \xrightarrow[\{|0\rangle_B, |1\rangle_B\}]{\text{measurement}} \text{Recipe II:}$$

measurement $\{|+\rangle_B, |-\rangle_B\}$

Ensembles with the same density operator



Can Alice distinguish the two states even partially?

NO!

Bob can remotely decide which of the states the system A is in.

Bob can postpone his decision indefinitely.

Theorem: Two states $\{p_j, |\phi_j\rangle\}$ and $\{q_k, |\psi_k\rangle\}$ with the same density operator are physically indistinguishable (hence are the same state).

Density operator

$\updownarrow$ One-to-one

Physical state