THE UNIVERSITY of EDINBURGH
informatics

Quantum Cyber Security

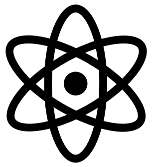
Lecture 4: Quantum Information Part II

Mina Doosti

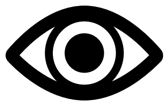
Overview

What do we want to learn in the next four lectures?

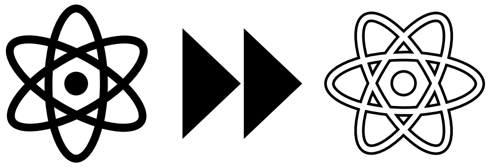
- Understanding the mathematics of quantum states or
  What's the most general way to describe quantum systems?
- Learning about quantum measurements and their most general mathematical description
- Learning about quantum operations and their most general mathematical description and their properties
- Learning some specific properties of quantum information and some basic concepts in information theory



Describe



Observe



Evolve

As a carrier of Information

Quantum system beyond one qubit

One qubit state lives in a Hilbert space of dimension 2 $|\psi\rangle \in \mathcal{H}$

A complex-valued vector in $\mathcal{H}$ (or $\mathcal{H}^2$) $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ complex

What if we have a larger system? How do we describe it?

Higher dimension: You can also have a d-dimensional vector in a d-dimensional Hilbert space

$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \in \mathcal{H}^3 \quad d=3$ $\qquad |\phi\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ 1 \\ 1 \end{pmatrix} \in \mathcal{H}^4 \quad d=4$

We can also have n qubits

The state of a n-qubit system lives in 2^n dimensional Hilbert space ($d = 2^n$). (why?)

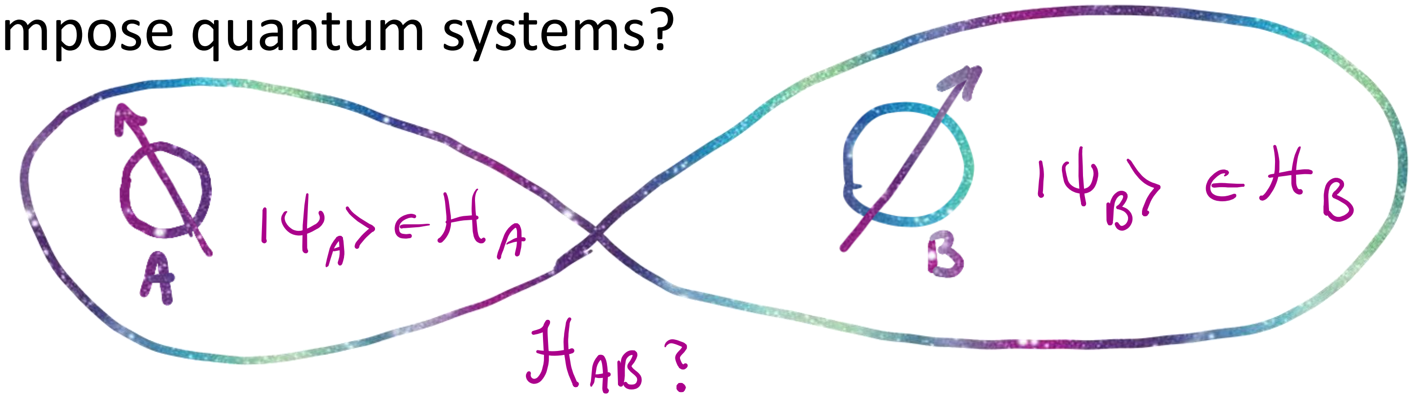
Ok, so far, we have the first postulate of quantum mechanics!

But if we have n qubit (let's say 2) they each have their own quantum state as well…

so how do we talk about them?

Composite systems

How to compose quantum systems?



Two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ can form a new Hilbert space $\mathcal{H}_{AB}$ which includes vectors that describes both system A and B

$$\dim \mathcal{H}_{AB} = \dim \mathcal{H}_A \times \dim \mathcal{H}_B$$

Its basis is built from basis of $\mathcal{H}_A$ and $\mathcal{H}_B$

How? By tensor product $\mathcal{H}_A \otimes \mathcal{H}_B = \mathcal{H}_{AB}$

We can compose vector spaces by tensor product.

Tensor product of vector spaces

Tensor product definition:

Let V and W be two vector spaces with dim m and n. The tensor product $V \otimes W$ of these vector spaces is a vector space of dimension $m \times n$ to which is associated a bilinear map that maps a pair $(v, w), v \in V, w \in W$ to an element of $V \otimes W$ denoted as $v \otimes w$.

Let $|i\rangle$ and $|j\rangle$ be an orthonormal bases for V and W respectively. Then $|i\rangle \otimes |j\rangle$ is an orthonormal basis for $V \otimes W$, i.e. $|\psi\rangle = \sum_{ij} \psi_{ij} |i\rangle \otimes |j\rangle$

Matrix representation:

$$A \otimes B = \sum_{ijkl} c_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l|$$

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}$$

Tensor product examples

Example with Dirac notation:

1) $|0\rangle \otimes |+\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}[|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle] = \frac{1}{\sqrt{2}}[|00\rangle + |01\rangle]$

2) $|-\rangle \otimes |-\rangle \otimes |+\rangle = \frac{1}{2\sqrt{2}}[(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle)] = \frac{1}{2\sqrt{2}}[|000\rangle + |001\rangle - |100\rangle - |101\rangle$ ...

3) $|01\rangle \otimes |-\rangle = |01\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}[|010\rangle - |011\rangle]$

Example with matrix notation:

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1 \times \begin{pmatrix}1\\0\end{pmatrix}\\ 0 \times \begin{pmatrix}1\\0\end{pmatrix}\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1 \times \begin{pmatrix}0\\1\end{pmatrix}\\ 0 \times \begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|\psi_{AB}\rangle = |+_A\rangle \otimes |1_B\rangle \rightarrow \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}\\ \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}\end{pmatrix} = \begin{pmatrix}0\\ 1/\sqrt{2}\\ 0\\ 1/\sqrt{2}\end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\0 & 4\end{pmatrix} \otimes \begin{pmatrix}2 & 1\\3 & i\end{pmatrix} = \begin{pmatrix}1 \times \begin{pmatrix}2 & 1\\3 & i\end{pmatrix} & 2 \times \begin{pmatrix}2 & 1\\3 & i\end{pmatrix}\\ 0 \times \begin{pmatrix}2 & 1\\3 & i\end{pmatrix} & 4 \times \begin{pmatrix}2 & 1\\3 & i\end{pmatrix}\end{pmatrix} = \begin{pmatrix}2 & 1 & 4 & 2\\3 & i & 6 & 2i\\0 & 0 & 8 & 4\\0 & 0 & 12 & 4i\end{pmatrix}$$

Properties of tensor product

Tensor product has the following properties:

- $c(|v\rangle \otimes |w\rangle) = (c|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c|w\rangle)$ where c is a scalar.
- $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
- $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$
- The tensor product is not commutative in general i.e. $|v\rangle \otimes |w\rangle \neq |w\rangle \otimes |v\rangle$
- We denote a vector tensored with itself k times as $|\psi\rangle^{\otimes k}$
- If A is a linear operator in V and B linear operator in W, then: $(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$

Tensor product of operators

Example 1:

$$O_1 |\psi_A\rangle = |\phi_A\rangle \qquad O_2 |\psi_B\rangle = |\phi_B\rangle$$

$$O_1 \otimes O_2$$

Act on $\underline{\underline{A}}$ Act on $\underline{\underline{B}}$

$$O_1 \otimes O_2 \left(|\psi_A\rangle \otimes |\psi_B\rangle\right) = O_1|\psi_A\rangle \otimes O_2|\psi_B\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$$

Example 2:

$$\begin{cases} X|0\rangle = |1\rangle \\ Z|1\rangle = (-1)|1\rangle \end{cases}$$

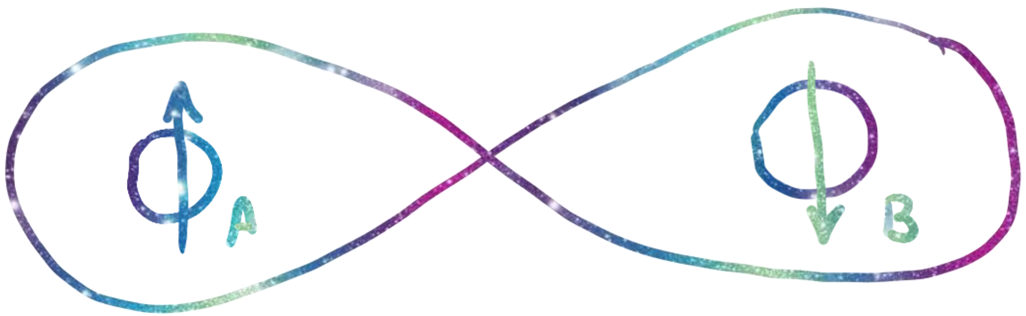
$$X \otimes Z\,|01\rangle = \underbrace{X|0\rangle} \otimes Z|1\rangle = |1\rangle \otimes (-1)|1\rangle = -|11\rangle$$

Example 3:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$H \otimes X = \begin{pmatrix} \frac{1}{\sqrt{2}}X & \frac{1}{\sqrt{2}}X \\ \frac{1}{\sqrt{2}}X & -\frac{1}{\sqrt{2}}X \end{pmatrix} = \begin{pmatrix} 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 \end{pmatrix}$$

What else is there in $\mathcal{H}_{AB}$?



$\in \mathcal{H}_{AB} \rightarrow$ Any vector here!

The other side of the first postulate!

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left[\,|{\uparrow}{\downarrow}\rangle + |{\downarrow}{\uparrow}\rangle\,\right] \in \mathcal{H}_{AB}$$

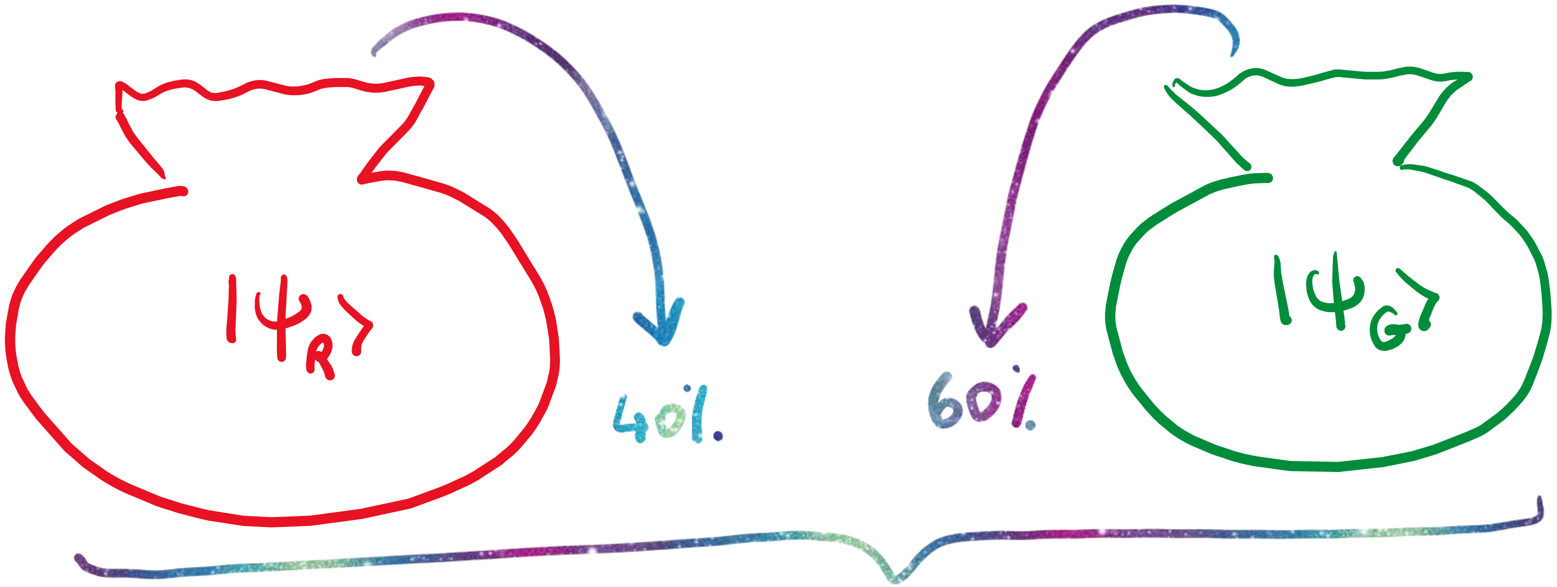
$|\psi_A\rangle \neq |{\uparrow}\rangle$ $\quad$ $|\psi_B\rangle \neq |{\uparrow}\rangle$

$|\psi_A\rangle \neq |{\downarrow}\rangle$ $\quad$ $|\psi_B\rangle \neq |{\downarrow}\rangle$

It seems that the vector representation is not enough!

We need a more general way to describe quantum states

Ensembles of quantum states



$$|\psi_?\rangle = ?$$

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

$$\rho = \underbrace{p_1}_{40\%}|\psi_R\rangle\langle\psi_R| + \underbrace{p_2}_{60\%}|\psi_G\rangle\langle\psi_G|$$

Density Matrix/Operator

A density operator is a linear operator $\rho \in \mathcal{L}(\mathcal{H}^d)$: $\mathcal{H}^d \rightarrow \mathcal{H}^d$ with the following properties:

ρ is Hermitian (or self-adjoint) i.e: $\rho = \rho^\dagger$

$Tr[\rho] = 1$: ρ is normalised

ρ is positive (or more precisely positive semidefinite): $\rho \geq 0$

→ Eigenvalues being real, positive and normalised

ρ can be represented by a $d \times d$ matirx

Why these properties? You can think of a quantum systems described by a density matrix, as generalised probability distributions.

From state vector to density matrices:

$|\psi\rangle$ pure state $\longrightarrow$ $\rho = |\psi\rangle\langle\psi|$ $\rightarrow$ density matrix

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \longrightarrow \rho = |00\rangle\langle 00| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Density Matrix: Examples

1) $|01\rangle\langle 01| = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

2) $|+y\rangle\langle +y| = \frac{1}{2}\left(|0\rangle + i|1\rangle\right)\left(\langle 0| - i\langle 1|\right) = \frac{1}{2}\left[|0\rangle\langle 0| - i|0\rangle\langle 1| + i|1\rangle\langle 0| + |1\rangle\langle 1|\right]$

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

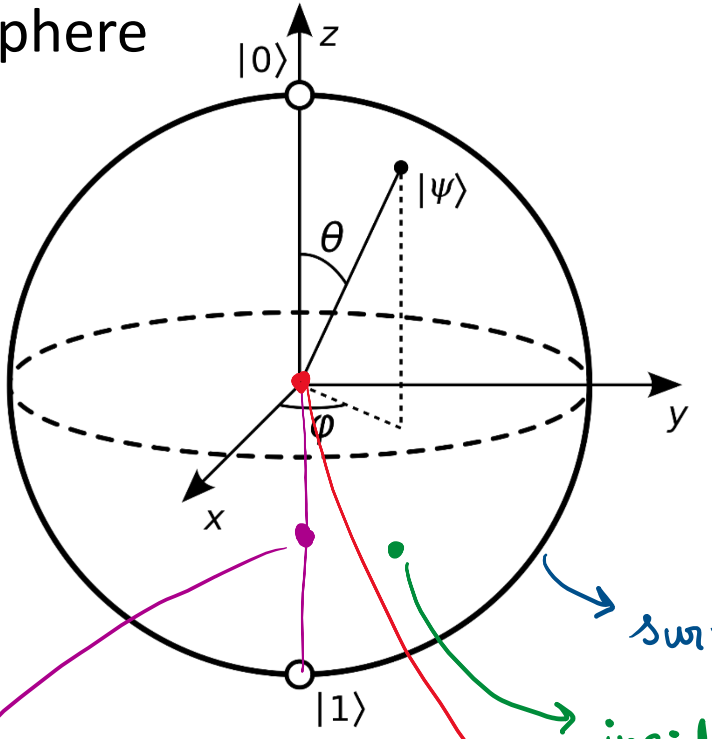
3) $\frac{1}{2}|000\rangle\langle 000| + \frac{1}{2}|111\rangle\langle 111| = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}\begin{pmatrix} 0 & \cdots & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & & & & & & & \vdots \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & & & & & & 1 \end{pmatrix}$

4) $\rho_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $\quad \rho_B = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$ $\quad \rho_A \otimes \rho_B = \begin{pmatrix} 1/2 & -i/2 & 0 & 0 \\ i/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

5) Is $\rho = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a density matrix? ✗ No

Bloch sphere, pure and mixed states

Bloch sphere



$$|\psi\rangle = e^{i\gamma}\left(\cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle\right)$$

Global phase

Any pure $|\psi\rangle \rightarrow$ Bloch vector $\vec{r} = (\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$

ex: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ $\theta = \frac{\pi}{2}$ $\varphi = 0$

surface: all the pure states — Rank 1 density matrices $\leftrightarrow Tr[\rho^2] = 1$

inside: all the mixed states — Mixture of 2 or more pure states

$$\rho = \frac{3}{4}|1\rangle\langle 1| + \frac{1}{4}|0\rangle\langle 0|$$

Maximally mixed state: same distance from all axis

$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ also $\rho = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{I}{2}$

Maximally mixed state in dimension d: $\rho_{mm} = \frac{\mathbb{I}_d}{d}$

Mixed states as ensembles

$$\begin{cases} p_1 = \frac{1}{2} & \rightarrow \quad |00\rangle \\ p_2 = \frac{1}{4} & \rightarrow \quad |+1\rangle \\ p_3 = \frac{1}{4} & \rightarrow \quad |11\rangle \end{cases}$$

$$\rho = \sum_x p_x |\psi_x\rangle\langle\psi_x|$$

Let's write down the density matrix that describes this ensemble:

$$\rho = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{4}|+1\rangle\langle +1| + \frac{1}{4}|11\rangle\langle 11|$$

Entanglement

If you can write the state of a composite system as tensor product of its subsystems, the state is separable.

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$$

ex: $|0\rangle_A \otimes |1\rangle_B$ or $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |0\rangle \otimes |+\rangle$

If the state cannot be written as a separable state, it is called an entangled state. In other words, for an entangled state, it is impossible to attribute a pure state to any of the subsystems.

$$|EPR\rangle = \frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle + |1_A 1_B\rangle\right)$$

Maybe the problem is the basis! Let's write it in another basis

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2\sqrt{2}}\left[(|+\rangle + |-\rangle) \otimes (|+\rangle + |-\rangle) + (|+\rangle - |-\rangle) \otimes (|+\rangle - |-\rangle)\right]$$

$$= \frac{1}{2\sqrt{2}}\left[|++\rangle + \cancel{|+-\rangle} + \cancel{|-+\rangle} + |--\rangle + |++\rangle - \cancel{|+-\rangle} - \cancel{|-+\rangle} + |--\rangle\right]$$

$$= \frac{1}{\sqrt{2}}\left[|++\rangle + |--\rangle\right]$$

still not separable!

Entanglement: describe subsystems by density matrix

$$|\psi_{AB}\rangle = |EPR\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$

$\downarrow$

?

$$\rho_A = \mathrm{Tr}_B\left[\,|\psi_{AB}\rangle\langle\psi_{AB}|\,\right] \qquad \rho_B = \mathrm{Tr}_A\left[\,|\psi_{AB}\rangle\langle\psi_{AB}|\,\right]$$

Called reduced density matrix

$\rightarrow$ Trace out subsystem B!

ρ_A

The state of the subsystems can be described by density matrices.

For a separable state we have: $\rho_{AB} = \rho_A \otimes \rho_B$

Partial trace recap:

Let $|i\rangle$, $|j\rangle$ and $|k\rangle, |l\rangle$ be orthonormal basis for A and B respectively. $M_{AB} = \sum_{ijkl} c_{ijkl} |i\rangle \langle j|_A \otimes |k\rangle\langle l|_B$

The partial trace over B is defined as:

$$
\begin{aligned}
M_A &= Tr_B(M_{AB}) \\
&= \sum_{ijkl} c_{ijkl} |i\rangle \langle j|_A \otimes Tr(|k\rangle\langle l|_B) \\
&= \sum_{ijkl} c_{ijkl} |i\rangle \langle j|_A \otimes \langle l|k\rangle_B \\
&= \sum_{ijkl} c_{ijkl} |i\rangle \langle j|_A \otimes \delta_{kl} \\
&= \sum_{ij} \sum_{k} c_{ijkk} \, |i\rangle \langle j|_A
\end{aligned}
$$

The partial trace over A can be defined similarly.

Quick note about trace: $Tr[\mathrm{ABC}] = \mathrm{Tr}[\mathrm{CAB}]$ (Cyclic property of the trace)

Reduced density matrix example

Let’s calculate reduced density matrices of EPR state:

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

$$\rho_{AB} = |EPR\rangle\langle EPR| = \frac{1}{2}\left[\,|0_A 0_B\rangle\langle 0_A 0_B| + |0_A 0_B\rangle\langle 1_A 1_B| + |1_A 1_B\rangle\langle 0_A 0_B| + |1_A 1_B\rangle\langle 1_A 1_B|\,\right]$$

$$\rho_A = Tr_B(\rho_{AB}) = \frac{1}{2}\left[\,|0\rangle\langle 0|_A \left(\overset{1}{\langle 0|0\rangle}\right)_B + |0\rangle\langle 1|\left(\overset{0}{\langle 0|1\rangle}\right)_B + |1\rangle\langle 0|\left(\overset{0}{\langle 1|0\rangle}\right)_B + |1\rangle\langle 1|\left(\overset{1}{\langle 1|1\rangle}\right)_B\,\right]$$

$$= \frac{1}{2}\left[\,|0\rangle\langle 0| + |1\rangle\langle 1|\,\right]_A$$

$$\rho_B = Tr_A(\rho_{AB}) = \frac{1}{2}\left[\,|0\rangle\langle 0| + |1\rangle\langle 1|\,\right]_B$$

One density operator to rule them all!

ρ

Pure state	Mixed state	Separable state	Entangled state
$\|\psi\rangle\langle\psi\|$	$\sum_x p_x \|\psi_x\rangle\langle\psi_x\|$	$\|\psi_i\rangle\otimes\|\psi_j\rangle$	$\|\psi_{ij}\rangle \neq \|\psi_i\rangle\otimes\|\psi_j\rangle$
rank 1		$\|\psi_{ij}\rangle\langle\psi_{ij}\|$	$\rho_i = \mathrm{Tr}_j[\|\psi_{ij}\rangle\langle\psi_{ij}\|]$

Measurements

Measurement is the way to extract (classical) information from a quantum system.

You have seen one-qubit measurements. But in general, the following rule applies to quantum measurements:

Born Rule:
The measured result for an observable O, on a quantum system $|\psi\rangle$ is given by its eigenvalues λ
The probability of getting a specific eigenvalue λ_i is equal to $\mathrm{p(i)} = \langle\psi|P_i|\psi\rangle$
or more generally for a density matrix ρ is given by $p(i) = Tr[P_i \rho P_i^\dagger]$
Where P_i is the projection onto the eigenspace of O corresponding to λ_i

But there are more general way to extract information from the most general quantum systems.

We will learn more about general measurements in the next lecture!

Resources

1. Quantum Computation and Quantum Information by *Nielsen & Chuang*: 2.1.7, 2.4

2. Introduction to Quantum Cryptography by *Thomas Vidick and Stephanie Wehner*: chapter 2

3. Quantum Information Theory by *Mark M. Wilde*: chapter 3