# Quantum Cyber Security
# Lecture 4: Quantum Information Basics II

Petros Wallden

University of Edinburgh

23rd January 2025

# The following four lectures

- Understand mathematics of quantum states

  Most general way to describe quantum systems

# The following four lectures

- Understand mathematics of quantum states

  Most general way to describe quantum systems

- Quantum measurements and their mathematics

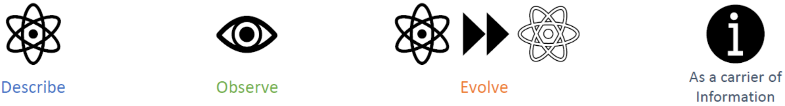
# The following four lectures

- Understand mathematics of quantum states

  Most general way to describe quantum systems
- Quantum measurements and their mathematics
- Quantum operations and their mathematics

- Understand mathematics of quantum states

  Most general way to describe quantum systems
- Quantum measurements and their mathematics
- Quantum operations and their mathematics
- Properties and concepts of classical and quantum information theory



# Quantum Systems beyond single qubit

- Single qubit in Hilbert space of dimension 2: $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

# Quantum Systems beyond single qubit

- Single qubit in Hilbert space of dimension 2: $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Can have system of higher dimension, e.g. $d$-dimension is called **qudit**

qutrit $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$; 4-dim $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$, etc

# Quantum Systems beyond single qubit

- Single qubit in Hilbert space of dimension 2: $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Can have system of higher dimension, e.g. $d$-dimension is called **qudit**

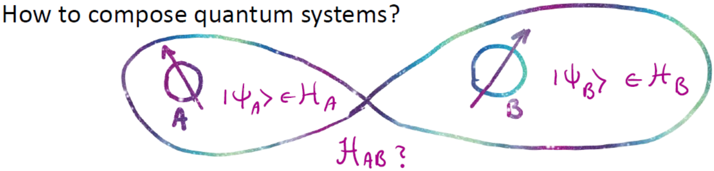
  qutrit $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$; 4-dim $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$, etc
- Or multiple qubits: $n$-qubits have states of dimension $d = 2^n$ Hilbert space

# Quantum Systems beyond single qubit

- Single qubit in Hilbert space of dimension 2: $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Can have system of higher dimension, e.g. $d$-dimension is called **qudit**

qutrit $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$; 4-dim $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$, etc

- Or multiple qubits: $n$-qubits have states of dimension $d = 2^n$ Hilbert space
- Let's see how to compose quantum systems (e.g. two qubits)




- Two Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ can form a new (composite) Hilbert space $\mathcal{H}_{AB}$

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

- Basis vectors of composite are the "product" of the basis vectors of the individual spaces
- **Tensor product** $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$

# Tensor Product of Vector Spaces

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 orthonormal bases for $V$ and $W$ respectively

  Then $|i\rangle \otimes |j\rangle$ is orthonormal basis for $V \otimes W$
- General state $|\psi\rangle_{VW} = \sum_{i,j} \psi_{ij} |i\rangle_V \otimes |j\rangle_W$

# Tensor Product of Vector Spaces

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 orthonormal bases for $V$ and $W$ respectively

  Then $|i\rangle \otimes |j\rangle$ is orthonormal basis for $V \otimes W$
- General state $|\psi\rangle_{VW} = \sum_{i,j} \psi_{ij} |i\rangle_V \otimes |j\rangle_W$
- **Matrix rep.** of operator tensor products:

  Let $A_{ij}$ matrix elements of $A$ and $B_{kl}$ of $B$:
  $A \otimes B = \sum i, j, k, l A_{ij} B_{kl} |i\rangle \langle j| \otimes |k\rangle \langle l|$

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

# Examples

- Dirac notation:

  $|0\rangle \otimes |+\rangle$, $|-\rangle \otimes |-\rangle \otimes |+\rangle$, $|01\rangle \otimes |-\rangle$

# Examples

- Dirac notation:

$|0\rangle \otimes |+\rangle$, $|-\rangle \otimes |-\rangle \otimes |+\rangle$, $|01\rangle \otimes |-\rangle$

- Matrix notation:

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

$|0\rangle \otimes |0\rangle = |00\rangle$ ; $|+\rangle \otimes |1\rangle$

# Examples

- Dirac notation:

  $|0\rangle \otimes |+\rangle, \; |-\rangle \otimes |-\rangle \otimes |+\rangle, \; |01\rangle \otimes |-\rangle$

- Matrix notation:

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

  $|0\rangle \otimes |0\rangle = |00\rangle \; ; \; |+\rangle \otimes |1\rangle$

- Operators:

$$\begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix} \otimes \begin{pmatrix} 2 & 1 \\ 3 & i \end{pmatrix}$$

# Properties of Tensor Products

- Properties:
  - $c(|v\rangle \otimes |w\rangle) = (c|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c|w\rangle)$ where c is a scalar.
  - $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
  - $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$

# Properties of Tensor Products

- Properties:
  - $c(|v\rangle \otimes |w\rangle) = (c|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c|w\rangle)$ where c is a scalar.
  - $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
  - $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$
- Tensor product isn't commutative $|v\rangle \otimes |w\rangle \neq |w\rangle \otimes |v\rangle$

  (not the order of the spaces is conventional, could reorder them if needed, but on all terms of one expression!)
- A vector tensored $k$-times with itself: $|\psi\rangle^{\otimes k}$

# Properties of Tensor Products

- Properties:
  - $c(|v\rangle \otimes |w\rangle) = (c|v\rangle) \otimes |w\rangle = |v\rangle \otimes (c|w\rangle)$ where c is a scalar.
  - $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$
  - $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$
- Tensor product isn't commutative $|v\rangle \otimes |w\rangle \neq |w\rangle \otimes |v\rangle$

  (not the order of the spaces is conventional, could reorder them if needed, but on all terms of one expression!)
- A vector tensored $k$-times with itself: $|\psi\rangle^{\otimes k}$
- If A acts on V and B acts on W, then

  $(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$

# Examples: tensor product operators

- $O_1 |\psi_1\rangle = |\phi_1\rangle$ and $O_2 |\psi_2\rangle = |\phi_2\rangle$

  $(O_1 \otimes O_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = O_1 |\psi_1\rangle \otimes O_2 |\psi_2\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$

# Examples: tensor product operators

- $O_1 |\psi_1\rangle = |\phi_1\rangle$ and $O_2 |\psi_2\rangle = |\phi_2\rangle$

  $(O_1 \otimes O_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = O_1 |\psi_1\rangle \otimes O_2 |\psi_2\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$

- $X |j\rangle = |j \oplus 1\rangle \ , \ Z |j\rangle = (-1)^j |j\rangle$

  $(X \otimes Z) |01\rangle = X |0\rangle \otimes Z |1\rangle = |1\rangle \otimes (-1) |1\rangle = - |11\rangle$

# Examples: tensor product operators

- $O_1 |\psi_1\rangle = |\phi_1\rangle$ and $O_2 |\psi_2\rangle = |\phi_2\rangle$

  $$(O_1 \otimes O_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = O_1 |\psi_1\rangle \otimes O_2 |\psi_2\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$$

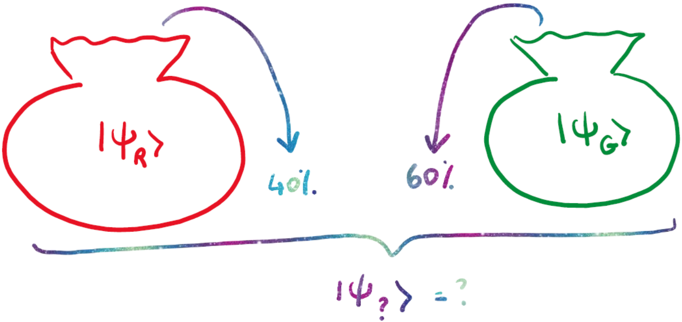
- $X |j\rangle = |j \oplus 1\rangle \ , \ Z |j\rangle = (-1)^j |j\rangle$

  $$(X \otimes Z) |01\rangle = X |0\rangle \otimes Z |1\rangle = |1\rangle \otimes (-1) |1\rangle = - |11\rangle$$

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

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

# Ensembles of Quantum States




- Examples:

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

$$\rho = p_1 |\psi_R\rangle\langle\psi_R| + p_2 |\psi_G\rangle\langle\psi_G| \text{ where } p_1 = 0.4\ ,\ \ p_2 = 0.6$$

# Density Matrices (Recall)

**Definition:** A **density matrix** is a matrix (or operator) $\rho$ that:

1. is Hermitian $\rho^\dagger = \rho$
2. positive semi-definite (i.e. has non-negative eigenvalues)
3. has unit trace $\mathrm{Tr}(\rho) = 1$

- Real eigenvalues, non-negative, normalised

# Density Matrices (Recall)

**Definition:** A **density matrix** is a matrix (or operator) $\rho$ that:

1. is Hermitian $\rho^\dagger = \rho$
2. positive semi-definite (i.e. has non-negative eigenvalues)
3. has unit trace $\mathrm{Tr}(\rho) = 1$

- Real eigenvalues, non-negative, normalised
- Pure state vector $|\psi\rangle$ goes to pure density matrix: $\rho_\psi := |\psi\rangle\langle\psi|$
- Can incorporate probabilities over quantum states (ensembles)

# Examples

- $|01\rangle \langle 01|$ (in matrix)

# Examples

- $|01\rangle\langle 01|$ (in matrix)
- $|+_y\rangle\langle +_y|$, where $|+_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ (in Dirac notation)

# Examples

- $|01\rangle\langle 01|$ (in matrix)
- $|+_y\rangle\langle +_y|$, where $|+_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ (in Dirac notation)
- $\frac{1}{2}|000\rangle\langle 000| + \frac{1}{2}|111\rangle\langle 111|$ (in matrix)

# Examples

- $|01\rangle\langle 01|$ (in matrix)
- $|+_y\rangle\langle +_y|$, where $|+_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ (in Dirac notation)
- $\frac{1}{2}|000\rangle\langle 000| + \frac{1}{2}|111\rangle\langle 111|$ (in matrix)
- $\rho_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ; $\rho_B = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$

  Express the composite $\rho_A \otimes \rho_B$

# Examples

- $|01\rangle\langle 01|$ (in matrix)
- $|+_y\rangle\langle +_y|$, where $|+_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ (in Dirac notation)
- $\frac{1}{2}|000\rangle\langle 000| + \frac{1}{2}|111\rangle\langle 111|$ (in matrix)
- $\rho_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ; $\rho_B = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$

  Express the composite $\rho_A \otimes \rho_B$
- Is $\rho = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a density matrix?

# Examples

- $|01\rangle\langle 01|$ (in matrix)
- $|+_y\rangle\langle +_y|$, where $|+_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ (in Dirac notation)
- $\frac{1}{2}|000\rangle\langle 000| + \frac{1}{2}|111\rangle\langle 111|$ (in matrix)
- $\rho_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ; $\rho_B = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$

  Express the composite $\rho_A \otimes \rho_B$
- Is $\rho = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a density matrix?
- Write the density matrix of the ensemble:
  $\{p_1 = 0.5\ ,\ |00\rangle\ ;\ p_2 = 0.25\ ,\ |+1\rangle\ ;\ p_3 = 0.25\ ,\ |11\rangle\}$

  $\rho = \sum_{i=1}^{3} p_i |\psi_i\rangle\langle\psi_i|$

# Examples

- $|01\rangle\langle 01|$ (in matrix)
- $|+_y\rangle\langle +_y|$, where $|+_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ (in Dirac notation)
- $\frac{1}{2}|000\rangle\langle 000| + \frac{1}{2}|111\rangle\langle 111|$ (in matrix)
- $\rho_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ; $\rho_B = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$

  Express the composite $\rho_A \otimes \rho_B$
- Is $\rho = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a density matrix?
- Write the density matrix of the ensemble:
  $\{p_1 = 0.5\ ,\ |00\rangle\ ;\ p_2 = 0.25\ ,\ |+1\rangle\ ;\ p_3 = 0.25\ ,\ |11\rangle\}$
  $\rho = \sum_{i=1}^{3} p_i |\psi_i\rangle\langle\psi_i|$
- All mixed states can be expressed as ensembles (diagonalise!)

# Entanglement

- There are states that CANNOT be written as tensor product of individual states

  **Product states**: $|\psi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$

# Entanglement

- There are states that CANNOT be written as tensor product of individual states

  **Product states**: $|\psi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$

- Bell states: $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

  This state **cannot** be written as product

# Entanglement

- There are states that CANNOT be written as tensor product of individual states

  **Product states**: $|\psi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$

- Bell states: $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

  This state **cannot** be written as product

- A (pure) state that cannot be written as product state, is **entangled**

# Entanglement

- There are states that CANNOT be written as tensor product of individual states

  **Product states**: $|\psi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$

- Bell states: $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

  This state **cannot** be written as product

- A (pure) state that cannot be written as product state, is **entangled**

- Mixed states that cannot be written as mixtures of product states are **entangled**

  Mixture of product states: $\rho = \sum_{ij} p_{ij}\rho_i \otimes \rho_j$

# Entanglement

- There are states that CANNOT be written as tensor product of individual states

  **Product states**: $|\psi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$

- Bell states: $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

  This state **cannot** be written as product

- A (pure) state that cannot be written as product state, is **entangled**

- Mixed states that cannot be written as mixtures of product states are **entangled**

  Mixture of product states: $\rho = \sum_{ij} p_{ij} \rho_i \otimes \rho_j$

- To describe a subsystem of a (pure or mixed) entangled state, we need density matrices!

# Bell states are entangled

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ Cannot be written as product state

# Bell states are entangled

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Cannot be written as product state

  Proof: Assume that there exists states $|a\rangle = a_0|0\rangle + a_1|1\rangle$ and $|b\rangle = b_0|0\rangle + b_1|1\rangle$ such that $|\Phi^+\rangle = |a\rangle \otimes |b\rangle$

# Bell states are entangled

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Cannot be written as product state

  Proof: Assume that there exists states $|a\rangle = a_0|0\rangle + a_1|1\rangle$ and $|b\rangle = b_0|0\rangle + b_1|1\rangle$ such that $|\Phi^+\rangle = |a\rangle \otimes |b\rangle$

  It follows that
  $|a\rangle \otimes |b\rangle = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle$

# Bell states are entangled

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Cannot be written as product state

  Proof: Assume that there exists states $|a\rangle = a_0|0\rangle + a_1|1\rangle$ and $|b\rangle = b_0|0\rangle + b_1|1\rangle$ such that $|\Phi^+\rangle = |a\rangle \otimes |b\rangle$

  It follows that
  $|a\rangle \otimes |b\rangle = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle$

  Since there are no $|01\rangle, |10\rangle$ terms, we know that
  $a_0 b_1 = a_1 b_0 = 0$

# Bell states are entangled

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Cannot be written as product state

  Proof: Assume that there exists states $|a\rangle = a_0\,|0\rangle + a_1\,|1\rangle$ and $|b\rangle = b_0\,|0\rangle + b_1\,|1\rangle$ such that $|\Phi^+\rangle = |a\rangle \otimes |b\rangle$

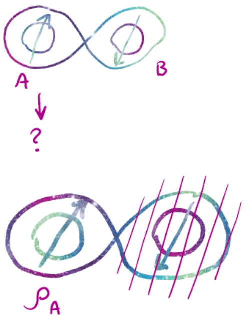
  It follows that
  $|a\rangle \otimes |b\rangle = a_0 b_0\,|00\rangle + a_0 b_1\,|01\rangle + a_1 b_0\,|10\rangle + a_1 b_1\,|11\rangle$

  Since there are no $|01\rangle\,,|10\rangle$ terms, we know that
  $a_0 b_1 = a_1 b_0 = 0$

  (i) if $a_0 = 0$ then the term that has $|00\rangle$ vanishes (which it shouldn't)

  (ii) if $b_1 = 0$ the term with $|11\rangle$ vanishes $\square$

# Subsystems and partial trace




- Let $\rho_{AB} = |\psi_{AB}\rangle \langle\psi_{AB}|$

  Then $\rho_A := \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B := \mathrm{Tr}_A(\rho_{AB})$
- It easy to see that for product states $\rho_{AB} = \rho_A \otimes \rho_B$ this is the case

# Partial Trace

- Consider $M_{AB} = \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \otimes \left|k\right\rangle \left\langle l\right|_B$
- Partial trace over B:

  $M_A := \mathrm{Tr}_B(M_{AB}) = \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \times \mathrm{Tr}(\left|k\right\rangle \left\langle l\right|_B)$

  (note the trace is number not a matrix)

  $= \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \times (\left\langle l\right| k\rangle_B)$ (using cyclic property)

  $= \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \times (\left\langle l\right| k\rangle_B)$ (using orthogonality)

  $\sum_{i,j} \sum_k c_{ijkk} \left|i\right\rangle \left\langle j\right|_A$

# Partial Trace

- Consider $M_{AB} = \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \otimes \left|k\right\rangle \left\langle l\right|_B$
- Partial trace over B:

  $M_A := \mathrm{Tr}_B(M_{AB}) = \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \times \mathrm{Tr}(\left|k\right\rangle \left\langle l\right|_B)$

  (note the trace is number not a matrix)

  $= \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \times (\left\langle l\right| k\rangle_B)$ (using cyclic property)

  $= \sum_{i,j,k,l} c_{ijkl} \left|i\right\rangle \left\langle j\right|_A \times (\left\langle l\right| k\rangle_B)$ (using orthogonality)

  $\sum_{i,j} \sum_k c_{ijkk} \left|i\right\rangle \left\langle j\right|_A$
- Reduced matrix (partial trace over $B$) is a matrix at space $A$
- Partial trace over $A$ is defined similarly

# Examples

- Reduced state for product states $\rho_{AB} = \rho_A \otimes \rho_B$

  As expected: $\rho_A$ and $\rho_B$

# Examples

- Reduced state for product states $\rho_{AB} = \rho_A \otimes \rho_B$

  As expected: $\rho_A$ and $\rho_B$

- Reduced state for entangled (Bell) state:

  $\rho_{AB} = |\Phi^+\rangle \langle \Phi^+|$

  $|\Phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$

  $\rho_A = \mathrm{Tr}(\rho_{AB}) = \cdots = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|)_A$

  $\rho_B = \mathrm{Tr}(\rho_{AB}) = \cdots = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|)_B$

# One density operator to rule them all!


**Pure state**

$|\psi\rangle\langle\psi|$

rank 1

**Mixed state**

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

**Separable state**

$|\psi_i\rangle \otimes |\psi_j\rangle$

$|\psi_{ij}\rangle\langle\psi_{ij}|$

**Entangled state**

$|\psi_{ij}\rangle \neq |\psi_i\rangle \otimes |\psi_j\rangle$

$\rho_i = Tr_j[|\psi_{ij}\rangle\langle\psi_{ij}|]$

# Measurements

- We have seen simple one qubit measurements

# Measurements

- We have seen simple one qubit measurements
- It generalises for observable $O$

**Born Rule:**
The measured result for an observable O, on a quantum system $|\psi\rangle$ is given by its eigenvalues $\lambda$
The probability of getting a specific eigenvalue $\lambda_i$ is equal to $\mathrm{p(i)} = \langle\psi|P_i|\psi\rangle$
or more generally for a density matrix $\rho$ 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 $\lambda_i$

# Measurements

- We have seen simple one qubit measurements
- It generalises for observable $O$

**Born Rule:**
The measured result for an observable O, on a quantum system $|\psi\rangle$ is given by its eigenvalues $\lambda$
The probability of getting a specific eigenvalue $\lambda_i$ is equal to $\mathrm{p(i)} = \langle\psi|P_i|\psi\rangle$
or more generally for a density matrix $\rho$ 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 $\lambda_i$

- Can define more general measurements (non-projective)

  See next lecture!

# Some resources

- Quantum Computation and Quantum Information by Nielsen & Chuang: 2.1.7, 2.4
- Introduction to Quantum Cryptography by Thomas Vidick and Stephanie Wehner: chapter 2
- Quantum Information Theory by Mark M. Wilde: chapter 3