Quantum Cyber Security
Lecture 2: Quantum Information Basics I

Petros Wallden

University of Edinburgh

18th January 2024

Motivation: From Bit-strings to Qubit-strings

- **Units of quantum information** are qubits
- **Registers** consists of strings of qubits

- **Units of quantum information** are qubits
- **Registers** consists of strings of qubits
- **Qubit-strings** $|110\rangle$ are (unit) vectors with complex coefficients E.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|101\rangle + i\,|011\rangle)$

Motivation: From Bit-strings to Qubit-strings

- **Units of quantum information** are qubits
- **Registers** consists of strings of qubits
- **Qubit-strings** $|110\rangle$ are (unit) vectors with complex coefficients E.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|101\rangle + i\,|011\rangle)$
- **Operations** (Gates) and **Observables** are linear maps (matrices): E.g. $H\,|x\rangle = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}\,|y\rangle$

Motivation: From Bit-strings to Qubit-strings

- **Units of quantum information** are qubits
- **Registers** consists of strings of qubits
- **Qubit-strings** $|110\rangle$ are (unit) vectors with complex coefficients E.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|101\rangle + i\,|011\rangle)$
- **Operations** (Gates) and **Observables** are linear maps (matrices): E.g. $H\,|x\rangle = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}\,|y\rangle$
- To extract **classical information** we require measurements
- Measurements are **probabilistic**: The coefficients determine the probability. E.g. $|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x\,|x\rangle$, then x occurs with probability $|a_x|^2$

Motivation: From Bit-strings to Qubit-strings

- **Units of quantum information** are qubits
- **Registers** consists of strings of qubits
- **Qubit-strings** $|110\rangle$ are (unit) vectors with complex coefficients E.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|101\rangle + i\,|011\rangle)$
- **Operations** (Gates) and **Observables** are linear maps (matrices): E.g. $H\,|x\rangle = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}\,|y\rangle$
- To extract **classical information** we require measurements
- Measurements are **probabilistic**: The coefficients determine the probability. E.g. $|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x\,|x\rangle$, then x occurs with probability $|a_x|^2$
- Multi-qubit operations can generate "**entanglement**": system behaves "holistically" (non-locally – see later)

Motivation: From Bit-strings to Qubit-strings

- **Units of quantum information** are qubits
- **Registers** consists of strings of qubits
- **Qubit-strings** $|110\rangle$ are (unit) vectors with complex coefficients E.g. $|\psi\rangle = \frac{1}{\sqrt{2}}(|101\rangle + i\,|011\rangle)$
- **Operations** (Gates) and **Observables** are linear maps (matrices): E.g. $H\,|x\rangle = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}\,|y\rangle$
- To extract **classical information** we require measurements
- Measurements are **probabilistic**: The coefficients determine the probability. E.g. $|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x\,|x\rangle$, then x occurs with probability $|a_x|^2$
- Multi-qubit operations can generate "**entanglement**": system behaves "holistically" (non-locally – see later)
- Q: Why we have speed-up?
  A: Like classical probabilistic algorithms BUT with **complex** "probabilities"

Definitions with Examples

A Qubit is a 2-dimensional unit vector

- For formal definitions look at: Math Supplement; Nielsen & Chuang; or first lectures of IQC (`https://opencourse.inf.ed.ac.uk/iqc/course-materials/schedule` or an older version `http://pwallden.gr/courseiqc.asp`)

Definitions with Examples

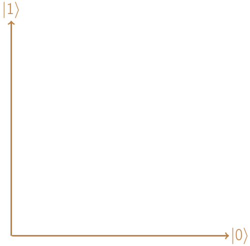
A Qubit is a 2-dimensional unit vector

- We will denote a vector $\vec{v}$ as $|v\rangle$

Definitions with Examples

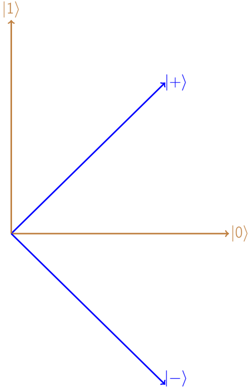
A Qubit is a 2-dimensional unit vector

- The unit vectors in the x-axis as $|0\rangle$ and in the y-axis as $|1\rangle$



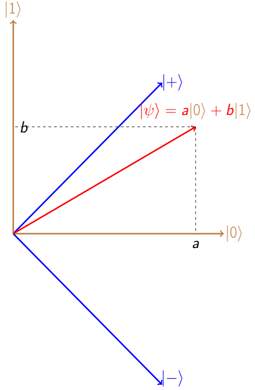
A Qubit is a 2-dimensional unit vector

- Another basis (45% rotated) is given by the vectors $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$



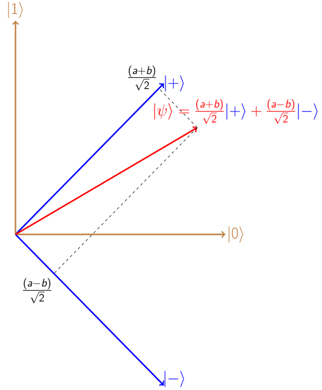
A Qubit is a 2-dimensional unit vector

- General Qubit: $|\psi\rangle = a|0\rangle + b|1\rangle$ where $|\,|\psi\rangle\,|^2 = 1 = |a|^2 + |b|^2$ and a, b are **complex numbers** in general



A Qubit is a 2-dimensional unit vector

- Can be expressed in the blue basis: $|\psi\rangle = \frac{(a+b)}{\sqrt{2}}|+\rangle + \frac{(a-b)}{\sqrt{2}}|-\rangle$



Definitions with Examples

- **Vector** (notation) $|\psi\rangle$ is called "**ket**".
  Example: $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$
- **Dual vector** is denoted $\langle\psi|$ and is called "**bra**". Coefficients are complex conjugate of the coefficients of the vectors
  Example: $\langle\psi| = a^*\,\langle 0| + b^*\,\langle 1|$
- **Inner product** (c.f. dot-product) is taken between a **vector** and a **dual vector** (c.f. "**bra-ket**").

Definitions with Examples

- **Vector** (notation) $|\psi\rangle$ is called "**ket**".
  Example: $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$
- **Dual vector** is denoted $\langle\psi|$ and is called "**bra**". Coefficients are complex conjugate of the coefficients of the vectors
  Example: $\langle\psi| = a^*\,\langle 0| + b^*\,\langle 1|$
- **Inner product** (c.f. dot-product) is taken between a **vector** and a **dual vector** (c.f. "**bra-ket**").
- Orthogonal vectors have zero inner product so:
  $\langle 0|\,1\rangle = \langle 1|\,0\rangle = 0$ and $\langle 0|\,0\rangle = \langle 1|\,1\rangle = 1$
- Example: $\langle\psi_2|\,\psi_1\rangle = a_2^* a_1 + b_2^* b_1 = \langle\psi_1|\,\psi_2\rangle^*$
  Let $|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$; $|\psi_2\rangle = \frac{1}{2}\left(i\,|0\rangle + \sqrt{3}\,|1\rangle\right)$
  Check: $\langle\psi_1|\,\psi_1\rangle = \langle\psi_2|\,\psi_2\rangle = 1$ and
  $\langle\psi_2|\,\psi_1\rangle = \frac{\sqrt{3}-i}{2\sqrt{2}}$; $\langle\psi_1|\,\psi_2\rangle = \frac{\sqrt{3}+i}{2\sqrt{2}}$

Definitions with Examples

In matrix notation:

Vectors: $|\psi_1\rangle = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$ and **Dual Vectors**: $\langle\psi_2| = \begin{pmatrix} a_2^* & b_2^* \end{pmatrix}$

In matrix notation:

Vectors: $|\psi_1\rangle = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$ and **Dual Vectors**: $\langle\psi_2| = \begin{pmatrix} a_2^* & b_2^* \end{pmatrix}$

- Operations (gates) and Observables correspond to **linear maps**
  (Complex valued) Matrix with matrix elements m_{ij}
  $M = \begin{pmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{pmatrix} = \sum_{i,j\in\{0,1\}} m_{ij} |i\rangle \langle j|$
- **Outer Product** between a vector and a dual vector (opposite order of inner "**ket-bra**"):
  $|\psi_1\rangle \langle\psi_2| = \begin{pmatrix} a_1 a_2^* & a_1 b_2^* \\ b_1 a_2^* & b_1 b_2^* \end{pmatrix}$

Example: $A = \begin{pmatrix} 1 & 1+i \\ 2 & 3+2i \end{pmatrix} = |0\rangle\langle 0| + (1+i)|0\rangle\langle 1| +$
$+2|1\rangle\langle 0| + (3+2i)|1\rangle\langle 1|$

Example: $A = \begin{pmatrix} 1 & 1+i \\ 2 & 3+2i \end{pmatrix} = |0\rangle\langle 0| + (1+i)|0\rangle\langle 1| +$
$+2|1\rangle\langle 0| + (3+2i)|1\rangle\langle 1|$

- **Adjoint** (Hermitian conjugate) of an operator is defined as: **transpose** and **conjugate element-wise**

  Example: $A^\dagger = \begin{pmatrix} 1 & 2 \\ 1-i & 3-2i \end{pmatrix}$ Note: $|v\rangle^\dagger = \langle v|$ and
  $(A|v\rangle)^\dagger = \langle v|A^\dagger$ and
  $(AB)^\dagger = B^\dagger A^\dagger$

Example: $A = \begin{pmatrix} 1 & 1+i \\ 2 & 3+2i \end{pmatrix} = |0\rangle\langle 0| + (1+i)|0\rangle\langle 1| +$
$+2|1\rangle\langle 0| + (3+2i)|1\rangle\langle 1|$

- **Adjoint** (Hermitian conjugate) of an operator is defined as: **transpose** and **conjugate element-wise**

  Example: $A^\dagger = \begin{pmatrix} 1 & 2 \\ 1-i & 3-2i \end{pmatrix}$ Note: $|v\rangle^\dagger = \langle v|$ and
  $(A|v\rangle)^\dagger = \langle v| A^\dagger$ and
  $(AB)^\dagger = B^\dagger A^\dagger$
- An operator B is called **Hermitian** (or self-adjoint) if $B^\dagger = B$
- Hermitian operators have real eigenvalues

Definitions with Examples

Example: $A = \begin{pmatrix} 1 & 1+i \\ 2 & 3+2i \end{pmatrix} = |0\rangle\langle 0| + (1+i)|0\rangle\langle 1| +$
$+2|1\rangle\langle 0| + (3+2i)|1\rangle\langle 1|$

- **Adjoint** (Hermitian conjugate) of an operator is defined as: **transpose** and **conjugate element-wise**

  Example: $A^\dagger = \begin{pmatrix} 1 & 2 \\ 1-i & 3-2i \end{pmatrix}$ Note: $|v\rangle^\dagger = \langle v|$ and
  $(A|v\rangle)^\dagger = \langle v| A^\dagger$ and
  $(AB)^\dagger = B^\dagger A^\dagger$
- An operator B is called **Hermitian** (or self-adjoint) if $B^\dagger = B$
- Hermitian operators have real eigenvalues

  Example: The matrix A above is NOT Hermitian, while the matrix B **is**
  $B = \begin{pmatrix} 1 & 2+3i \\ 2-3i & 5 \end{pmatrix} = B^\dagger$

- An important class of Hermitian operators are the **Projection** operators which are defined as: $P^2 = P$
  These operators, restrict/project a vector to some subspace of the total Hilbert space

Definitions with Examples

- An important class of Hermitian operators are the **Projection** operators which are defined as: $P^2 = P$
  These operators, restrict/project a vector to some subspace of the total Hilbert space
  Example: $P = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ this projects to the subspace defined by the vector $|0\rangle$

- An important class of Hermitian operators are the **Projection** operators which are defined as: $P^2 = P$
  These operators, restrict/project a vector to some subspace of the total Hilbert space

  Example: $P = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ this projects to the subspace defined by the vector $|0\rangle$

- An operator U is called **unitary** if $UU^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Definitions with Examples

- An important class of Hermitian operators are the **Projection** operators which are defined as: $P^2 = P$
  These operators, restrict/project a vector to some subspace of the total Hilbert space

  Example: $P = |0\rangle \langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ this projects to the subspace defined by the vector $|0\rangle$

- An operator U is called **unitary** if $UU^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

  Unitary operators preserve the inner product of vectors
  $\langle v| w\rangle = \langle v| U^\dagger U |w\rangle$

- **Operations**/gates/channels for (pure) quantum states are unitaries and they map quantum states to quantum states $U|\psi\rangle = |\phi\rangle$ noting that $\langle\phi|\phi\rangle = 1 = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle$

  Examples: Identity I; Pauli X, Y and Z gates

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

  Hadamard H

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

Example:

- The quantum NOT-gate is the Pauli X:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Acts as the NOT-gate to computational basis vectors: $|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$

For a general qubit: $\alpha |0\rangle + \beta |1\rangle \rightarrow \alpha |1\rangle + \beta |0\rangle$

$\alpha |0\rangle + \beta |1\rangle$ 

$\alpha |1\rangle + \beta |0\rangle$

- **Measurement** (projective) for pure states
- Computational basis: Given the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we measure in the $\{|0\rangle, |1\rangle\}$ basis

- With probability $|\alpha|^2$ we get the outcome 0; output state is $|0\rangle$
- With probability $|\beta|^2$ we get the outcome 1; output state is $|1\rangle$

- General basis: We express the state in that basis and repeat

  Example: To measure in the $\{|+\rangle, |-\rangle\}$ basis we re-express $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in that basis:

  $|\psi\rangle = \frac{(a+b)}{\sqrt{2}}|+\rangle + \frac{(a-b)}{\sqrt{2}}|-\rangle$

- Outcome $+$ with prob $|\frac{(a+b)}{\sqrt{2}}|^2$ and final state $|+\rangle$
- Outcome $-$ with prob $|\frac{(a-b)}{\sqrt{2}}|^2$ and final state $|-\rangle$

Definitions with Examples

- **Check:** What happens if one measures $|+\rangle$ in the $\{|0\rangle, |1\rangle\}$ and in the $\{|+\rangle, |-\rangle\}$ bases?

- Measurement formally: Given two projection P_1, P_2 where $P_1 + P_2 = I$

  - Outcome cor. to P_1 with probability $\langle\psi| P_1 |\psi\rangle$ and output state $(P_1 |\psi\rangle) \frac{1}{\sqrt{\langle\psi|P_1|\psi\rangle}}$

  - Outcome cor. to P_2 with probability $\langle\psi| P_2 |\psi\rangle$ and output state $(P_2 |\psi\rangle) \frac{1}{\sqrt{\langle\psi|P_2|\psi\rangle}}$

- Note: the sum of probabilities is one:

$$\langle\psi| P_1 |\psi\rangle + \langle\psi| P_2 |\psi\rangle = \langle\psi| (P_1 |\psi\rangle + P_2 |\psi\rangle) =$$

$$= \langle\psi| (P_1 + P_2) |\psi\rangle = \langle\psi| I |\psi\rangle = 1$$

Definitions with Examples

- We call **trace** of an operator A the following $\mathrm{Tr}(A) = \sum_i A_{ii}$ and is defined for square matrices

- We call **trace** of an operator A the following $\mathrm{Tr}(A) = \sum_i A_{ii}$ and is defined for square matrices

  Example: $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $\mathrm{Tr}(A) = a_{11} + a_{22}$

- We call **trace** of an operator A the following $\mathrm{Tr}(A) = \sum_i A_{ii}$ and is defined for square matrices

  Example: $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $\mathrm{Tr}(A) = a_{11} + a_{22}$

  The trace is cyclic symmetric:
  $\mathrm{Tr}(ABC) = \mathrm{Tr}(BCA) = \mathrm{Tr}(CAB)$

- We call **trace** of an operator A the following $\mathrm{Tr}(A) = \sum_i A_{ii}$ and is defined for square matrices

  Example: $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $\mathrm{Tr}(A) = a_{11} + a_{22}$

  The trace is cyclic symmetric:
  $\mathrm{Tr}(ABC) = \mathrm{Tr}(BCA) = \mathrm{Tr}(CAB)$

  The trace of an operator is invariant under unitary similarity transformations $A \rightarrow UAU^\dagger$
  $\mathrm{Tr}(UAU^\dagger) = \mathrm{Tr}(U^\dagger UA) = \mathrm{Tr}(A)$

Density Matrices and Mixed States

- We represented q-states as vectors $|\psi\rangle$

Density Matrices and Mixed States

- We represented q-states as vectors $|\psi\rangle$

  We can also represent the states as operators, which we call **density matrices:** $\rho_\psi = |\psi\rangle\langle\psi|$

Density Matrices and Mixed States

- We represented q-states as vectors $|\psi\rangle$

  We can also represent the states as operators, which we call **density matrices:** $\rho_\psi = |\psi\rangle\langle\psi|$

  Examples:

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

Density Matrices and Mixed States

- We represented q-states as vectors $|\psi\rangle$

  We can also represent the states as operators, which we call **density matrices:** $\rho_\psi = |\psi\rangle\langle\psi|$

  Examples:

  1. $|0\rangle \longrightarrow |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$
  2. $|+\rangle := 1/\sqrt{2}\,(|0\rangle + |1\rangle) \longrightarrow |+\rangle\langle +| = 1/2 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

Density Matrices and Mixed States

- We represented q-states as vectors $|\psi\rangle$

  We can also represent the states as operators, which we call **density matrices:** $\rho_\psi = |\psi\rangle\langle\psi|$

  Examples:

  1. $|0\rangle \longrightarrow |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$
  2. $|+\rangle := 1/\sqrt{2}\,(|0\rangle + |1\rangle) \longrightarrow |+\rangle\langle +| = 1/2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

- Using this representation we can represent the state of quantum systems that are **not completely known**.

- We represented q-states as vectors $|\psi\rangle$

  We can also represent the states as operators, which we call **density matrices:** $\rho_\psi = |\psi\rangle\langle\psi|$

  Examples:

  1. $|0\rangle \longrightarrow |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$
  2. $|+\rangle := 1/\sqrt{2}\,(|0\rangle + |1\rangle) \longrightarrow |+\rangle\langle +| = 1/2 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

- Using this representation we can represent the state of quantum systems that are **not completely known**.
- Definition: Assume that the (real) quantum state is one of a number of states $\{|\psi_i\rangle\}_i$, each of them occurring with probability p_i. We call $\{p_i, |\psi_i\rangle\}$ an **ensemble of states**.

Density Matrices and Mixed States

- We represented q-states as vectors $|\psi\rangle$

  We can also represent the states as operators, which we call **density matrices:** $\rho_\psi = |\psi\rangle\langle\psi|$

  Examples:

  1. $|0\rangle \longrightarrow |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$
  2. $|+\rangle := 1/\sqrt{2}\,(|0\rangle + |1\rangle) \longrightarrow |+\rangle\langle +| = 1/2 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

- Using this representation we can represent the state of quantum systems that are **not completely known**.
- Definition: Assume that the (real) quantum state is one of a number of states $\{|\psi_i\rangle\}_i$, each of them occurring with probability p_i. We call $\{p_i, |\psi_i\rangle\}$ an **ensemble of states**.

  The state of this system is described by the following density matrix: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

Density Matrices and Mixed States

- Definition: When a density matrix ρ cannot be expressed in terms of a single pure state $\rho \neq |\psi\rangle\langle\psi| \ \forall \ \psi$, we say that it is a **mixed state**

Density Matrices and Mixed States

- Definition: When a density matrix ρ cannot be expressed in terms of a single pure state $\rho \neq |\psi\rangle\langle\psi| \ \forall\ \psi$, we say that it is a **mixed state**
- The mixed states include **two types of randomness**:
  1. **Classical randomness** since we do not know which is the (real) pure quantum state. This randomness is due to the lack of knowledge that we (the observers) have. Is the same with the randomness of classical physics (epistemic).

Density Matrices and Mixed States

- Definition: When a density matrix ρ cannot be expressed in terms of a single pure state $\rho \neq |\psi\rangle \langle\psi| \ \forall \ \psi$, we say that it is a **mixed state**
- The mixed states include **two types of randomness**:
  1. **Classical randomness** since we do not know which is the (real) pure quantum state. This randomness is due to the lack of knowledge that we (the observers) have. Is the same with the randomness of classical physics (epistemic).
  2. Fundamental **quantum randomness**. This is due to the fact that even if we know the exact pure quantum state (have maximum information about the system), multiple outcomes may occur.

Example: Classical Vs Quantum Randomness

- Mixed state:

$$\rho_1 = 1/2\,|0\rangle\langle 0| + 1/2\,|1\rangle\langle 1| = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

Example: Classical Vs Quantum Randomness

- Mixed state:

$$\rho_1 = 1/2 \left|0\right\rangle \left\langle 0\right| + 1/2 \left|1\right\rangle \left\langle 1\right| = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

- Pure state (equal superposition):

$$\rho_2 = \left|+\right\rangle \left\langle +\right| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

Example: Classical Vs Quantum Randomness

- Mixed state:

$$\rho_1 = 1/2 \left|0\right\rangle \left\langle 0\right| + 1/2 \left|1\right\rangle \left\langle 1\right| = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

- Pure state (equal superposition):

$$\rho_2 = \left|+\right\rangle \left\langle +\right| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

- Measured in computational basis $\{\left|0\right\rangle, \left|1\right\rangle\}$ both give same probabilities (but for ρ_1 is classical randomness while for ρ_2 is quantum randomness).
- Measured in the Hadamard basis $\{\left|+\right\rangle, \left|-\right\rangle\}$ give very different probabilities

Example: Classical Vs Quantum Randomness

- Mixed state:

$$\rho_1 = 1/2\,|0\rangle\langle 0| + 1/2\,|1\rangle\langle 1| = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

- Pure state (equal superposition):

$$\rho_2 = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

- Measured in computational basis $\{|0\rangle, |1\rangle\}$ both give same probabilities (but for ρ_1 is classical randomness while for ρ_2 is quantum randomness).
- Measured in the Hadamard basis $\{|+\rangle, |-\rangle\}$ give very different probabilities
- Difference between maximally mixed and equal superposition!

Density Matrices

Definition: A **density matrix** is a matrix (or operator) ρ that:

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

Definition: A **density matrix** is a matrix (or operator) ρ that:

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

Exercise: Check that these conditions are satisfied

1. for pure density matrices
2. for density matrices of the form $\rho = \sum_i p_i \left|\psi\right\rangle \left\langle\psi\right|$

Mixed States

- **Different** ensembles can result to the **same** density matrix!

Mixed States

- **Different** ensembles can result to the **same** density matrix!

Example: $\rho = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}$

Ensemble 1: $\{p(0) = 3/4, |0\rangle, p(1) = 1/4, |1\rangle\}$

Ensemble 2: $\{p(a) = 1/2, |a\rangle, p(b) = 1/2, |b\rangle\}$ where

$|a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle$

$|b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$

- **Different** ensembles can result to the **same** density matrix!

Example: $\rho = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}$

Ensemble 1: $\{p(0) = 3/4, |0\rangle, p(1) = 1/4, |1\rangle\}$

Ensemble 2: $\{p(a) = 1/2, |a\rangle, p(b) = 1/2, |b\rangle\}$ where

$|a\rangle = \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle$

$|b\rangle = \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle$

Check that: $\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$

Operations and Measurements for Mixed States

- More information will be given in later lectures.
- **Operations**: $\rho \to U\rho U^\dagger$; norm same $\mathrm{Tr}(U\rho U^\dagger) = \mathrm{Tr}(\rho) = 1$

  Example: Evolve by X the state $\rho = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}$.

$$X\rho X^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1/4 & 0 \\ 0 & 3/4 \end{pmatrix}$$

Operations and Measurements for Mixed States

- More information will be given in later lectures.
- **Operations**: $\rho \to U\rho U^\dagger$; norm same $\mathrm{Tr}(U\rho U^\dagger) = \mathrm{Tr}(\rho) = 1$

  Example: Evolve by X the state $\rho = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}$.

$$X\rho X^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1/4 & 0 \\ 0 & 3/4 \end{pmatrix}$$

- **Measurements:** Projective measurement P_1, P_2, at state ρ.

- Probability of outcomes $p_1 = \mathrm{Tr}(P_1\rho)$; $p_2 = \mathrm{Tr}(P_2\rho)$
- State after measurement

$$\rho_1 = P_1\rho P_1 \frac{1}{\mathrm{Tr}(P_1\rho)} \; ; \; \rho_2 = P_2\rho P_2 \frac{1}{\mathrm{Tr}(P_2\rho)}$$

Observables and Expectation Values

- **Observable** $O = O^\dagger$ is a Hermitian matrix

Observables and Expectation Values

- **Observable** $O = O^\dagger$ is a Hermitian matrix
- **Expectation value** of O given pure state $|\psi\rangle$ is given by "sandwich-ing" it:

$$\langle O\rangle_\psi = \langle\psi| O |\psi\rangle$$

Observables and Expectation Values

- **Observable** $O = O^\dagger$ is a Hermitian matrix
- **Expectation value** of O given pure state $|\psi\rangle$ is given by "sandwich-ing" it:

$$\langle O \rangle_\psi = \langle \psi | O | \psi \rangle$$

- **Expectation value** of O given mixed state $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ is given by (cf cyclic trace):

$$\langle O \rangle_\rho = \mathrm{Tr}(O\rho) = \sum_i p_i \langle \psi_i | O | \psi_i \rangle$$

Observables and Expectation Values

- **Observable** $O = O^\dagger$ is a Hermitian matrix
- **Expectation value** of O given pure state $|\psi\rangle$ is given by "sandwich-ing" it:

$$\langle O \rangle_\psi = \langle \psi | O | \psi \rangle$$

- **Expectation value** of O given mixed state $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$ is given by (cf cyclic trace):

$$\langle O \rangle_\rho = \mathrm{Tr}(O\rho) = \sum_i p_i \langle \psi_i | O | \psi_i \rangle$$

- Possible values of measuring the observable are the **eigenvalues**
- Probability of each outcome is given by **projecting on the corresponding eigenspace**