An Introduction to Quantum Computing

Lecture 16:

Density Operators

Paolo Zuliani

Dipartimento di Informatica
Università di Roma "La Sapienza", Rome, Italy

Agenda

- Mixed states and traces
- Density matrices
- The rules of Quantum Mechanics with density matrices
- The von Neumann Entropy and the Holevo bound

Mixed States

Definition

A ket $|v\rangle \in \mathcal{H}$ is a *pure state.*

Mixed States

Definition

A ket $|v\rangle \in \mathcal{H}$ is a *pure state.*

Definition

Let $\{|v_1\rangle, \ldots |v_N\rangle\}$ be pure states and $w_1, \ldots, w_N$ be positive numbers such that $\sum_i w_i = 1$. The *mixed state* ρ is the set:

$$\rho = \{|v_i\rangle, w_i\}_{i=1}^{N}$$

A mixed state tells us that our quantum system is in pure state $|v_i\rangle$ with 'classical' probability w_i.

Mixed States

Rule 3: when measuring observable A on (pure) state $|v\rangle$ we have that

$$\mathrm{Prob}(A = \lambda_i; |v\rangle) = \langle v|P_i v\rangle \qquad (\text{equivalently } \langle A\rangle_v = \langle v|Av\rangle)$$

where P_i is the projector associated to the i-th eigenspace of A.

Mixed States

Rule 3: when measuring observable A on (pure) state $|v\rangle$ we have that

$$\mathrm{Prob}(A = \lambda_i; |v\rangle) = \langle v|P_i v\rangle \qquad (\text{equivalently } \langle A\rangle_v = \langle v|Av\rangle)$$

where P_i is the projector associated to the i-th eigenspace of A.

How about measuring A on a mixed state $\rho = \{|v_i\rangle, w_i\}_{i=1}^{N}$?

Mixed States

Rule 3: when measuring observable A on (pure) state $|v\rangle$ we have that

$$\mathrm{Prob}(A = \lambda_i; |v\rangle) = \langle v|P_i v\rangle \qquad (\text{equivalently } \langle A\rangle_v = \langle v|Av\rangle)$$

where P_i is the projector associated to the i-th eigenspace of A.

How about measuring A on a mixed state $\rho = \{|v_i\rangle, w_i\}_{i=1}^N$?

Assuming the quantum and classical probabilities are independent, we get

$$\mathrm{Prob}(A = \lambda_i; \rho) = \sum_{j=1}^N w_j \mathrm{Prob}(A = \lambda_i; |v_j\rangle) = \sum_{j=1}^N w_j \langle v_j|P_i v_j\rangle$$

Trace of a Linear Operator

Definition

Let $\{e_i\}$ be an orthonormal basis for an Hilbert space $\mathcal{H}$, and A be an operator on $\mathcal{H}$. The *trace* of A is defined

$$\mathrm{tr}(A) = \sum_i \langle e_i | A e_i \rangle$$

Trace of a Linear Operator

Definition

Let $\{e_i\}$ be an orthonormal basis for an Hilbert space $\mathcal{H}$, and A be an operator on $\mathcal{H}$. The *trace* of A is defined

$$\operatorname{tr}(A) = \sum_i \langle e_i | A e_i \rangle$$

Note: it is a generalisation of the usual trace of a matrix.

<u>Exercise</u>: show that $\operatorname{tr}(A)$ is independent of the basis chosen (hence it is well defined!)

Trace of a Linear Operator

Definition

Let $\{e_i\}$ be an orthonormal basis for an Hilbert space $\mathcal{H}$, and A be an operator on $\mathcal{H}$. The *trace* of A is defined

$$\mathrm{tr}(A) = \sum_i \langle e_i | A e_i \rangle$$

Note: it is a generalisation of the usual trace of a matrix.

<u>Exercise</u>: show that $\mathrm{tr}(A)$ is independent of the basis chosen (hence it is well defined!)

Let us rework Rule 3:

$$\langle v | A v \rangle = \langle v | A \sum_i |e_i\rangle\langle e_i|\, v\rangle = \sum_i \langle v | A\, |e_i\rangle\langle e_i|\, v\rangle$$

Trace of a Linear Operator

Definition

Let $\{e_i\}$ be an orthonormal basis for an Hilbert space $\mathcal{H}$, and A be an operator on $\mathcal{H}$. The *trace* of A is defined

$$\mathrm{tr}(A) = \sum_i \langle e_i | A e_i \rangle$$

Note: it is a generalisation of the usual trace of a matrix.

Exercise: show that $\mathrm{tr}(A)$ is independent of the basis chosen (hence it is well defined!)

Let us rework Rule 3:

$$\begin{aligned} \langle v | A v \rangle &= \langle v | A \sum_i | e_i \rangle\langle e_i | \, v \rangle = \sum_i \langle v | A \, | e_i \rangle\langle e_i | \, v \rangle \\ &= \sum_i \langle e_i | v \rangle \langle v | A e_i \rangle = \sum_i \langle e_i | P_v A e_i \rangle = \mathrm{tr}(P_v A) \end{aligned}$$

where $P_v = | v \rangle\langle v |$.

Mixed State Operator

Definition

Let $\{|v_1\rangle, \ldots |v_N\rangle\}$ be pure states and $w_1, \ldots, w_N$ be positive numbers such that $\sum_i w_i = 1$. The *mixed state operator* ρ is defined:

$$\rho = \sum_i w_i P_{v_i} = \sum_i w_i |v_i\rangle\langle v_i|$$

Mixed State Operator

Definition

Let $\{|v_1\rangle, \ldots |v_N\rangle\}$ be pure states and $w_1, \ldots, w_N$ be positive numbers such that $\sum_i w_i = 1$. The *mixed state operator* ρ is defined:

$$\rho = \sum_i w_i P_{v_i} = \sum_i w_i |v_i\rangle\langle v_i|$$

Let us now compute the probability of measuring λ_i on the mixed state ρ:

$$\mathrm{Prob}(A = \lambda_i; \rho) = \sum_{j=1} w_j \langle v_j | P_i v_j \rangle$$

Mixed State Operator

Definition

Let $\{|v_1\rangle, \dots |v_N\rangle\}$ be pure states and $w_1, \dots, w_N$ be positive numbers such that $\sum_i w_i = 1$. The *mixed state operator* ρ is defined:

$$\rho = \sum_i w_i P_{v_i} = \sum_i w_i |v_i\rangle\langle v_i|$$

Let us now compute the probability of measuring λ_i on the mixed state ρ:

$$\mathrm{Prob}(A = \lambda_i; \rho) = \sum_{j=1} w_j \langle v_j | P_i v_j\rangle = \sum_j w_j \,\mathrm{tr}(P_{v_j} P_i)$$

Mixed State Operator

Definition

Let $\{|v_1\rangle, \ldots |v_N\rangle\}$ be pure states and $w_1, \ldots, w_N$ be positive numbers such that $\sum_i w_i = 1$. The *mixed state operator* ρ is defined:

$$\rho = \sum_i w_i P_{v_i} = \sum_i w_i |v_i\rangle\langle v_i|$$

Let us now compute the probability of measuring λ_i on the mixed state ρ:

$$\begin{aligned}\text{Prob}(A = \lambda_i; \rho) &= \sum_{j=1} w_j \langle v_j | P_i v_j \rangle = \sum_j w_j \operatorname{tr}(P_{v_j} P_i) \\ &= \operatorname{tr}(\sum_j w_j P_{v_j} P_i)\end{aligned}$$

Mixed State Operator

Definition

Let $\{|v_1\rangle, \ldots |v_N\rangle\}$ be pure states and $w_1, \ldots, w_N$ be positive numbers such that $\sum_i w_i = 1$. The *mixed state operator* ρ is defined:

$$\rho = \sum_i w_i P_{v_i} = \sum_i w_i |v_i\rangle\langle v_i|$$

Let us now compute the probability of measuring λ_i on the mixed state ρ:

$$\begin{aligned}
\mathrm{Prob}(A = \lambda_i; \rho) &= \sum_{j=1} w_j \langle v_j | P_i v_j \rangle = \sum_j w_j \, \mathrm{tr}(P_{v_j} P_i) \\
&= \mathrm{tr}(\sum_j w_j P_{v_j} P_i) \\
&= \mathrm{tr}(\rho P_i)
\end{aligned}$$

Density Matrices

Definition

A *density matrix* is an operator ρ satisfying:

- ρ is positive (*i.e.*, $\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0$);
- $\mathrm{tr}(\rho) = 1$;
- $[\rho = \rho^\dagger]$ (but this follows from positivity).

Density Matrices

Definition

A *density matrix* is an operator ρ satisfying:

- ρ is positive (*i.e.*, $\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0$);
- $\mathrm{tr}(\rho) = 1$;
- $[\rho = \rho^\dagger]$ (but this follows from positivity).

Let us show that a positive operator ρ is self-adjoint:

Density Matrices

Definition

A *density matrix* is an operator ρ satisfying:

- ρ is positive (*i.e.*, $\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0$);
- $\mathrm{tr}(\rho) = 1$;
- $[\rho = \rho^\dagger]$ (but this follows from positivity).

Let us show that a positive operator ρ is self-adjoint:

$$\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0$$

Density Matrices

Definition

A *density matrix* is an operator ρ satisfying:

- ρ is positive (*i.e.*, $\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0$);
- $\mathrm{tr}(\rho) = 1$;
- $[\rho = \rho^\dagger]$ (but this follows from positivity).

Let us show that a positive operator ρ is self-adjoint:

$$\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0 \quad \Longrightarrow$$
$$\forall v \in \mathcal{H}, \langle v|\rho v\rangle = \langle v|\rho v\rangle^* = \langle \rho v|v\rangle = \langle \rho^\dagger v|v\rangle$$

Density Matrices

Definition

A *density matrix* is an operator ρ satisfying:

- ρ is positive (*i.e.*, $\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0$);
- $\mathrm{tr}(\rho) = 1$;
- $[\rho = \rho^\dagger]$ (but this follows from positivity).

Let us show that a positive operator ρ is self-adjoint:

$$
\begin{aligned}
&\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0 \quad \Longrightarrow \\
&\forall v \in \mathcal{H}, \langle v|\rho v\rangle = \langle v|\rho v\rangle^* = \langle \rho v|v\rangle = \langle \rho^\dagger v|v\rangle \quad \Longrightarrow \\
&\forall v \in \mathcal{H}, \langle \rho v|v\rangle = \langle \rho^\dagger v|v\rangle
\end{aligned}
$$

Density Matrices

Definition

A *density matrix* is an operator ρ satisfying:

- ρ is positive (*i.e.*, $\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0$);
- $\mathrm{tr}(\rho) = 1$;
- $[\rho = \rho^\dagger]$ (but this follows from positivity).

Let us show that a positive operator ρ is self-adjoint:

$$\forall v \in \mathcal{H}, \langle v|\rho v\rangle \geqslant 0 \quad \Longrightarrow$$
$$\forall v \in \mathcal{H}, \langle v|\rho v\rangle = \langle v|\rho v\rangle^* = \langle \rho v|v\rangle = \langle \rho^\dagger v|v\rangle \quad \Longrightarrow$$
$$\forall v \in \mathcal{H}, \langle \rho v|v\rangle = \langle \rho^\dagger v|v\rangle \quad \Longrightarrow \text{(show that } \forall z, \langle x|z\rangle = \langle y|z\rangle \implies x = y)$$
$$\forall v \in \mathcal{H}, \rho v = \rho^\dagger v$$

Density Matrices

Exercise: prove that a mixed state operator is a density matrix.

Density Matrices

Exercise: prove that a mixed state operator is a density matrix.

Any density matrix ρ is self-adjoint, hence can apply the spectral theorem and write:

$$\rho = \sum_i y_i P_{\psi_i}$$

where the $|\psi_i\rangle$'s are an orthonormal basis and the y_i's are probabilities summing to 1.

Density Matrices

Exercise: prove that a mixed state operator is a density matrix.

Any density matrix ρ is self-adjoint, hence can apply the spectral theorem and write:

$$\rho = \sum_i y_i P_{\psi_i}$$

where the $|\psi_i\rangle$'s are an orthonormal basis and the y_i's are probabilities summing to 1.

Note that orthonormality is not required when modelling classically weighted sum of states (*i.e.*, when the system is in state $|\psi_i\rangle$ with probability y_i).

Density Matrices

A density matrix does NOT admit a unique decomposition as a mixed state operator!

Density Matrices

A density matrix does NOT admit a unique decomposition as a mixed state operator!

Example:

Consider density matrix $\rho = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. It is easy to show that:

$$\rho = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

which suggests that our system is in pure state $|0\rangle$ with (classical) probability 50% and in pure state $|1\rangle$ again with (classical) probability 50%.

Density Matrices

A density matrix does NOT admit a unique decomposition as a mixed state operator!

Example:

Consider density matrix $\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. It is easy to show that:

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

which suggests that our system is in pure state $|0\rangle$ with (classical) probability 50% and in pure state $|1\rangle$ again with (classical) probability 50%. However:

$$\rho = \frac{1}{2}\left[\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right] + \frac{1}{2}\left[\frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\right]$$

Density Matrices

A density matrix does NOT admit a unique decomposition as a mixed state operator!

Example:

Consider density matrix $\rho = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. It is easy to show that:

$$\rho = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

which suggests that our system is in pure state $|0\rangle$ with (classical) probability 50% and in pure state $|1\rangle$ again with (classical) probability 50%. However:

$$\rho = \frac{1}{2}\left[\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\right] + \frac{1}{2}\left[\frac{1}{2}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\right]$$

Exercise: verify that the two matrices above are projectors (recall a projector P satisfies $P^2 = P$ and $P = P^\dagger$).

Density Matrices

Proposition

The set of density matrices is convex, i.e., *given density matrices* $\rho_1, \ldots, \rho_N$ *and positive numbers* $w_1, \ldots, w_N$ *such that* $\sum_i w_i = 1$, *then* $\sum_i w_i \rho_i$ *is a density matrix.*

Exercise: prove the proposition above.

Density Matrices

Proposition

The set of density matrices is convex, i.e., *given density matrices* $\rho_1, \ldots, \rho_N$ *and positive numbers* $w_1, \ldots, w_N$ *such that* $\sum_i w_i = 1$, *then* $\sum_i w_i \rho_i$ *is a density matrix.*

Exercise: prove the proposition above.

Density matrices of the form $|\psi\rangle\langle\psi|$ are called *pure states*, the rest are *mixed*.

Density Matrices

Proposition

The set of density matrices is convex, i.e., *given density matrices* $\rho_1, \ldots, \rho_N$ *and positive numbers* $w_1, \ldots, w_N$ *such that* $\sum_i w_i = 1$, *then* $\sum_i w_i \rho_i$ *is a density matrix.*

Exercise: prove the proposition above.

Density matrices of the form $|\psi\rangle\langle\psi|$ are called *pure states*, the rest are *mixed*.

Proposition

Let ρ *be a density matrix. Then* $\mathrm{tr}(\rho^2) \leqslant 1$ *and* $\mathrm{tr}(\rho^2) = 1$ *iff* ρ *is a pure state.*

Density Matrices

Proposition

The set of density matrices is convex, i.e., *given density matrices* $\rho_1, \ldots, \rho_N$ *and positive numbers* $w_1, \ldots, w_N$ *such that* $\sum_i w_i = 1$, *then* $\sum_i w_i \rho_i$ *is a density matrix.*

Exercise: prove the proposition above.

Density matrices of the form $|\psi\rangle\langle\psi|$ are called *pure states*, the rest are *mixed*.

Proposition

Let ρ *be a density matrix. Then* $\mathrm{tr}(\rho^2) \leqslant 1$ *and* $\mathrm{tr}(\rho^2) = 1$ *iff* ρ *is a pure state.*

Thus, a state ρ is mixed iff $\mathrm{tr}(\rho^2) < 1$.

Density Matrices

Proposition

Let ρ be a density matrix. Then $\mathrm{tr}(\rho^2) \leqslant 1$ *and* $\mathrm{tr}(\rho^2) = 1$ *iff* ρ *is a pure state.*

Let us prove it.

Density Matrices

Proposition

Let ρ be a density matrix. Then $\mathrm{tr}(\rho^2) \leqslant 1$ and $\mathrm{tr}(\rho^2) = 1$ iff ρ is a pure state.

Let us prove it.
ρ is positive hence self-adjoint, so by the spectral theorem we can write:

$$\rho = \sum_i \lambda_i P_i$$

where the λ_i's are the eigenvalues and the P_i's are the eigenspace projectors of ρ, respectively.

Density Matrices

Proposition

Let ρ be a density matrix. Then $\mathrm{tr}(\rho^2) \leqslant 1$ and $\mathrm{tr}(\rho^2) = 1$ iff ρ is a pure state.

Let us prove it.
ρ is positive hence self-adjoint, so by the spectral theorem we can write:

$$\rho = \sum_i \lambda_i P_i$$

where the λ_i's are the eigenvalues and the P_i's are the eigenspace projectors of ρ, respectively. The eigenvalues are all positive and satisfy $\sum_i \lambda_i = 1$ since $\mathrm{tr}(\rho) = 1$.

Density Matrices

Proposition

Let ρ be a density matrix. Then $\mathrm{tr}(\rho^2) \leqslant 1$ and $\mathrm{tr}(\rho^2) = 1$ iff ρ is a pure state.

Let us prove it.
ρ is positive hence self-adjoint, so by the spectral theorem we can write:

$$\rho = \sum_i \lambda_i P_i$$

where the λ_i's are the eigenvalues and the P_i's are the eigenspace projectors of ρ, respectively. The eigenvalues are all positive and satisfy $\sum_i \lambda_i = 1$ since $\mathrm{tr}(\rho) = 1$.

$$\mathrm{tr}(\rho\rho) = \mathrm{tr}(\rho \sum_i \lambda_i P_i) = \mathrm{tr}(\sum_{i,j} \lambda_i \lambda_j P_i P_j) = \mathrm{tr}(\sum_i \lambda_i^2 P_i) = \sum_i \lambda_i^2 \leqslant 1.$$

Density Matrices

Proposition

Let ρ be a density matrix. Then $\mathrm{tr}(\rho^2) \leqslant 1$ and $\mathrm{tr}(\rho^2) = 1$ iff ρ is a pure state.

Let us prove it.
ρ is positive hence self-adjoint, so by the spectral theorem we can write:

$$\rho = \sum_i \lambda_i P_i$$

where the λ_i's are the eigenvalues and the P_i's are the eigenspace projectors of ρ, respectively. The eigenvalues are all positive and satisfy $\sum_i \lambda_i = 1$ since $\mathrm{tr}(\rho) = 1$.

$$\mathrm{tr}(\rho\rho) = \mathrm{tr}(\rho \sum_i \lambda_i P_i) = \mathrm{tr}(\sum_{i,j} \lambda_i \lambda_j P_i P_j) = \mathrm{tr}(\sum_i \lambda_i^2 P_i) = \sum_i \lambda_i^2 \leqslant 1.$$

Now, $\sum_i \lambda_i^2 = 1$ iff there is only one term in the sum, *i.e.*, ρ is a pure state.

The Rules of Quantum Mechanics with Density Matrices

Rule 1: The state space of Quantum Mechanics is a Hilbert space $\mathcal{H}$ (the "physical" state of a system is a **density matrix**).

The Rules of Quantum Mechanics with Density Matrices

Rule 1: The state space of Quantum Mechanics is a Hilbert space $\mathcal{H}$ (the "physical" state of a system is a **density matrix**).

Rule 2: A closed system evolves over time under **unitary transformations**. Applying unitary operator U to state ρ has the effect

$$\rho \to U\rho U^{\dagger}.$$

The Rules of Quantum Mechanics with Density Matrices

Rule 1: The state space of Quantum Mechanics is a Hilbert space $\mathcal{H}$ (the "physical" state of a system is a **density matrix**).

Rule 2: A closed system evolves over time under **unitary transformations**. Applying unitary operator U to state ρ has the effect

$$\rho \to U\rho U^\dagger.$$

Here is "why":

$$\{|\psi_i\rangle, w_i\} \xrightarrow{U} \{U|\psi_i\rangle, w_i\}$$

The Rules of Quantum Mechanics with Density Matrices

Rule 1: The state space of Quantum Mechanics is a Hilbert space $\mathcal{H}$ (the "physical" state of a system is a **density matrix**).

Rule 2: A closed system evolves over time under **unitary transformations**. Applying unitary operator U to state ρ has the effect

$$\rho \to U\rho U^\dagger.$$

Here is "why":

$$\{|\psi_i\rangle, w_i\} \xrightarrow{U} \{U|\psi_i\rangle, w_i\}$$

$$\sum_i w_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i w_i U|\psi_i\rangle (U|\psi_i\rangle)^\dagger = \sum_i w_i U|\psi_i\rangle\langle\psi_i| U^\dagger = U\rho U^\dagger$$

The Rules of Quantum Mechanics with Density Matrices

Rule 1: The state space of Quantum Mechanics is a Hilbert space $\mathcal{H}$ (the "physical" state of a system is a **density matrix**).

Rule 2: A closed system evolves over time under **unitary transformations**. Applying unitary operator U to state ρ has the effect

$$\rho \to U\rho U^\dagger.$$

Here is "why":

$$\{|\psi_i\rangle, w_i\} \xrightarrow{U} \{U|\psi_i\rangle, w_i\}$$

$$\sum_i w_i |\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i w_i U|\psi_i\rangle (U|\psi_i\rangle)^\dagger = \sum_i w_i U|\psi_i\rangle\langle\psi_i| U^\dagger = U\rho U^\dagger$$

The (linear) function that maps ρ to $U\rho U^\dagger$ is called a *superoperator*.

The Rules of Quantum Mechanics with Density Matrices

Rule 3: A measurement is described by a collection $M = \{M_m\}$ of **measurement operators** that satisfy $\sum_m M_m^\dagger M_m = I$ (where m indexes the measurement outcomes).

The Rules of Quantum Mechanics with Density Matrices

Rule 3: A measurement is described by a collection $M = \{M_m\}$ of **measurement operators** that satisfy $\sum_m M_m^\dagger M_m = I$ (where m indexes the measurement outcomes).

The probability of measuring outcome m in state ρ is:

$$\text{Prob}(M = m; \rho) = \text{tr}(M_m^\dagger M_m \rho)$$

The Rules of Quantum Mechanics with Density Matrices

Rule 3: A measurement is described by a collection $M = \{M_m\}$ of **measurement operators** that satisfy $\sum_m M_m^\dagger M_m = I$ (where m indexes the measurement outcomes).

The probability of measuring outcome m in state ρ is:

$$\mathrm{Prob}(M = m; \rho) = \mathrm{tr}(M_m^\dagger M_m \rho)$$

The state ρ_m resulting after obtaining measurement outcome m is:

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}$$

The Rules of Quantum Mechanics with Density Matrices

Rule 3: A measurement is described by a collection $M = \{M_m\}$ of **measurement operators** that satisfy $\sum_m M_m^\dagger M_m = I$ (where m indexes the measurement outcomes).

The probability of measuring outcome m in state ρ is:

$$\mathrm{Prob}(M = m; \rho) = \mathrm{tr}(M_m^\dagger M_m \rho)$$

The state ρ_m resulting after obtaining measurement outcome m is:

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}$$

Exercise: verify that the probability Rule 3 above reduces to the usual rule for a self-adjoint observable (the measurement operators are simply the projectors on the eigenspaces).

Shannon Entropy

After Claude Shannon (electrical engineer; 1916-2001).

We have a source that produces symbols (from a finite alphabet) via a random process:

$$symb_1 \; @ \; p_1, symb_2 \; @ \; p_2, \ldots, symb_n \; @ \; p_n$$

The source can be thus thought of as a random variable.

How can we quantify the resources needed to store the symbols generated?

Shannon Entropy

After Claude Shannon (electrical engineer; 1916-2001).

We have a source that produces symbols (from a finite alphabet) via a random process:

$$symb_1 \,@\, p_1, symb_2 \,@\, p_2, \ldots, symb_n \,@\, p_n$$

The source can be thus thought of as a random variable.

How can we quantify the resources needed to store the symbols generated?

Definition

Given a random variable $X = \{s_i \,@\, p_i\}$, the <u>Shannon entropy</u> is

$$H(X) = -\sum_i p_i \log p_i$$

Note: if $p_i = 0$ then we assume $p_i \log p_i = 0$.

Shannon Entropy

Example:
Consider a binary source, *i.e.*, it emits only two symbols:

$$\{\text{Pistacchio, } @\, p;\ \text{Stracciatella}\, @\, (1-p)\}$$

Shannon Entropy

Example:
Consider a binary source, *i.e.*, it emits only two symbols:

$$\{\text{Pistacchio, @}\, p;\ \text{Stracciatella @}\, (1-p)\}$$

$$H(p) = -p \log p - (1-p)\log(1-p)$$

$H(p)$ is largest for $p = \frac{1}{2}$ and smallest for $p = 0$ (or $p = 1$).

Shannon Entropy

Definition

The joint entropy of random variables X, Y is:

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y)$$

Definition

The mutual information of random variables X, Y is:

$$H(X : Y) = H(X) + H(Y) - H(X, Y)$$

$H(X : Y)$ is informally the amount of information that X and Y have in common.

The von Neumann Entropy

After John (János) von Neumann (mathematician; 1903-1957).

Definition

The entropy of a density matrix ρ is:

$$S(\rho) = -\operatorname{tr}(\rho \log \rho)$$

or equivalently:

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i$$

where the λ_i's are the eigenvalues of ρ.

The von Neumann Entropy

After John (János) von Neumann (mathematician; 1903-1957).

Definition

The entropy of a density matrix ρ is:

$$S(\rho) = -\operatorname{tr}(\rho \log \rho)$$

or equivalently:

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i$$

where the λ_i's are the eigenvalues of ρ.

<u>Example</u>: consider the density matrix I/n in an n-dimensional Hilbert space.

$$S(I/n) = -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} = -\frac{1}{n} \log \frac{1}{n} \sum_{i=1}^{n} = -\log \frac{1}{n} = \log n$$

In fact, I/n is the state with highest entropy.

Holevo Bound

Context: a game between two parties, Alice and Bob.

Alice has a random source of symbols $X = 1, \ldots, n$ with probability $p_1, \ldots, p_n$. Bob aims at determining the value of X.

Holevo Bound

Context: a game between two parties, Alice and Bob.

Alice has a random source of symbols $X = 1, \ldots, n$ with probability $p_1, \ldots, p_n$. Bob aims at determining the value of X.

Alice prepares a state ρ_X chosen from $\rho_1, \ldots, \rho_n$ and gives it to Bob, who performs a quantum measurement, denoted Y, to guess X as best as he can.

Holevo Bound

Context: a game between two parties, Alice and Bob.

Alice has a random source of symbols $X = 1, \ldots, n$ with probability $p_1, \ldots, p_n$. Bob aims at determining the value of X.

Alice prepares a state ρ_X chosen from $\rho_1, \ldots, \rho_n$ and gives it to Bob, who performs a quantum measurement, denoted Y, to guess X as best as he can.

Classically: $H(X : Y) \leqslant H(X)$, so Bob "wins" if $H(X : Y) = H(X)$. (And classical states can be easily distinguished.)

Holevo Bound

Context: a game between two parties, Alice and Bob.

Alice has a random source of symbols $X = 1, \ldots, n$ with probability $p_1, \ldots, p_n$. Bob aims at determining the value of X.

Alice prepares a state ρ_X chosen from $\rho_1, \ldots, \rho_n$ and gives it to Bob, who performs a quantum measurement, denoted Y, to guess X as best as he can.

Classically: $H(X : Y) \leqslant H(X)$, so Bob "wins" if $H(X : Y) = H(X)$. (And classical states can be easily distinguished.)

Quantumly: non-orthogonal quantum states cannot be distinguished with certainty! (Remember the BB84 quantum key-distribution protocol.)

Holevo Bound

After Alexander Holevo (physicist; 1943 -).

Theorem

Suppose Alice prepares ρ_X for $X = 1, \ldots, n$ with probability $p_1, \ldots, p_n$. Suppose Bob performs a measurement on ρ_X with outcome Y. Then:

$$H(X : Y) \leqslant S(\rho) - \sum_i p_i \log S(\rho_i)$$

where $\rho = \sum_i p_i \rho_i$.

Holevo Bound

After Alexander Holevo (physicist; 1943 -).

Theorem

Suppose Alice prepares ρ_X for $X = 1, \ldots, n$ with probability $p_1, \ldots, p_n$. Suppose Bob performs a measurement on ρ_X with outcome Y. Then:

$$H(X : Y) \leqslant S(\rho) - \sum_i p_i \log S(\rho_i)$$

where $\rho = \sum_i p_i \rho_i$.

One can also show that $S(\rho) - \sum_i p_i \log S(\rho_i) \leqslant H(X)$ (with equality iff the states are orthogonal). Thus, in general Bob cannot learn X with certainty.