Lecture 2
Fundamentals of quantum information

January 14, 2020

The Density Matrix

- How can we model the quantum state after a measurement ?
  ex: $|0\rangle$ with prob. $\frac{1}{2}$ and $|1\rangle$ with prob. $\frac{1}{2}$?
- How can we describe the quantum state relative to a subsystem?
  ex: the first qubit of the EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

What we want is a perfect and concise description of a quantum state

$2 \neq$ states can not be distinguished iff they have the same description

Observable

- An equivalent description of measurements
- Given by a self-adjoint operator $\mathbf{M}$ ($\mathbf{M}^* = \mathbf{M}$)
- $\mathbf{M}$ is diagonalizable in an orthonormal basis, the orthogonal projections $\mathbf{P}_\lambda$ onto the eigenspaces V_λ determine the measurement
- Output of the measurement : eigenvalue λ. Measurement $= \lambda$ with probability $p_\lambda \stackrel{\text{def}}{=} \|\mathbf{P}_\lambda |\psi\rangle\|^2$

$$
\begin{aligned}
|\psi\rangle &= \sum_\lambda \mathbf{P}_\lambda |\psi\rangle \\
\mathbf{M}|\psi\rangle &= \sum_\lambda \lambda \mathbf{P}_\lambda |\psi\rangle \\
\langle M \rangle_{|\psi\rangle} &\stackrel{\text{def}}{=} \sum_\lambda p_\lambda \lambda \\
&= \sum_\lambda \lambda \|\mathbf{P}_\lambda |\psi\rangle\|^2 \\
&= \langle\psi| \mathbf{M} |\psi\rangle
\end{aligned}
$$

Measurements on a probability mixture of quantum states

- Quantum state ρ probabilistic mixture of quantum states $|\psi_j\rangle$: $\rho = |\psi_j\rangle$ with probability p_j. We have for any observable $\mathbf{M}$:

$$
\begin{aligned}
\langle \mathbf{M} \rangle_\rho &= \sum_j p_j \langle \mathbf{M} \rangle_{|\psi_j\rangle} \\
&= \sum_j p_j \langle \psi_j | \mathbf{M} | \psi_j \rangle \\
&= \sum_j p_j \mathbf{Tr} \langle \psi_j | \mathbf{M} | \psi_j \rangle \\
&= \sum_j p_j \mathbf{Tr} \left(\mathbf{M} | \psi_j \rangle \langle \psi_j | \right) \\
&= \mathbf{Tr} \left(\mathbf{M} \sum_j p_j | \psi_j \rangle \langle \psi_j | \right)
\end{aligned}
$$

$\Rightarrow$ define $\rho \stackrel{\text{def}}{=} \sum_j p_j |\psi_j\rangle \langle \psi_j|$

The density matrix

Définition[**density matrix**] The density matrix ρ corresponding to a probabilistic mixture of states $|\psi_j\rangle$, the corresponding quantum state being equal to $|\psi_j\rangle$ with probability p_j is given by

$$\boxed{\rho \stackrel{\text{def}}{=} \sum_j p_j \, |\psi_j\rangle \, \langle\psi_j|}$$

The density matrix of a qubit

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad \langle\psi| = \begin{pmatrix} \bar{\alpha} & \bar{\beta} \end{pmatrix}$$

$$|\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix} = \begin{pmatrix} \alpha\overline{\alpha} & \alpha\overline{\beta} \\ \overline{\alpha}\beta & \beta\overline{\beta} \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \alpha\overline{\beta} \\ \overline{\alpha}\beta & |\beta|^2 \end{pmatrix}$$

Exercise

Compute the density matrix of

1. the probabilistic mixture of $|0\rangle$ (prob $\frac{1}{2}$) and $|1\rangle$ (prob $\frac{1}{2}$)
2. the probabilistic mixture of $|+\rangle \stackrel{\text{def}}{=} \frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}$ (prob $\frac{1}{2}$) and $|-\rangle \stackrel{\text{def}}{=} \frac{|0\rangle}{\sqrt{2}} - \frac{|1\rangle}{\sqrt{2}}$
3. What can you conclude ?

Characterizations of density matrices

Theorem 1. *An operator ρ acting on a Hilbert space $\mathcal{H}$ is a density operator iff*

1. *ρ is self-adjoint*
2. *ρ is positive semidefinite*
3. *$\mathbf{Tr}(\rho) = 1$*

- $\mathbf{Tr}(\rho) = 1$

$$\begin{aligned}
\mathbf{Tr}\left(\sum_{j=1}^{k} p_j \left|\psi_j\right\rangle \left\langle\psi_j\right|\right) &= \sum_{j=1}^{k} p_j Tr(\left|\psi_j\right\rangle \left\langle\psi_j\right|) \\
&= \sum_{j=1}^{k} p_j \mathbf{Tr}(\langle\psi_j|\psi_j\rangle) \\
&= 1
\end{aligned}$$

- ρ is positive semidefinite

$$\begin{aligned}
\text{If} \quad \rho &= \sum_{j=1}^{k} p_j \left|\psi_j\right\rangle \left\langle\psi_j\right| \\
\text{then for any } \left|\phi\right\rangle \quad \left\langle\phi\right| \rho \left|\phi\right\rangle &= \sum_{j=1}^{k} p_j \left\langle\phi|\psi_j\right\rangle \left\langle\psi_j|\phi\right\rangle \\
&= \sum_{j=1}^{k} p_j \left|\left\langle\phi|\psi_j\right\rangle\right|^2 \geq 0
\end{aligned}$$

Pure and mixed states

Définition[**pure state**] A quantum system whose state $|\psi\rangle$ is known exactly is said to be in pure state.

Définition[**mixed state**] A quantum system which is not in pure state is said to be in mixed state.

Theorem 2.

$$\begin{aligned} \mathbf{Tr}(\rho^2) &\leq 1 \\ \mathbf{Tr}(\rho^2) &= 1 \Leftrightarrow \rho \textit{ is a pure state} \\ \mathbf{Tr}(\rho^2) &< 1 \Leftrightarrow \rho \textit{ is a mixed state} \end{aligned}$$

Exercise

Prove the previous theorem.

The Bloch ball representation

$$\sigma_x \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y \stackrel{\text{def}}{=} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Let $\mathbf{a} \stackrel{\text{def}}{=} (a_x, a_y, a_z)$ (Bloch vector) $\sigma \stackrel{\text{def}}{=} (\sigma_x, \sigma_y, \sigma_z)$

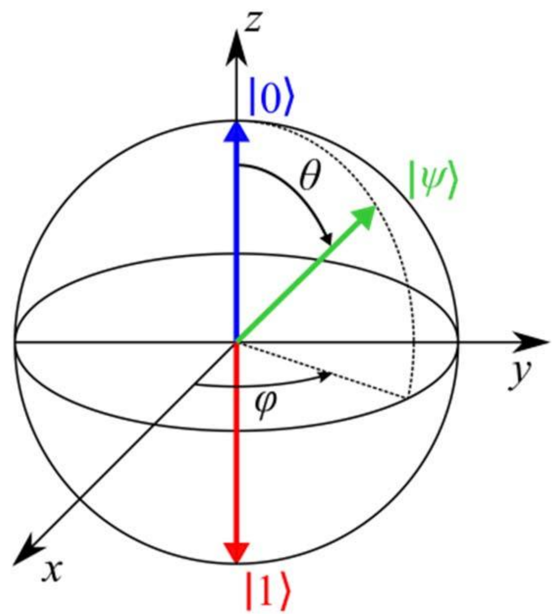
$$\begin{aligned}
\mathbf{Tr}\rho = 1 \ + \mathbf{Tr}(\sigma_*) = 0 \Rightarrow \rho &= \frac{1}{2}(\mathbf{Id} + \mathbf{a} \cdot \sigma) \\
&= \frac{1}{2}\mathbf{Id} + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z \\
&= \frac{1}{2}\begin{pmatrix} 1 + a_z & a_x - ia_y \\ a_x + ia_y & 1 - a_z \end{pmatrix} \\
\det \rho &= \frac{1}{4}(1 - ||\mathbf{a}||^2) \\
\mathbf{Tr}\rho^2 &= \frac{1}{2}(1 + ||\mathbf{a}||^2)
\end{aligned}$$

- ρ is a density matrix iff $||\mathbf{a}|| \leq 1$, ρ is a pure state iff $||\mathbf{a}|| = 1$

Bloch ball representation : ρ is represented by $\mathbf{a}$

The Bloch ball

$$|\psi\rangle = \cos\theta/2\,|0\rangle + e^{i\phi}\sin\theta/2\,|1\rangle$$



Projective measurement

$$\mathbf{M} = \sum_\lambda \lambda \mathbf{P}_\lambda$$

- Initial state $|\psi\rangle$. We measure λ with probability

$$\begin{aligned} p_\lambda &= \| \mathbf{P}_\lambda |\psi\rangle \|^2 \\ &= \langle\psi| \mathbf{P}_\lambda^2 |\psi\rangle \\ &= \mathbf{Tr}(\mathbf{P}_\lambda^2 |\psi\rangle \langle\psi|) \end{aligned}$$

  and the output is $|\psi_\lambda\rangle \stackrel{\text{def}}{=} \frac{\mathbf{P}_\lambda|\psi\rangle}{\|\mathbf{P}_\lambda|\psi\rangle\|} = \frac{\mathbf{P}_\lambda|\psi\rangle}{\sqrt{p_\lambda}}$

- Output is a probabilistic mixtures of states ψ_λ with prob. p_λ.

$$\begin{aligned} \rho &= \sum_\lambda p_\lambda |\psi_\lambda\rangle \langle\psi_\lambda| \\ &= \sum_\lambda p_\lambda \frac{1}{p_\lambda} \mathbf{P}_\lambda |\psi\rangle \langle\psi| \mathbf{P}_\lambda \\ &= \sum_\lambda \mathbf{P}_\lambda |\psi\rangle \langle\psi| \mathbf{P}_\lambda \end{aligned}$$

Measurement for a density operator ρ

$$
\begin{aligned}
\mathbf{M} &= \sum_{\lambda} \lambda \mathbf{P}_{\lambda} \\
\mathbf{P}_{\lambda}^{2} &= \mathbf{P}_{\lambda} \\
\mathbf{P}_{\lambda}^{*} &= \mathbf{P}_{\lambda} \\
\sum_{\lambda} \mathbf{P}_{\lambda} &= \mathbf{Id} \\
\rho' &= \sum_{\lambda} \mathbf{P}_{\lambda}\, \rho\, \mathbf{P}_{\lambda}
\end{aligned}
$$

Unitary Evolution

$$
\begin{aligned}
|\psi\rangle &\rightarrow \mathbf{U}\,|\psi\rangle \\
\rho = |\psi\rangle\,\langle\psi| &\mapsto \mathbf{U}\,|\psi\rangle\,\langle\psi|\,\mathbf{U}^* \\
\mathbf{U}^*\mathbf{U} &= \mathbf{Id}
\end{aligned}
$$

In general

$$\boxed{\rho' = \mathbf{U}\rho\mathbf{U}^*}$$

CPTP operation

- Most general quantum operation = Completely positive trace preserving (CPTP) operation

Définition A CPTP map Φ is defined from a collection of matrices $\mathbf{A}_1, \cdots, \mathbf{A}_k$ such that

$$\sum_{j=1}^{k} \mathbf{A}_j^* \mathbf{A}_j = \mathbf{Id}$$

and

$$\boxed{\Phi(\rho) \stackrel{\text{def}}{=} \sum_{j=1}^{k} \mathbf{A}_j \rho \mathbf{A}_j^*}$$

Exercise

Let

$$\mathbf{A}_0 = \mathbf{Id} \otimes |0\rangle \quad \mathbf{A}_1 = \mathbf{Id} \otimes |1\rangle$$

1. Show that they define a CPTP map as $\Phi(\rho) = \mathbf{A}_0 \rho \mathbf{A}_0^* + \mathbf{A}_1 \rho \mathbf{A}_1^*$
2. What is the effect of this map on $\sigma_1 \otimes \sigma_2$?

Partial trace = reduction to a subsystem

Problem 1. $\rho_{AB} \in \mathcal{A} \otimes \mathcal{B}$, *what is the quantum state with respect to* $\mathcal{A}$ *?*

Answer:

$$\begin{aligned} \rho_A &\stackrel{\text{def}}{=} \mathbf{Tr}_B(\rho_{AB}) \quad \text{where} \\ \mathbf{Tr}_B(X \otimes Y) &= \mathbf{Tr}(Y)X \end{aligned}$$

This is a CPTP map

$$
\begin{aligned}
\mathbf{Tr}_B(\rho) &= \sum_a \mathbf{Id} \otimes \langle a| \;\; \rho \; \mathbf{Id} \otimes |a\rangle \\
&= \sum_a \mathbf{A}_a \rho \mathbf{A}_a^* \\
\mathbf{A}_a &= \mathbf{Id} \otimes \langle a| \\
\sum_a \mathbf{A}_a^* \mathbf{A}_a &= \mathbf{Id}
\end{aligned}
$$

Where does this expression come from ?

- $\mathbf{M}$ an observable on system A and $\tilde{\mathbf{M}}$ the corresponding observable for the composite system AB

$$\tilde{\mathbf{M}} = \sum_{\lambda} \lambda(\mathbf{P}_{\lambda} \otimes \mathbf{Id})$$

Physical consistency

$$\langle \mathbf{M} \rangle_{\rho_A} = \langle \tilde{\mathbf{M}} \rangle_{\rho_{AB}}$$

$$\begin{aligned} \langle \mathbf{M} \rangle_{\rho_A} &= \mathbf{Tr}(\mathbf{M}\rho_A) \\ \langle \tilde{\mathbf{M}} \rangle_{\rho_A} &= \mathbf{Tr}(\mathbf{M} \otimes \mathbf{Id}\rho_{AB}) \end{aligned}$$

Exercise

Consider the EPR pair

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

1. Compute the density matrix ρ_{AB} of the EPR pair.
2. Compute the reduced density matrices ρ_A and ρ_B with respect to the first and second qubit respectively
3. Is $\rho_{AB} = \rho_A \otimes \rho_B$?

Exercise : teleportation

1. Compute the reduced density operator of Bob's system once Alice has performed her measurement but before he has learned ab
2. What can you conclude ?

Schmidt decomposition

Theorem 3. *$\forall \left|\psi\right\rangle \in \mathcal{A} \otimes \mathcal{B}$, $\exists! d$, an orthonormal set $\left|a_1\right\rangle, \cdots, \left|a_d\right\rangle \in \mathcal{A}$ and an orthornormal set $\left|b_1\right\rangle, \cdots, \left|b_d\right\rangle \in \mathcal{A}$ and positive $\lambda_1, \cdots, \lambda_d$ such that*

$$\left|\psi\right\rangle = \sum_{i=1}^{d} \lambda_i \left|a_i\right\rangle \left|b_i\right\rangle \tag{1}$$

Exercise

Consider$|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$

1. Consider $\rho_A = \mathbf{Tr}_{\mathcal{B}} |\psi\rangle \langle\psi|$. Show that we can write

$$\rho_A = \sum_{j=1}^{n} p_j |\psi_j\rangle \langle\psi_j|$$

   for a certain orthonormal set $\{|\psi_1\rangle, \cdots, |\psi_k\rangle\}$ and a certain probability vector $(p_1, \ldots, p_k)$
2. Show that we can write $|\psi\rangle$ as

$$|\psi\rangle = \sum_{j=1}^{n} |\mu_j\rangle |\nu_j\rangle$$

   for some choice of vectors $\nu_1, \cdots, \nu_n$.

The Schmidt number

Définition[**Schmidt number**] The number of non zero λ_i's is called the Schmidt number of the decomposition. This number does not depend on the decomposition and it depends only on $|\psi\rangle$.

Theorem 4. *A pure state $|\psi\rangle$ is entangled iff its Schmidt number is > 1.*

Exercise

Find the Schmidt decomposition of the states

1. $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
2. $\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$
3. $\frac{|00\rangle+|01\rangle+|10\rangle}{\sqrt{3}}$

Bit commitment

- Alice and Bob do not trust each other
- Alice has chosen a bit b
- Right now she does not want to reveal b to Bob, but wants to convince him that indeed she chose b and not $1 - b$
- Much later Alice reveals b to Bob and Bob is convinced that this is indeed the value she chose in the past

The protocol must be

- Binding : Alice should not be able to change the b she committed
- Concealing : Bob should not be able to identify b until Alice reveals it

Very useful tool in cryptography

- coin flipping
- zero knowledge proofs
- secure multiparty computation...

Can be done classically under computational security assumptions

Bit commitment with a safe

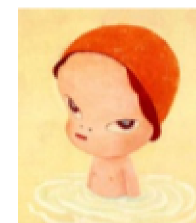
Commit phase

- Alice writes x on a piece of paper
- She puts the paper in a safe. She is the only one to have the code of the safe
- she hands the safe to Bob

$x \in \{0, 1\}$

$\longrightarrow$

$\longrightarrow$



Reveal phase

- Alice reveals x and the code to unlock the safe
- Bob opens the safe to check x

Unconditionally secure bit quantum commitment protocol ?

$$
\begin{aligned}
S_0 &\stackrel{\text{def}}{=} \{|0\rangle, |1\rangle\} \\
S_1 &\stackrel{\text{def}}{=} \{|+\rangle, |-\rangle\}, \text{ with} \\
|+\rangle &\stackrel{\text{def}}{=} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
|-\rangle &\stackrel{\text{def}}{=} \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\end{aligned}
$$

When Alice wants to commit to b

1. Commit phase : Alice choose $|\psi\rangle$ uniformly at random in S_b and sends $|\psi\rangle$ to Bob
2. Reveal phase : Alice reveals ab to Bob where ab is a classical description of $|\psi\rangle$:

$$
\begin{aligned}
00 &\leftrightarrow |0\rangle \\
10 &\leftrightarrow |1\rangle \\
01 &\leftrightarrow |+\rangle \\
11 &\leftrightarrow |-\rangle
\end{aligned}
$$

3. Verification phase : Bob measures $|\psi\rangle$ in the basis S_b

Exercise (warm up)

Suppose that $|\phi\rangle$ and $|\phi\rangle \in \mathcal{A} \otimes \mathcal{B}$ satsify

$$\mathbf{Tr}_{\mathcal{B}} |\phi\rangle \langle\phi| = \mathbf{Tr}_{\mathcal{B}} |\psi\rangle \langle\psi| .$$

Show that there exists a unitary $\mathbf{U}$ such that

$$(\mathbf{Id} \otimes \mathbf{U}) |\phi\rangle = |\psi\rangle .$$

Exercise

1. Verify that the protocol is concealing
2. Find a cheating strategy for Alice
3. Use the previous exercise to show that there is always a cheating strategy for Alice, irrespective of the protocol whenever the protocol is concealing

The EPR paradox

Alice		Bob
$Q = \pm 1$	$\longleftrightarrow$	$S = \pm 1$
$R = \pm 1$		$T = \pm 1$

Exercise: the Bell inequality

1. Show that $QS + RS + RT - QT = \pm 2$. You may use that $QS + RS + RT - QT = (Q + R)S + (R - Q)T$
2. Deduce the Bell inequality $\boxed{\langle QS\rangle_+\langle RS\rangle_+\langle RT\rangle_-\langle QT\rangle_\leq 2}$

The quantum experiment

$$
\begin{aligned}
|\psi\rangle &\stackrel{\text{def}}{=} \frac{|01\rangle - |10\rangle}{\sqrt{2}} \\
\text{Alice} &: \text{first qubit} \\
\text{Bob} &: \text{second qubit} \\
Q &\stackrel{\text{def}}{=} \text{meas. according to } \sigma_Z \\
R &\stackrel{\text{def}}{=} \text{meas. according to } \sigma_X \\
S &\stackrel{\text{def}}{=} \text{meas. according to } \frac{-\sigma_Z - \sigma_X}{\sqrt{2}} \\
T &\stackrel{\text{def}}{=} \text{meas. according to } \frac{\sigma_Z - \sigma_X}{\sqrt{2}}
\end{aligned}
$$

What is $\langle QS\rangle_{+}\langle RS\rangle_{+}\langle RT\rangle_{-}\langle QT\rangle_{?}$

realism and locality

(1) realism assumption: the physical properties have definite values Q, R, S and T which exist independent of observation.

(2) locality assumption Alice measurement does not influence Bob's measurement.

One of these assumptions is violated by these quantum experiments.

Exercise : a maximal violation of Bell's inequality

Let $\mathbf{A}_0$, $\mathbf{A}_1$, $\mathbf{B}_0$, $\mathbf{B}_1$ be observables with eigenvalues in $[-1, 1]$ and $|\psi\rangle$ be a quantum state upon which the $\mathbf{A}_i \otimes \mathbf{B}_j$'s act. Let

$$\mathbf{M} \stackrel{\text{def}}{=} \mathbf{A}_0 \otimes \mathbf{B}_0 + \mathbf{A}_0 \otimes \mathbf{B}_1 + \mathbf{A}_1 \otimes \mathbf{B}_0 - \mathbf{A}_1 \otimes \mathbf{B}_1$$

1. Show that $\langle\psi| \mathbf{M} |\psi\rangle \leq \|\mathbf{M} |\psi\rangle\|$
2. Show that $\|\mathbf{M} |\psi\rangle\| \leq \||\phi_0\rangle + |\phi_1\rangle\| + \||\phi_0\rangle - |\phi_1\rangle\|$ for $|\phi_b\rangle \stackrel{\text{def}}{=} (\mathbf{Id} \otimes \mathbf{B}_b) |\psi\rangle$.
3. Deduce from this Tsirelson's inequality, namely

$$\langle \mathbf{A}_0 \otimes \mathbf{B}_0 \rangle_{|\psi\rangle} + \langle \mathbf{A}_0 \otimes \mathbf{B}_1 \rangle_{|\psi\rangle} + \langle \mathbf{A}_1 \otimes \mathbf{B}_0 \rangle_{|\psi\rangle} - \langle \mathbf{A}_1 \otimes \mathbf{B}_1 \rangle_{|\psi\rangle} \leq 2\sqrt{2} \qquad (2)$$