Master lecture: Elements of quantum information theory

Density operators

A system is in state $|\psi_i\rangle$ with probability p_i.

Let P_m be a projector. Prob. of measurement result m:

$$p(m) = \sum_i p_i \langle\psi_i|P_m|\psi_i\rangle = tr\Big[P_m\Big(\sum_i p_i|\psi_i\rangle\langle\psi_i|\Big)\Big] \equiv tr(P_m\rho)$$

where the density op.

$$\boxed{\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|}$$

$$\langle\psi_i|P_m|\psi_i\rangle = \sum_k \langle\psi_i|k\rangle\langle k|P_m|\psi_i\rangle = \sum_k \langle k|P_m|\psi_i\rangle\langle\psi_i|k\rangle = tr(P_m|\psi_i\rangle\langle\psi_i|)$$

States represented by density operators.

- ρ density op. $\Leftrightarrow$ ρ positive and $tr(\rho) = 1$.

  Proof $\Rightarrow$: $\langle\varphi|\rho|\varphi\rangle = \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \geq 0$

  $tr\,\rho = \sum_i p_i\, tr(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1$

  $\Leftarrow$: ρ pos. $\Rightarrow$ $\rho = \sum_i \lambda_i |i\rangle\langle i|$ where $\lambda_i \geq 0$. $tr(\rho) = 1 \Rightarrow \sum_i \lambda_i = 1$.

- ρ pure if $\rho = |\psi\rangle\langle\psi|$ for some $|\psi\rangle$; otherwise mixed.

Ex.: $p = \frac{1}{2}: |0\rangle$, $p = \frac{1}{2}: |1\rangle$. $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{\mathbb{1}}{2}$

Can this state be represented by $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$?

A measurement in "computational basis" cannot distinguish between ρ and $|+\rangle$.

But rewrite to basis $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$:

$\rho = \frac{\mathbb{1}}{2} = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$: Measur. in basis $\{|+\rangle, |-\rangle\}$ gives 50% for each, while $|+\rangle$ gives result "+" with certainty.

Ex.: $p = \frac{1}{2}: |0\rangle$, $p = \frac{1}{2}: |1\rangle$ gives $\rho = \frac{\mathbb{1}}{2}$
$p = \frac{1}{2}: |+\rangle$, $p = \frac{1}{2}: |-\rangle$ gives $\rho = \frac{\mathbb{1}}{2}$ } same state!

$\{p_i, |\psi_i\rangle\}$ and $\{q_j, |\varphi_j\rangle\}$ generate same density op. iff

$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\varphi_j\rangle$ for unitary u.

Partial trace

$$\overbrace{A \qquad B}^{\rho}$$

Measure P_m on system A.

$$p(m) = tr(P_m \otimes 1\ \rho) = tr_A\, tr_B(P_m \otimes 1\ \rho) = tr_A\left(P_m\, \overbrace{tr_B(\rho)}^{\equiv \rho_A}\right) \quad \text{(reduced density op.)}$$

Even though the total state is known to be $|\psi\rangle$ (pure state), the reduced density op. ρ_A can be mixed!

Ex.: Total system in state $|\psi\rangle = \dfrac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}$ (Bell state)

(completely mixed)

$$\Rightarrow \rho_A = \frac{1}{2} tr_B\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{\mathbb{1}}{2}$$

We note that density operators are not only useful in situations with ignorance!

$$\overbrace{A \qquad B}^{|\psi\rangle}$$

Purification

Schmidt decomposition:

$$|\psi\rangle = \sum_i \sqrt{\lambda_i}\, |i\rangle_A |i\rangle_B \quad \leftarrow \text{always possible to write in this form}$$

Purification: Let ρ_A be any state on system A.

Then there exists a pure state $|\psi\rangle$ s.t. $tr_B(|\psi\rangle\langle\psi|) = \rho_A$.

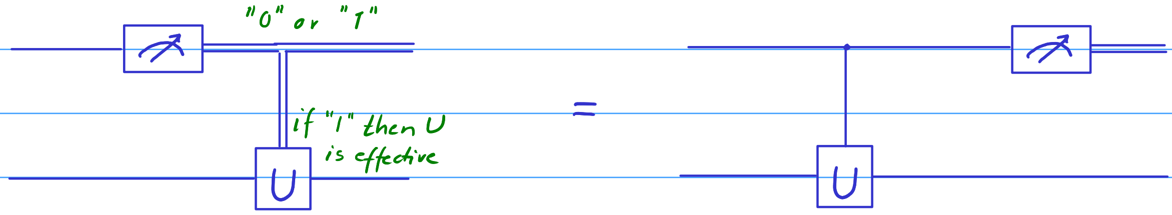
Any (mixed) state can be seen as pure in a larger state space!

Proof: Since ρ_A is hermitian, we can write

$\rho_A = \sum_i \lambda_i |i\rangle\langle i|_A$. We have $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$.

Construct $|\psi\rangle = \sum_i \sqrt{\lambda_i}\, |i\rangle_A |i\rangle_B$, and note that $tr_B(|\psi\rangle\langle\psi|) = \rho_A$.

Principle of deferred measurement



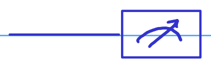
controlled-U gate: $|0\rangle|0\rangle \mapsto |0\rangle|0\rangle$

$|0\rangle|1\rangle \mapsto |0\rangle|1\rangle$

$|1\rangle|0\rangle \mapsto |1\rangle U|0\rangle$

$|1\rangle|1\rangle \mapsto |1\rangle U|1\rangle$

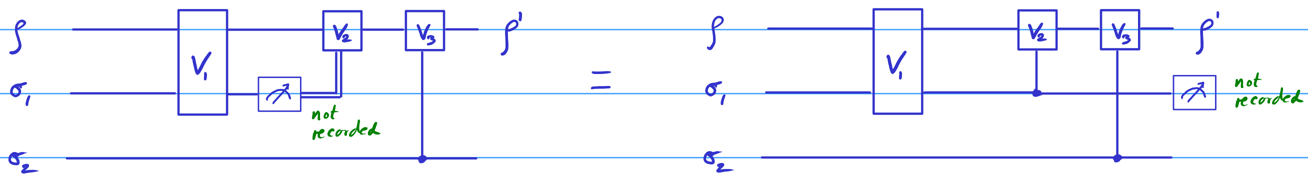
Principle of implicit measurement

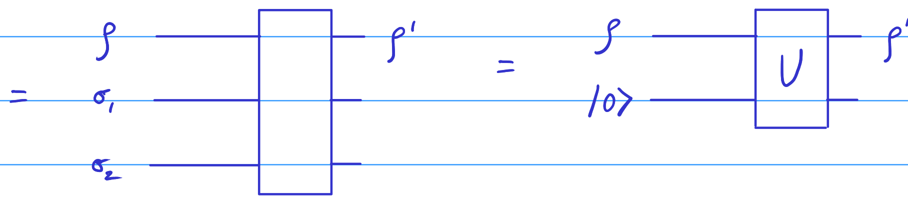


(measurement result not recorded)

ρ_A —— ρ_A' $\qquad\qquad \rho_A' = \rho_A$

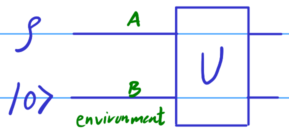
Ex: A complicated quantum operation:





The most general quantum operation is a unitary op. on a larger state space!

Quantum operations



$$\rho' = \mathcal{E}(\rho) = tr_B\left(U\, \rho \otimes |0\rangle\langle 0|\, U^+\right)$$
$$= \sum_k \langle e_k|\, U\, \rho \otimes |0\rangle\langle 0|\, U^+\, |e_k\rangle$$
$$= \sum_k \langle e_k|U|0\rangle\, \rho\, \langle 0|U^+|e_k\rangle = \sum_k E_k \rho E_k^+$$

where $E_k = \langle e_k|U|0\rangle$ = Kraus operators, $\sum_k E_k^+ E_k = \mathbb{1}$

If information is obtained (measurement that is recorded, result "k"):

$\rho' = E_k \rho E_k^+$ (strictly, should have been normalized: $\dfrac{E_k \rho E_k^+}{tr(E_k \rho E_k^+)}$)

$E_k^+ E_k \leq \mathbb{1}$

Unitary freedom: $\{E_k\}$ and $\{F_k\}$ give the same quantum op. iff

$E_k = \sum_j u_{kj} F_j$ for some unitary u.

Distance measures

Trace distance : $D(\rho,\sigma) = \frac{1}{2} tr|\rho-\sigma| = \dots$

$$= \max_P tr(P(\rho-\sigma)) = \max_P [tr(P\rho) - tr(P\sigma)]$$

$= \max_P$ difference in probability of obtaining the meas. result P.

Quantifies our ability to distinguish between ρ and σ.

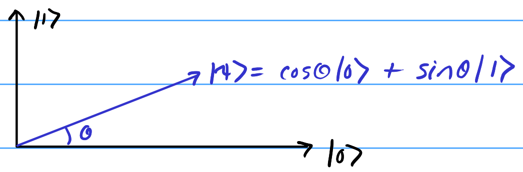
Fidelity :

$$F(\sigma,\rho) = tr\sqrt{\sigma^{1/2}\rho\,\sigma^{1/2}}$$

$$F(|\psi\rangle\langle\psi|,\rho) = tr\sqrt{|\psi\rangle\langle\psi|\rho|\psi\rangle\langle\psi|} = \sqrt{\langle\psi|\rho|\psi\rangle}$$

$$F(|\psi\rangle,|\varphi\rangle) = |\langle\psi|\varphi\rangle| = \text{overlap}$$

Ex: Any two pure states.



$F(|\psi\rangle,|0\rangle) = |\langle 0|\psi\rangle| = \cos\theta$

$D(|\psi\rangle,|0\rangle) = \dots = \sin\theta$

$[\ \rho-\sigma = |\psi\rangle\langle\psi| - |0\rangle\langle 0|$

$$= \begin{bmatrix} \cos^2\theta - 1 & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{bmatrix}$$

So for pure states $D = \sqrt{1-F^2}$.

In general : $1-F \leq D \leq \sqrt{1-F^2}$

Uhlmann's theorem : $F(\rho,\sigma) = \max_{|\psi\rangle,|\varphi\rangle} \langle\psi|\varphi\rangle$, $|\psi\rangle$ purification of ρ
$|\varphi\rangle$ — " — σ

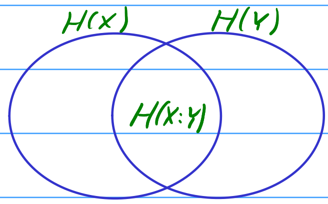
Holevo bound

Alice prepares ρ_x, $x = 0, 1, \dots, n$, with probability p_x

Gives the state to Bob without telling x.

Bob has then the state $\rho = \sum_x p_x \rho_x$.

Bob measures ρ, result Y.



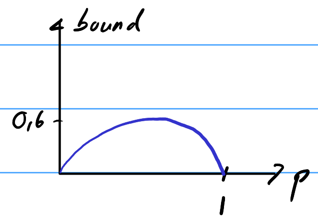
For any measurement Bob can do: $H(X:Y) \le S(\rho) - \sum_x p_x S(\rho_x)$

mutual Shannon inf. — von Neuman entropy $S(\rho) = -\mathrm{tr}\, \rho \log_2 \rho$ (base 2)

Ex: Alice gives either $|0\rangle$ or $|+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ to Bob, prob. p for $|0\rangle$.

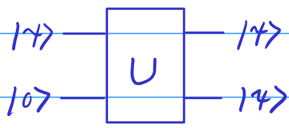
$\rho = p|0\rangle\langle 0| + (1-p)|+\rangle\langle +|$

$H(X:Y) \le S(\rho)$



Maximum ~ 0,6 bit mutual information, less than 1 bit because Bob cannot distinguish reliably between $|0\rangle$ and $|+\rangle$.

No-cloning theorem



Assume the cloner works for inputs $|\psi\rangle$ and also $|\varphi\rangle$.

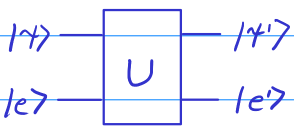
$$\langle\psi| \otimes \langle\psi|\; |\varphi\rangle \otimes |\varphi\rangle = \langle\psi| \otimes \langle 0|\, U^+ U\, |\varphi\rangle \otimes |0\rangle$$

$$\langle\psi|\varphi\rangle^2 \qquad\qquad \langle\psi|\varphi\rangle$$

So $\langle\psi|\varphi\rangle^2 = \langle\psi|\varphi\rangle$ which means that $\langle\psi|\varphi\rangle = 0$ or 1.

The cloner only works for equal or orthogonal states.

What about "amplifiers"?



$$\left.\begin{aligned} |\psi'\rangle|e'\rangle &= U|\psi\rangle|e\rangle \\ |0'\rangle|e_0'\rangle &= U|0\rangle|e\rangle \end{aligned}\right\} \Rightarrow \langle 0|\psi\rangle = \langle 0'|\psi'\rangle\langle e_0'|e'\rangle \Rightarrow |\langle 0'|\psi'\rangle| \ge |\langle 0|\psi\rangle|$$

That is, differences have diminished; no amplification.

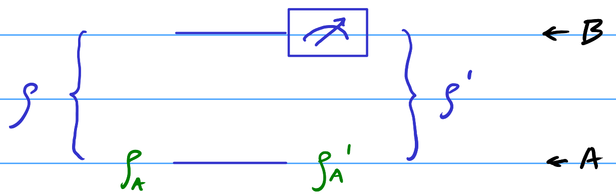
Amplifiers necessarily add noise (spontaneous emission).

More generally it can be shown that $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \le D(\rho, \sigma)$ for trace-preserving $\mathcal{E}$.

I.e. quantum operations reduce distance between two states.

Appendix

Principle of implicit measurement – proof:



Measurement result not recorded.

Let P_m be projectors on the upper wire state space.

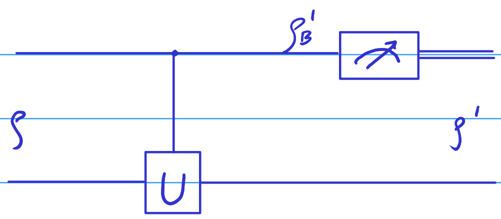
Probability of outcome m: $p(m)$.

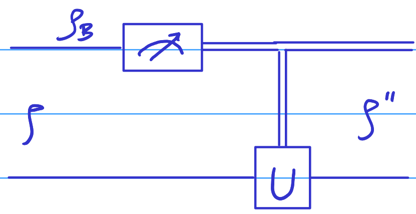
Postmeasurement state if result m: $\dfrac{P_m \otimes \mathbb{1}\, \rho\, P_m \otimes \mathbb{1}}{p(m)}$

Measurement result not recorded: $\rho' = \sum_m p(m) \dfrac{P_m \otimes \mathbb{1}\, \rho\, P_m \otimes \mathbb{1}}{p(m)} = \sum_m P_m \otimes \mathbb{1}\, \rho\, P_m \otimes \mathbb{1}$

$$\Rightarrow \rho_A' = tr_B(\rho') = \sum_n \langle n|_B \sum_m P_m \otimes \mathbb{1}\, \rho\, P_m \otimes \mathbb{1}\, |n\rangle_B = \sum_m \langle m|_B\, \rho\, |m\rangle_B = tr_B(\rho)$$
$$= \rho_A .$$

Principle of deferred measurement – proof:





Let the controlled-U be denoted CU.

First prove $P_m \otimes \mathbb{1}\; CU = CU\, P_m \otimes \mathbb{1}$. Let $|\psi\rangle = \sum_{ij} a_{ij} |i\rangle |j\rangle$ be arbitrary.

$$CU\, P_m \otimes \mathbb{1}\, |\psi\rangle = \begin{cases} \sum_j a_{0j} |0\rangle |j\rangle, & m=0 \\ \sum_j a_{1j} |1\rangle U|j\rangle, & m=1 \end{cases}$$

$$P_m \otimes \mathbb{1}\; CU\, |\psi\rangle = P_m \otimes \mathbb{1} \left(\sum_j a_{0j} |0\rangle |j\rangle + \sum_j a_{1j} |1\rangle U |j\rangle \right)$$

$$= \begin{cases} \sum_j a_{0j} |0\rangle |j\rangle, & m=0 \\ \sum_j a_{1j} |1\rangle U|j\rangle, & m=1 \end{cases}$$

Proving that identical measur. statistics:

Let P_m be a projector on system B.

$$tr_B\left(P_m \otimes \mathbb{1}\ CU\rho CU^\dagger\right) = tr_B\left(P_m \otimes \mathbb{1}\ \rho\right) \quad \text{since } P_m \otimes \mathbb{1}\ CU = CU P_m \otimes \mathbb{1}$$

Proving that $\rho'' = \rho'$:

If $m=0$: $\rho' = \frac{P_0 CU \rho CU^\dagger P_0}{p(0)} = \frac{CU P_0 \rho P_0 CU^\dagger}{p(0)} = \frac{P_0 \rho P_0}{p(0)} = \rho''$

If $m=1$: $\rho' = \frac{P_1 CU \rho CU^\dagger P_1}{p(1)} = \frac{CU P_1 \rho P_1 CU^\dagger}{p(1)} = \frac{\mathbb{1} \otimes U\ P_1 \rho P_1\ \mathbb{1} \otimes U^\dagger}{p(1)} = \rho''$