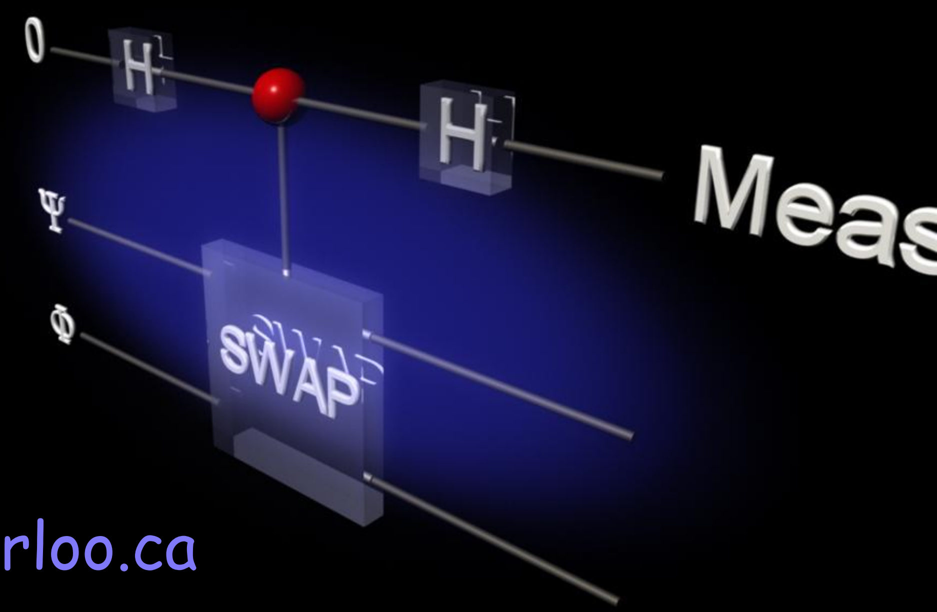
Introduction to Quantum Information Processing

CS467 C&O481 PHYS467

Lecture 7 (29 January 2013)

Michele Mosca mmosca@iqc.uwaterloo.ca

Tuesdays and Thursdays 10am-11:15am



IQC Institute for Quantum Computing

UNIVERSITY OF WATERLOO

PI PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Reading

- All of Chapters 1 and 2. From sections 3.1 till 3.5.2. Chapter 4. Sections 5.1 and 5.2.

Partial trace

- How can we compute probabilities for a partial system? Do we need to know the state of the whole system?

  Example:

$$\sum_{x,y} \alpha_{xy} |x\rangle |y\rangle$$

- Suppose we are only able to interact with or measure the first system.
- For convenience, denote $\boxed{|\Phi_y\rangle = \sum_x \frac{\alpha_{xy}}{\sqrt{p_y}} |x\rangle}$ $\quad p_y = \sum_x |\alpha_{xy}|^2$
- So $\displaystyle\sum_{x,y} \alpha_{xy} |x\rangle |y\rangle = \sum_y \sqrt{p_y} |\Phi_y\rangle |y\rangle$

- E.g. suppose we wish to compute the probability of measuring $|w\rangle$ in the first register.

$$\Pr(w) = \sum_y \left|\alpha_{wy}\right|^2 = \sum_y p_y \left|\frac{\alpha_{wy}}{\sqrt{p_y}}\right|^2$$

$$= \sum_y p_y Tr\left(|w\rangle\langle w\|\Phi_y\rangle\langle\Phi_y|\right)$$

$$= Tr\left(|w\rangle\langle w|\left(\sum_y p_y|\Phi_y\rangle\langle\Phi_y|\right)\right)$$

- So what really matters is $$\sum_y p_y \left|\Phi_y\right\rangle\left\langle\Phi_y\right|$$

- So we are interested in the map

$$\left(\sum_{x,y}\alpha_{xy}\left|x\right\rangle\left|y\right\rangle\right)\left(\sum_{v,z}\alpha^*_{vz}\left\langle v\right|\left\langle z\right|\right)$$

$$=\left(\sum_y \sqrt{p_y}\left|\Phi_y\right\rangle\left|y\right\rangle\right)\left(\sum_z \sqrt{p_z}\left\langle\Phi_z\right|\left\langle z\right|\right)$$

$$\mapsto \sum_y p_y \left|\Phi_y\right\rangle\left\langle\Phi_y\right|$$

- What is this map??

Partial trace

- One way to describe this map is as the map

$$\sum_y \sqrt{p_y}\left|\Phi_y\right\rangle\left|y\right\rangle \mapsto \left\{\left(p_y, \left|\Phi_y\right\rangle\right)\right\}$$

(can think of this as measuring the 2nd register, but not looking at the outcome)

- Using density matrix representation for states:

$$\rho = \sum_{y,z} \sqrt{p_y p_z}\left|\Phi_y\right\rangle\left\langle\Phi_z\right| \otimes \left|y\right\rangle\left\langle z\right|$$

$$\mapsto \sum_y p_y \left|\Phi_y\right\rangle\left\langle\Phi_y\right| = Tr_2\rho$$

Partial trace

$$\rho = Tr_2 \rho$$

is in fact a linear map that takes bipartite states to single-system states

$$Tr_2\left(|i\rangle\langle k| \otimes |j\rangle\langle l|\right) = |i\rangle\langle k| \otimes Tr\left(|j\rangle\langle l|\right)$$

$$= |i\rangle\langle k| \otimes \langle l|j\rangle = \langle l|j\rangle |i\rangle\langle k|$$

Confirm that

$$\rho = \sum_{y,z} \sqrt{p_y p_z} |\Phi_y\rangle\langle\Phi_z| \otimes |y\rangle\langle z|$$

$$\mapsto \sum_{y,z} \sqrt{p_y p_z} |\Phi_y\rangle\langle\Phi_z| \otimes \langle z\|y\rangle = \sum_y p_y |\Phi_y\rangle\langle\Phi_y|$$

Partial trace

- We can also trace out the first system.

$$Tr_1\left(|i\rangle\langle k|\otimes|j\rangle\langle l|\right)=Tr\left(|i\rangle\langle k|\right)\otimes|j\rangle\langle l|$$

- Back to our example:

$$\sum_{x,y}\alpha_{xy}|x\rangle|y\rangle=\sum_{x}\sqrt{p_x}|x\rangle|\Theta_x\rangle$$

Partial trace using matrices

- Tracing out the 2nd system

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \xrightarrow{Tr_2} \begin{bmatrix} Tr\begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix} & Tr\begin{bmatrix} a_{02} & a_{03} \\ a_{12} & a_{13} \end{bmatrix} \\ Tr\begin{bmatrix} a_{20} & a_{21} \\ a_{30} & a_{31} \end{bmatrix} & Tr\begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} a_{00} + a_{11} & a_{02} + a_{13} \\ a_{20} + a_{31} & a_{22} + a_{33} \end{bmatrix}$$

Distant transformations don't change the local density matrix

- Notice that a unitary transformation on the system that is traced out does not affect the result of the partial trace.

i.e.

$$\sum_y \sqrt{p_y}\,|\Phi_y\rangle U|y\rangle \cong (I \otimes U)\rho(I \otimes U^\dagger)$$

$$\xrightarrow{Trace_2} \left\{\left(p_{y,}\,|\Phi_y\rangle\right)\right\} \cong \rho_2 = Tr_2\rho$$

*(can think of this as measuring the 2nd register **in any basis**, and not looking at the outcome)*

Partial trace

- For example, consider tracing out by measuring the second qubit in the computational basis and ignoring the outcome

$$\alpha|00\rangle + \beta|11\rangle \xrightarrow{Tr_2} |\alpha|^2 |0\rangle\langle 0| + |\beta|^2 |1\rangle\langle 1|$$

- In a different basis

$$\alpha|00\rangle + \beta|11\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle + \beta|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$+\frac{1}{\sqrt{2}}\left(\alpha|0\rangle - \beta|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

Partial trace

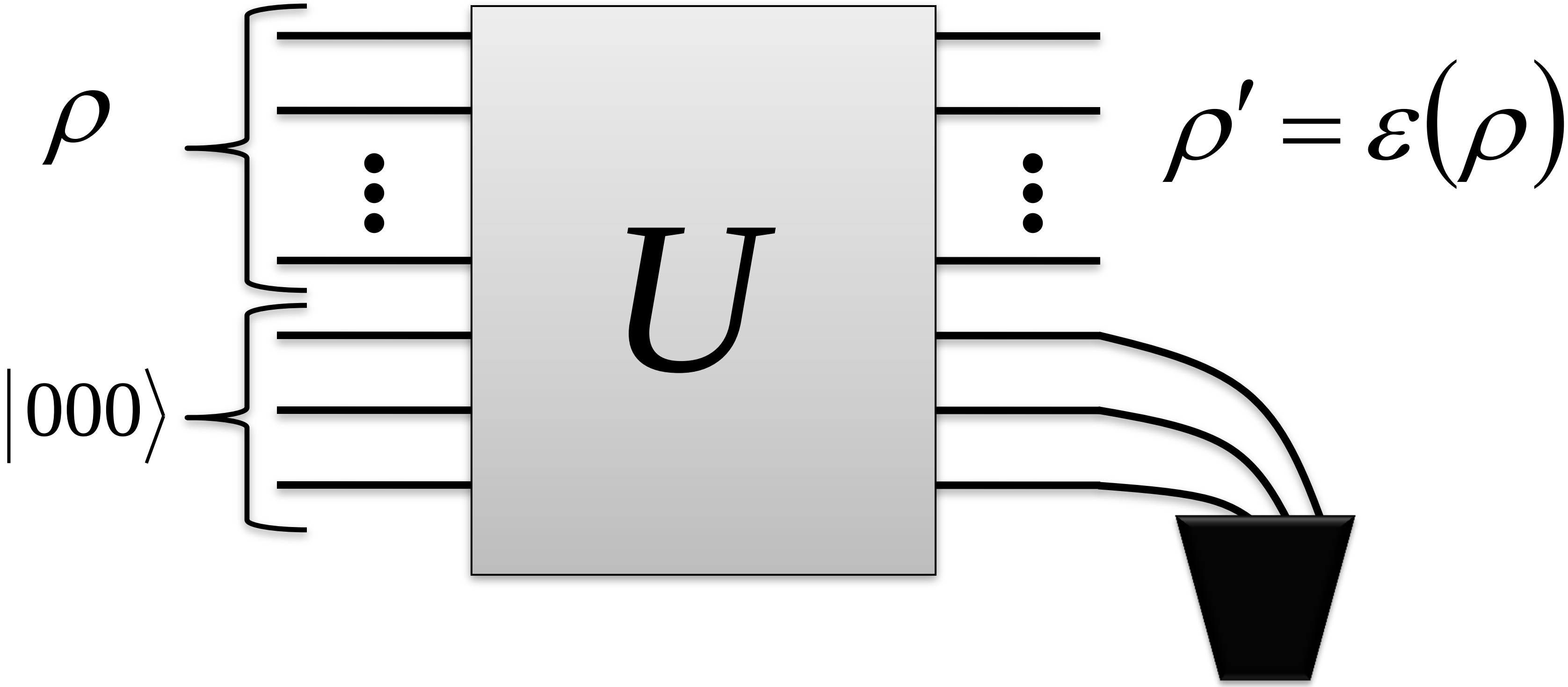
$$\frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)+\frac{1}{\sqrt{2}}\left(\alpha|0\rangle-\beta|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)$$

$$\xrightarrow{Tr_2}\frac{1}{2}\left(\alpha|0\rangle+\beta|1\rangle\right)\left(\alpha^*\langle 0|+\beta^*\langle 1|\right)$$

$$+\frac{1}{2}\left(\alpha|0\rangle-\beta|1\rangle\right)\left(\alpha^*\langle 0|-\beta^*\langle 1|\right)$$

$$=|\alpha|^2|0\rangle\langle 0|+|\beta|^2|1\rangle\langle 1|$$

Aside:
General operation



$$\rho \mapsto \rho' = Tr_2\left(\rho \otimes |000\rangle\langle 000|\right)$$

Important

- Thus, any general quantum transformation on the traced out system, including measurement (without communicating back the answer) does not affect the partial trace.

- “Tracing out” the second system corresponds to discarding or ignoring the second system. Hypothetical operations, like measurements, on the second system might help with some mathematical or conceptual analysis, but they are not physically significant if the second system is truly isolated/discarded.

Why?

- Operations on the 2nd system do not affect the statistics of any outcomes of measurements on the first system

- Note that if it were possible to affect the statistics non-locally, then a party in control of the 2nd system could instantaneously communicate information to a party controlling the 1st system.

Schmidt decomposition theorem

- Consider a bipartite state

$$|\Psi\rangle = \sum_{x,y} \alpha_{xy} |x\rangle |y\rangle$$

- ***Theorem***: There exist orthonormal bases $\{|\phi_i\rangle\}$, $\{|\psi_j\rangle\}$ for the first and second system, respectively, and non-negative real numbers $p_0 \geq p_1 \geq \cdots$ such that

$$|\Psi\rangle = \sum_i \sqrt{p_i} |\phi_i\rangle |\psi_i\rangle$$

- The values $\sqrt{p_i}$ are called the *Schmidt coefficients*, and the number of non-zero values is called the *Schmidt number* of $|\Psi\rangle$.

Schmidt decomposition theorem

- How do I find the Schmidt decomposition? How do I find the orthonormal bases?
- Note that if $\left|\Psi\right\rangle = \sum_i \sqrt{p_i}\left|\phi_i\right\rangle\left|\psi_i\right\rangle$ is the Schmidt decomposition, then

$$Tr_2\left|\Psi\right\rangle\left\langle\Psi\right| = \sum_i p_i\left|\phi_i\right\rangle\left\langle\phi_i\right|$$

will be diagonal in the Schmidt basis.

Thus diagonalizing $Tr_2\left|\Psi\right\rangle\left\langle\Psi\right|$ will reveal the Schmidt basis for the first system, as well as the Schmidt coefficients.

Once the first system is expressed in its Schmidt basis, the Schmidt basis for the second system is easily found.

A more efficient and elegant solution is given in N&C.

Note that local transformations don’t change the Schmidt coefficients

$$\sum_y \sqrt{p_y}\, U_A \left|\phi_y\right\rangle U_B \left|\psi_y\right\rangle = \sum_y \sqrt{p_y} \left|\phi_y'\right\rangle \left|\psi_y'\right\rangle$$

with new Schmidt bases:

$$\left\{\left|\phi_y'\right\rangle\right\}, \left\{\left|\psi_y'\right\rangle\right\}$$

Recall: Distant transformations don't change the local density matrix

- Recall that a unitary transformation on the system that is traced out does not affect the result of the partial trace
- I.e.

$$\sum_y \sqrt{p_y}\left|\phi_y\right\rangle U\left|\psi_y\right\rangle \cong (I \otimes U)\left|\Psi\right\rangle\left\langle\Psi\right|\left(I \otimes U^{\dagger}\right)$$

$$\xrightarrow{Trace_2} \sum_i \sqrt{p_i}\left|\phi_i\right\rangle\left\langle\phi_i\right| = Tr_2\left|\Psi\right\rangle\left\langle\Psi\right|$$

Conversely:

- Any two purifications of the same dimension of the same state are equivalent up to a local unitary on the ancilla system.
- I.e. If

$$Tr_2|\psi\rangle\langle\psi| = Tr_2|\phi\rangle\langle\phi|$$

then

$$|\psi\rangle = (I \otimes U)|\phi\rangle$$

for some U

- Easy to prove with Schmidt decomposition
- Can be used to prove that “bit commitment” is impossible.

Purification of a mixed state

- Suppose we have the mixed state

$$\{(|\phi_k\rangle, p_k) \,|\, k = 1,2,\ldots,M\}, |\phi_k\rangle \in H = \mathrm{C}^N$$

- This state is described by the density matrix

$$\rho = \sum_{k=1}^{M} p_k |\phi_k\rangle\langle\phi_k| \qquad \rho \in L(H)$$

- A purification of this mixed state is a pure state $|\phi\rangle \in H_a \otimes H$ in some larger Hilbert space satisfying

$$\rho = Tr_a |\phi\rangle\langle\phi|$$

Purification of a mixed state

$$\rho = \sum_{k=1}^{M} p_k \left|\phi_k\right\rangle\left\langle\phi_k\right|$$

- One example of a purification is

$$\left|\phi\right\rangle = \sum_{i=1}^{M} \sqrt{p_i}\left|i\right\rangle\left|\phi_i\right\rangle \qquad \left|\phi\right\rangle \in H_a \otimes H,$$

$$H_a = C^M$$

- How big does H_a ***need*** to be??

Recall: Spectral decomposition

We can diagonalize

$$\rho = \sum_{k=1}^{N} q_k |\psi_k\rangle\langle\psi_k|$$

where $|\psi_k\rangle$ is an eigenvector with eigenvalue q_k and $\{|\psi_k\rangle\}$ forms an orthonormal basis.

We can assume, w.l.o.g. that

$$q_1 \geq q_2 \geq \cdots \geq q_N \geq 0$$

So

$$\rho = \sum_{k=1}^{s} q_k |\psi_k\rangle\langle\psi_k|$$

where s is the number of non-zero eigenvalues (i.e. the rank) of ρ.

- Thus, a purification for ρ is

$$|\gamma\rangle = \sum_{i=0}^{s} \sqrt{q_i}\,|i\rangle|\psi_i\rangle$$

- Thus the dimension of H_a does not need to be more than the rank of ρ.

- Exercise: the dimension of H_a must be at least the rank of ρ

Bit Commitment

http://www.cs.uwaterloo.ca/~watrous/lecture-notes/519/19.ps

- Alice has a bit **b** she wishes to <u>commit</u> to Bob

- But Alice does not want Bob to know what the bit is until she chooses to <u>reveal</u> it

- Bob wants to be assured that Alice doesn’t change the value of the bit before it is revealed.

- Any protocol for bit commitment must be:
  - **Binding** (Alice cannot change the bit after she commits it)
  - **Concealing** (Bob cannot learn about the bit until it is revealed by Alice)

Example

- Alice locks the one bit message in a box
- To reveal, she provides Bob a key to the box
- If Bob truly had no way to look inside the box without the key, this scheme would be concealing.
- If Alice could not remotely change the value of the bit, or via the key she provides Bob, this would be binding.

No information theoretically secure classical bit commitment protocol

- No protocol can be both information theoretically concealing and binding

- It is possible to achieve information theoretically concealing, and computationally binding, or vice versa.

Can quantum mechanics help??

Can quantum mechanics help?

A possible (incorrect) protocol

- To commit “0” Alice sends either $|0\rangle$ or $|1\rangle$ with equal probability

- To commit “1” Alice sends either $|+\rangle$ or $|-\rangle$ with equal probability

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Can quantum mechanics help?

- To reveal, Alice sends Bob a classical description of which of the four states she sent; Bob checks her claim with a measurement

- Before the reveal phase, from Bob's perspective, he has

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

in either case, so the protocol is indeed concealing

But is it binding?

- It might appear that if Alice sends Bob a description of a state different from what she originally sent, she will get caught with probability $1/2$

- This argument is flawed.

- Alice could implement her first step by sending Bob one half of the state

$$\sqrt{\frac{1}{2}}|0\rangle|0\rangle+\sqrt{\frac{1}{2}}|1\rangle|1\rangle \qquad \text{or} \qquad \sqrt{\frac{1}{2}}|0\rangle|+\rangle+\sqrt{\frac{1}{2}}|1\rangle|-\rangle$$

But is it binding?

- Alice could implement her first step by sending Bob one half of the entangled state

$$\sqrt{\frac{1}{2}}|0\rangle|0\rangle+\sqrt{\frac{1}{2}}|1\rangle|1\rangle \qquad \text{or} \qquad \sqrt{\frac{1}{2}}|0\rangle|+\rangle+\sqrt{\frac{1}{2}}|1\rangle|-\rangle$$

- ***If*** she irreversibly measures her half of the state, the previous logic would apply.

- However, a dishonest Alice can maintain her half of the state without measuring it, and change it to the other entangled state at any time if she wishes, by a local operation. Then she can measure her half, and tell Bob she sent the state for the second half corresponding to the outcome of her measurement.

But is it binding?

- Check

$$\sqrt{\frac{1}{2}}|0\rangle|0\rangle + \sqrt{\frac{1}{2}}|1\rangle|1\rangle = (H \otimes I)\sqrt{\frac{1}{2}}|0\rangle|+\rangle + \sqrt{\frac{1}{2}}|1\rangle|-\rangle$$

- Thus the given protocol is ***not*** binding.

- In fact, there cannot exist any quantum bit commitment scheme that is both information theoretically concealing and information theoretically binding.