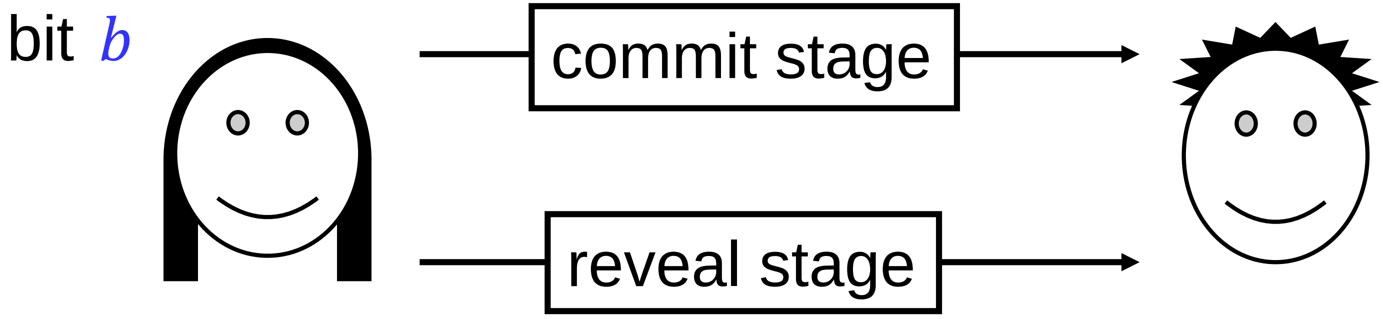
Introduction to Quantum Information Processing
QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 19 (2017)

Jon Yard
QNC 3126
jyard@uwaterloo.ca
http://math.uwaterloo.ca/~jyard/qic710

The story of bit commitment

Bit-commitment



- Alice has a bit b that she wants to ***commit*** to Bob:
- After the ***commit*** stage, Bob should know nothing about b, but Alice should not be able to change her mind
- After the ***reveal*** stage, either:
  - Bob should learn b and accept its value, or
  - Bob should reject Alice's reveal message, if she deviates from the protocol

Simple physical implementation

- **Commit:** Alice writes b down on a piece of paper, locks it in a safe, sends the safe to Bob, but keeps the key
- **Reveal:** Alice sends the key to Bob, who then opens the safe
- Desirable properties:
  - **Binding:** Alice cannot change b after **commit**
  - **Concealing:** Bob learns nothing about b until **reveal**

Question: why should anyone care about bit-commitment?

Answer: it is a useful primitive operation for other protocols, such as coin-flipping, and "zero-knowledge proof systems"

Complexity-theoretic implementation

Alice and Bob agree on:

- a ***one-way function**** $f: \{0,1\}^n \rightarrow \{0,1\}^n$

(easy to compute but hard to invert)

- a ***hard-core predicate*** $h: \{0,1\}^n \rightarrow \{0,1\}$ for f

(easy to compute from x but hard to compute from $f(x)$).

Commit: Alice picks a random $x \in \{0,1\}^n$, sets $y = f(x)$ and $c = b \oplus h(x)$ and then sends y and c to Bob

Reveal: Alice sends x to Bob, who verifies that $y = f(x)$ and then sets $b = c \oplus h(x)$

This is (i) perfectly binding and (ii) computationally concealing, based on the hardness of predicate h.

***** should be one-to-one

Quantum implementation

- Inspired by the success of QKD, one can try to use the properties of quantum mechanical systems to design an information-theoretically secure bit-commitment scheme
- One simple idea:
  - To **commit** to **0**, Alice sends a random state from $\{|0\rangle, |1\rangle\}$
  - To **commit** to **1**, Alice sends a random state from $\{|+\rangle, |-\rangle\}$
  - Bob measures each qubit received in a random basis
  - To **reveal**, Alice tells Bob exactly which states she sent in the commitment stage (by sending its index 00, 01, 10, or 11), and Bob checks for consistency with his measurement results
- A FOCS paper appeared in 1993 proposing a quantum bit-commitment scheme and a proof of security.

Impossibility proof (I)

- Not only was the 1993 scheme shown to be insecure, but it was later shown that ***no such scheme can exist!***
- To understand the impossibility proof, recall that any two purifications are related by a unitary on the purifying system.

If $|\psi_0\rangle$, $|\psi_1\rangle$ are two bipartite states such that

$$\mathrm{Tr}_1|\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_1|\psi_1\rangle\langle\psi_1|$$

I explained a few lecture ago that there exists a unitary U (acting on the first register) such that $(U \otimes I)|\psi_0\rangle = |\psi_1\rangle$.
We will prove this momentarily.

[Mayers '96][Lo & Chau '96]

Impossibility proof (II)

- For the protocol to be concealing, Bob should see the same density matrix regardless of Alice's commitment.
- Protocol can be "purified" so that Alice's commit states are $|\psi_0\rangle$ & $|\psi_1\rangle$ (where she sends the second register to Bob).
- By applying U to her register, Alice can cheat and change her commitment from $b = 0$ to $b = 1$ (by changing from $|\psi_0\rangle$ to $|\psi_1\rangle$).

So if Alice has a quantum computer, any perfectly concealing protocol cannot be binding!

Schmidt decomposition

Schmidt decomposition

Theorem:

Let $|\psi\rangle$ be ***any*** bipartite quantum state:

$$|\psi\rangle = \sum_{a=1}^{m} \sum_{b=1}^{n} \alpha_{a,b} |a\rangle|b\rangle$$

(where we can assume $n \leq m$)

Then there exist orthonormal states $|\mu_1\rangle, |\mu_2\rangle, \dots, |\mu_n\rangle$ and $|\phi_1\rangle, |\phi_2\rangle, \dots, |\phi_n\rangle$ such that

$$|\psi\rangle = \sum_{x=1}^{n} \sqrt{p_x} |\mu_x\rangle|\phi_x\rangle$$

and where $|\phi_1\rangle, |\phi_2\rangle, \dots, |\phi_n\rangle$ are the eigenvectors of

$$\rho = \mathrm{Tr}_1 |\psi\rangle\langle\psi| = \sum_{x} p_x |\phi_x\rangle\langle\phi_x|$$

Proof uses singular value decomposition of matrices.

Singular value decomposition

<u>**Theorem:**</u>

Let $A \in \mathbb{C}^{m\times n}$ be an *arbitrary* matrix (assume $n \le m$).
Then there exist unitaries $U \in \mathbb{C}^{m\times m}$, $V \in \mathbb{C}^{n\times n}$ and a "diagonal" matrix

$$D = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_n \\ 0 & 0 & 0 \end{pmatrix} \in \mathbb{C}^{m\times n}, \qquad d_i \ge 0$$

such that $A = UDV$.

Note that if A is Hermitian, then $V = U^\dagger$.

Also note that if A is unitary or diagonal, there is nothing to do.

Application: Polar decomposition $A = UP$, where $A \in \mathbb{C}^{n\times n}$ and P is positive semidefinite.

Schmidt decomposition: proof

$$|\psi\rangle = \sum_{a=1}^{m}\sum_{b=1}^{n}\alpha_{a,b}|a\rangle|b\rangle$$

View the coefficients α_{ab} as a matrix $\alpha \in \mathbb{C}^{m\times n}$.
By the singular value decomposition, we can write
$\alpha = udv$ for unitaries $u \in \mathbb{C}^{m\times m}$, $v \in \mathbb{C}^{n\times n}$ and a "diagonal" matrix $d \in \mathbb{C}^{m\times n}$ with $d_c \geq 0$.

Because $\sum_c d_c^2 = \mathrm{Tr}\, d^2 = \mathrm{Tr}\, \alpha^\dagger\alpha = \sum_{ab}|\alpha_{ab}|^2 = 1$,
there exist probabilities p_c such that $d_c = \sqrt{p_c}$.

Defining $|\mu_c\rangle = \sum_a u_{ac}|a\rangle$ and $|\phi_c\rangle = \sum_b v_{cb}|b\rangle$, we get

$$|\psi\rangle = \sum_{a=1}^{m}\sum_{b=1}^{n}\alpha_{a,b}|a\rangle|b\rangle = \sum_{a=1}^{m}\sum_{b=1}^{n}\sum_{c=1}^{n}u_{ac}\sqrt{p_c}v_{cb}|a\rangle|b\rangle = \sum_{c=1}^{n}\sqrt{p_c}|\mu_c\rangle|\phi_c\rangle$$

and the theorem is proved.

Application: purifications

Theorem: If $|\psi_0\rangle$, $|\psi_1\rangle$ are two purifications of a density matrix ρ, i.e. if they are bipartite states such that

$$\rho = \mathrm{Tr}_1 |\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_1 |\psi_1\rangle\langle\psi_1|$$

then there exists a unitary U (acting on the first register) such that

$$(U \otimes I)|\psi_0\rangle = |\psi_1\rangle$$

- **Proof:** By the Schmidt decomposition,

$$|\psi_0\rangle = \sum_{c=1}^{n} \sqrt{p_c}|\mu_c\rangle|\phi_c\rangle \text{and } |\psi_1\rangle = \sum_{c=1}^{n} \sqrt{p_c}|\mu_c'\rangle|\phi_c\rangle$$

We can define U so that $U|\mu_c\rangle = |\mu_c'\rangle$ for $c = 1, \ldots, n$ $\blacksquare$

Measuring entanglement

(brief)

Entangled vs product states

Consider the following pure states:

1) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
2) $|0\rangle|1\rangle$
3) $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$
4) $\frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$
5) $.99|00\rangle + .07|11\rangle + .07|22\rangle + .07|33\rangle + .07|44\rangle$

Which are entangled and which are product states?

Which are *more* entangled than the others?

One approach: Schmidt rank

Another (more operational) approach: Entanglement entropy

Schmidt rank

Schmidt rank measures entanglement by number of nonzero Schmidt coefficients (= rank of $\mathrm{Tr}_1|\psi\rangle\langle\psi|$)

Schmidt rank	State
2	1) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
1	2) $|0\rangle|1\rangle$
1	3) $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$
2	4) $\frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$
5	5) $.99|00\rangle + .07|11\rangle + .07|22\rangle + .07|33\rangle + .07|44\rangle$

Entanglement entropy

Entanglement entropy measures entanglement by the entropy of $\mathrm{Tr}_1|\psi\rangle\langle\psi|$

Entropy	State
1	1) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
0	2) $|0\rangle|1\rangle$
0	3) $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$
$.811$	4) $\frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$
$.18$	5) $.99|00\rangle + .07|11\rangle + .07|22\rangle + .07|33\rangle + .07|44\rangle$

Operationally motivated measure of the “information” each System has about the other, via Schumacher compression. Area laws…

Some properties

1) Invariant under local unitaries
2) Non-increasing under Local Operations and Classical Communication (LOCC)

Next time: More on entanglement measures, both for pure and for **mixed** states