# LECTURE 25
## CS229r: ITECS

4/30/2019

TODAY:

QUANTUM INFORMATION THEORY

- Basics of Quantum Mechanics
  - State, Tranformations, Observations
- Basic Quantum Interaction Tasks
- Some fundamental limits (without proofs)

---

~~QIT: Originates in the~~

Acknowledgements: Thanks to Amir Shanehsazzadeh for ~~making~~ asking me learn this. To Thomas Vidick for careful lengthy explanations over email. And for pointing me to the below:

References: Quantum Information Theory (2nd Edition), by Mark M. Wilde.

Also available as arxiv: 1106.1445

[See esp. Chapters 6 & 8].

Quantum "Information" $\triangleq$ What it takes to describe the behavi[our]
of a quantum particle / system?

$\triangleq$ What can be conveyed by a quantu[m]
particle / system?

x

Eg. "Classically": $X \sim \text{Bern}(p)$

- describing requires "p"
- Information conveyed $= H(p) \leq 1$.

x

Eg. - Single electron may be in one of two states (or super[position]
$|0\rangle$ or $|1\rangle$ [spin up or spin down]

- What does it take to describe n electrons?
- What does it take to decribe these electrons after some physical operations?
- How much "information" can be "channeled" through these n electrons?

x

To understand :- Need to understand effect of <u>operations</u>

- What can be "observed" or <u>measured</u>

# Short Summary

## Quantum State :

- 1 qubit → unit vector in $\mathbb{C}^2$
  (1 electron)

  basis $|0\rangle, |1\rangle \in \mathbb{C}^2$ "orthonormal"

  Inner product $\langle 0|1\rangle = 0$

  $\langle 0|0\rangle = \langle 1|1\rangle = 1$

- n qubits – unit vector in $\mathbb{C}^{2^n}$

  – basis $|x\rangle \in \mathbb{C}^{2^n}$ $\quad x \in \{0,1\}^n$

  $\langle x|x\rangle = 1 \quad \forall x$

  $\langle x|y\rangle = 0 \quad \forall x \neq y$

Pure States

Mixed State = Prob. Dist. over pure states.

## Quantum "Mechanics"

Only operations are "unitary"

i.e., $T : |\phi\rangle \longrightarrow |\psi\rangle \qquad |\phi\rangle, |\psi\rangle \in \mathbb{C}^{2^n}$

must satisfy $\{T(|x\rangle)\}_{x \in \{0,1\}^{2^n}}$ are orthoromal

& $T(|\psi\rangle) + T(|\phi\rangle) = T(|\psi\rangle + |\phi\rangle)$.

linear.

## Measurements

- Can't read off coefficients of "qubit" or "qubit" system!
- Instead if bit in state $\alpha|0\rangle + \beta|1\rangle$

  measurement leads to "0" w.p. $\alpha^2$

  & "1" w.p. $\beta^2$

- More generally if ~~bit~~ system in state $\sum c_x |x\rangle$

  get "x" w.p. $c_x^2$

- Partial measurement: State $\sum c_{xy} |xy\rangle$

  $\Rightarrow$ get "$\alpha$" w.p. $\sum_y c_{\alpha y}^2$ ; resulting state (projected to "y" i

$$\frac{\sum_y c_{\alpha y} |y\rangle}{\sum c_{\alpha y}^2}$$

---

Challenge in dealing with Quantum: Unitary operations can distingu different $(\alpha, \beta)$;

- But never actually reveal it!

- Main Ingredients in <u>Quantum Information Theory</u>

① How to describe unknown quantum state?

"Quantum Entropy" / "Compression".

② How to use an ~~unknown~~ noiseless (quantum) channel to exchange bits / qubits?

③ Noisy version.

①: What does it take to describe a quantum state (mixed)

- a priori $n$ qubit system = Prob. Dist over $\mathbb{C}^{2^n}$!

(Doubly exponentially many degrees of freedom?).

- [von Neumann]: (i) Density Matrix describes everything

(ii) Entropy of state says how to convey element.

<u>Density Matrix</u>: - pure state $\sum c_x|x\rangle \Rightarrow M = (M_{xy})_{xy} = (c_x^* \cdot c_y)_{xy}$

complex conj.

- $M \in \mathbb{C}^{2^n \times 2^n}$

- mixed state $\sum_i p_i c_x^i |x\rangle \to \sum p_i M^{(i)}$

$M^{(i)}_{xy} = (c_x^i)^* \cdot (c_y^i)$.

Claim: if ~~two~~ qubit "mixed" states $|\psi\rangle$ & $|\phi\rangle$ have same density matrix then no series of unitaries & POVM can distinguish them.

measurement

Example: $|\psi\rangle = \cos\theta\,|0\rangle + \cancel{\sin\theta}\,\sin\theta\,|1\rangle$ w.p. $\frac{1}{2}$

$\cos\theta\,|0\rangle - \sin\theta\,|1\rangle$ w.p. $\frac{1}{2}$

$|\phi\rangle = |0\rangle$ w.p. $\cos^2\theta$

$|1\rangle$ w.p. $1-\cos^2\theta$

same density $\Rightarrow$ indistinguishable.

---

Suppose system $|\psi\rangle$ is a mixture of $|\psi^i\rangle$ w.p. $p_i$ & this is known to Alice & Bob.

Now suppose $|\psi^i\rangle$ is sampled w.p. $p_i$; How many (qubits?) needed to convey this?

SKETCHY WARNING !! !!

"Entropy of $|\psi\rangle$": ~~Diagonalize density matrix;~~

~~Take~~ ~~Com~~ = Shannon Entropy of eigenvalues of density matrix!

Interesting facts: (1) Quantum Entropy $\triangleq$ von Neumann entropy predates Shannon.

(2) Generalizes Shannon!

# Quantum Communication (Noiseless Case):

Notation

## Objectives

① Transmit classical bit | $+[c \to c]$

② Transmit qubit | $+[q \to q]$

③ Share Entanglement | $+[qq]$

"+" indicates generation

## Resources

① Classical Channel | $-[c \to c]$

② Quantum Channel | $-[q \to q]$

③ Shared Entanglement | $-[qq]$

"−" indicates consumption

## ~~Simple~~ Some "Theorems"

① ⓐ $[q \to q] \geq [c \to c]$

"Can use quantum channel to communicate a classical bit"

ⓑ "Optimal" (if $\alpha[q \to q] \geq \beta[c \to c]$ then $\alpha \geq \beta$) ["Holevo's Theorem"]

- Fundamental feature of quantum mechanics.
- Proof? (I don't know.)

# + Two Non-trivial Protocols

## 2 Superdense Coding

$$[qq] + [q \to q] \geq 2[c \to c]$$

1 Qubit exchanged + 1 prior entanglement $\Rightarrow$ 2 classical bits of communication

- Say $\boxed{\text{entangled state is } \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)}$ $\leftarrow [qq]$

[notation $|b_1 b_2\rangle_{XY}$ is X in state $b_1$ & Y in state $b_2$

A → with Alice
B → with Bob]

1. Alice operates on her bit A in one of four ways

| | | | |
|---|---|---|---|
| 1 | $|0\rangle \to |0\rangle$ | $|1\rangle \to |1\rangle$ | $I$ |
| 2 | $|0\rangle \to |1\rangle$ | $|1\rangle \to |0\rangle$ | $X$ |
| 3 | $|0\rangle \to |0\rangle$ | $|1\rangle \to -|1\rangle$ | $Z$ |
| 4 | $|0\rangle \to |1\rangle$ | $|1\rangle \to -|0\rangle$ | $XZ$ |

2. $\boxed{\text{Send her qubit to Bob.}}$ $\to [q \to q]$

Bob in one of four state

1. $|00\rangle + |11\rangle$
2. $|10\rangle + |01\rangle$
3. $|00\rangle - |11\rangle$
4. $|10\rangle - |01\rangle$

All four orthogonal! Bob can distign $\to 2[c \to c]$

## 3 Teleportation

$$[qq] + 2[c \to c] \geq [q \to q]$$

[Proof in appendix. Might be omitted in lecture.]

### Main "Theorem" of Noiseless Quantum Communication

Above protocols are all that can be achieved.

if $\alpha[qq] + \beta[q \to q] + \gamma[c \to c] \geq 0$

then $(\alpha, \beta, \gamma)$ is a conic combination of

$(0, 1, -1) \to$ trivial

$(1, 1, -2) \to$ Superdense coding

$(1, -1, 2) \to$ Teleportation.

"Invitation to learn more quantum information theory".

# Appendix

- Unknown quantum state $\psi = \alpha|0\rangle + \beta|1\rangle$ in reg A. ~~Alice~~
- Shared entanglement $\phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ in regs $B \to$ Al
  & C

[A,B with Alice, B with Bo

$\Rightarrow$ Initial State =

$$\frac{1}{\sqrt{2}}\left(\alpha|000\rangle_{ABC} + \alpha|011\rangle_{ABC} + \beta|100\rangle_{ABC} + \beta|111\rangle_{ABC}\right)$$

- Alice Operations

  1. $(A,B) \to (A, A \oplus B)$
  2. Hadamard(A) : $|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ; $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  3. Measure (A,B) & send to Bob. (2 classical bits)

- Resulting State

After ①: $\frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right)$

~~After ②: $\frac{1}{2}(\alpha|000\rangle + \alpha|010\rangle + \alpha|100\rangle +$~~

After ②: 
$$\frac{1}{2}\begin{pmatrix} \alpha|000\rangle + \alpha|011\rangle + \beta|010\rangle + \beta|001\rangle \\ + \alpha|100\rangle + \alpha|111\rangle - \beta|110\rangle - \beta|101\rangle \end{pmatrix}$$

QED

| | Bob's action |
|---|---|
| $= \frac{1}{2}\big( |00\rangle_{AB}(\alpha|0\rangle + \beta|1\rangle)$ | $\to$ Nothing |
| $+ |01\rangle(\alpha|1\rangle + \beta|0\rangle)$ | $\to |1\rangle \to |0\rangle$ ; $|0\rangle \to |1\rangle$ |
| $|10\rangle(\alpha|0\rangle - \beta|1\rangle)$ | $\to |0\rangle \to |0\rangle$ ; $|1\rangle \to -|1\rangle$ |
| $|11\rangle(\alpha|1\rangle - \beta|0\rangle)$ | $\to |1\rangle \to |0\rangle$ ; $|0\rangle \to -|1\rangle$ |