Today:

Quantum Information Theory

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

QIT: Originated in the

Acknowledgements: Thanks to Amir Shamsaazadeh for asking me to learn this. To Thomas Vilich for careful lengthy explanations over email. And for pointing me to the below:


Also available as arxiv: 1106.1445
[See esp. Chapters 6 & 8].
Quantum "Information" = What it takes to describe the behavior of a quantum particle / system?

≡ What can be conveyed by a quantum particle / system?

E.g.: "Classically": \( X \sim \text{Bern}(p) \)
- describing requires "p"
- Information conveyed = \( H(p) \leq 1 \)

E.g.: Single electron may be in one of two states (or superpositions)
\( |0\rangle \text{ or } |1\rangle \) [spin up or spindown]

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

To understand: Need to understand effect of operations
- What can be "observed" or measured
Quantum State:
- 1 qubit \( \rightarrow \) 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 \( |x\rangle \in \mathbb{C}^{2^n} \) \( x \in \{0,1\}^n \)
  - \( \langle x | 1 \rangle = 0 \) \( \forall x \neq y \)
  - Mixed State = Prob. Dist. over pure states.

Quantum "Mechanics"

Only operations are "unitary"

\[ |\Psi\rangle \overset{T}{\rightarrow} |\Phi\rangle \]

\( |\Phi\rangle, |\Psi\rangle \in \mathbb{C}^{2^n} \)

must satisfy \( \{ T(|x\rangle) \} \) \( x \in \{0,1\}^n \) are orthonormal

\[ \langle T(|\Psi\rangle) + T(|\Phi\rangle) = T(|\Psi\rangle + |\Phi\rangle) \]

linearity
Measurements

- Can't read off coefficients of "qubit" or "qubit" system!

- Instead if bit in state \( |10\rangle + \beta |11\rangle \)
  measurement leads to "0" w.p. \( \alpha^2 \)
  & "1" w.p. \( \beta^2 \)

- More generally if system in state \( \leq C_x |1x\rangle \)
  get "x" w.p. \( C_x^2 \)

- Partial measurement: state \( \leq C_{xy} |1xy\rangle \)

\[ \implies \text{get "x" w.p. } \leq C_{xy}^2 \text{; resulting state } = \text{ (projected to "y" is) } \leq C_{xy}^2 |1y\rangle \]

\[ \leq C_{xy}^2 |1y\rangle \]

---

Challenge in dealing with Quantum: Unitary operations can change

different \((\alpha, \beta)\);

- But never actually reveal it!
Main Ingredients in Quantum Information Theory

1. How to describe unknown quantum state?
   "Quantum Entropy" / "Compression".

2. How to use an unknown noisy (quantum) channel to exchange bits/qubits?


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]:
  2. Entropy of a state says how to convey element.

**Density Matrix:**
- Pure state $\leq c_x |x\rangle \rightarrow M_{xy} = (c_x^* c_y)_{xy}$
- $M \in \mathbb{C}^{2^n \times 2^n}$
- Mixed state $\leq \sum_i \rho_i |i\rangle \rightarrow \leq \sum_i \rho_i M^{(i)}$
  $M^{(i)}_{xy} = (c_x^* c_y)$.
Claim: If two qubit "mixed" states $|\psi\rangle$ and $|\phi\rangle$ have the same density matrix, then no series of unitaries & POVMs can distinguish them.

Example: $|\psi\rangle = \cos \theta |0\rangle + \sin \theta |1\rangle$ 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 $|\psi\rangle$ w.p. $p_i$ and this is known to Alice & Bob.

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

"Entropy of $|\psi\rangle" := \text{Diagonalize density matrix};$

$H = \text{Shannon Entropy of eigenvalues of density matrix}$

Interesting facts:
1. Quantum Entropy $\equiv$ von Neumann Entropy $\prec$ Shannon.
2. Generalizes Shannon.
Quantum Communication (Noiseless Case):

Objectives

1. Transmit classical bit $+ [c \rightarrow c]$
2. Transmit qubit $+ [q \rightarrow q]$
3. Share Entanglement $+ [qq]$

Notation

"+" indicates generation

Resources

1. Classical Channel $- [c \rightarrow c]$
2. Quantum Channel $- [q \rightarrow q]$
3. Shared Entanglement $- [qq]$

"-" indicates consumption

Some "Theorems"

1. $[q \rightarrow q] \geq [c \rightarrow c]$
   "Can use quantum channel to communicate a classical bit"

5. "Optimal" if $\alpha [q \rightarrow q] \geq \beta [c \rightarrow c]$
   (then $\alpha \geq \beta$
   "Holevo's Theorem"
   - Fundamental feature of quantum mechanics.
   - Proof? (I don't know.)
Two Non-trivial Protocols

1. Superdense Coding

\[ [q_1] + [q \rightarrow q] \geq 2 [c \rightarrow c] \]

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

- Say entangled state is \( \frac{1}{\sqrt{2}} (|00\rangle_A^B + |11\rangle_A^B) \)

[notation \( |b_x, b_y\rangle_{xy} \)]

is \( x \) in state \( b_x \)

\( y \) in state \( b_y \)

A \( \rightarrow \) with Alice

B \( \rightarrow \) with Bob

1. Alice operates on her bit \( i \) in one of four ways

   1. \( |0\rangle \rightarrow |0\rangle \)
   2. \( |0\rangle \rightarrow |1\rangle \)
   3. \( |0\rangle \rightarrow |0\rangle \)
   4. \( |0\rangle \rightarrow |1\rangle \)

2. Send her qubit to Bob.

Bob in one of four state

\[ [q \rightarrow q] \]

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 distinguish
Teleportation

\[ [q_2] + 2[c\rightarrow c] \geq [q_2 \rightarrow 2] \]

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

Main "Theorem" of Noisless Quantum Communication

Above protocols are all that can be achieved. If

\[ \lambda [q_2] + \beta [q_2 \rightarrow 2] + \gamma [c\rightarrow c] \geq 0 \]

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

- \((0, 1, -1) \rightarrow \text{trivial}\)
- \((1, 1, -2) \rightarrow \text{Superdense coding}\)
- \((1, -1, 2) \rightarrow \text{Teleportation}\)

"Invitation to learn more Quantum Information Theory"
Appendix

- Unknown quantum state $\Psi = \alpha|0\rangle + \beta|1\rangle$ in reg $A$.

- Shared entanglement $\Phi = \frac{1}{\sqrt{2}} \left( |100\rangle + |111\rangle \right)$ in reg $B \rightarrow C$.

\[ \left[ A, B \text{ with Alice, C with Bob} \right] \]

$\Rightarrow$ 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. $(A, B) \rightarrow (A, A \oplus B)$
  2. Hadamard $(A): |0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$; $|1\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$
  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: $\frac{1}{2} \left( \alpha |000\rangle + \alpha |101\rangle \right)$

  After 3: $\frac{1}{2} \left( \alpha |000\rangle + \alpha |101\rangle + \beta |110\rangle + \beta |100\rangle + \beta |110\rangle - \beta |010\rangle \right)$

\[
= \frac{1}{2} \left( \begin{array}{l}
100\rangle_A (\alpha |0\rangle + \beta |1\rangle) \\
+ 101\rangle_B (\alpha |1\rangle + \beta |0\rangle) \\
110\rangle (\alpha |0\rangle - \beta |1\rangle) \\
111\rangle (\alpha |1\rangle - \beta |0\rangle)
\end{array} \right)
\]

$\Rightarrow$ Bob's action:

\
\begin{array}{l}
-> \text{Nothing} \\
\rightarrow |1\rangle \rightarrow |10\rangle; |10\rangle \rightarrow |11\rangle \\
\rightarrow |10\rangle \rightarrow |10\rangle; |11\rangle \rightarrow |11\rangle
\end{array}