1/4/2010

Lecture 1

- Introduction of myself
  - how got into quantum
- get names + interests from everyone

- syllabus

10-15 min.

What is quantum Shannon theory?

study of capability of noisy phys. systems to preserve correlations.

named after Shannon - "father of info. theory"

"q. info science" is too broad

q. comp., q. algo., q. complexity theory, quantum communication complexity theory, ent. theory, QKD, QEC, ...

— connected to these subfields

- need to know quantum gates (q. comp)
- private information transmission is intimately related to BB84 QKD
- quantum capacity related to quantum error correction

1/4/2016

QST = Info theory ∧ Quantum Mechanics

1970s (much more effort in 1990s) (ongoing efforts) — 1948 (done) — 1926 (done)

"second quantum revolution"

Info theory – founded by Shannon in 1948

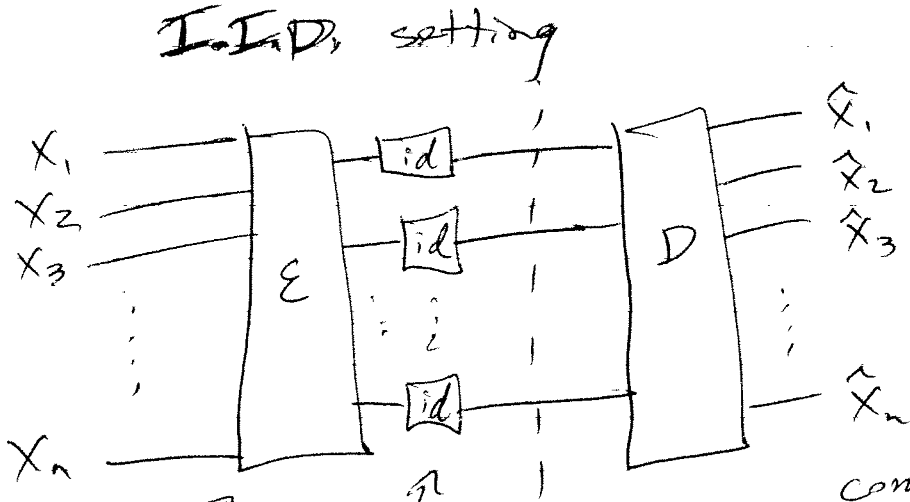
– single-handedly solved two of the most important tasks & laid the foundations

just mention these for now (more detail next class)

<u>Data Compression</u>

information source – some random variable X w/ dist. $p_X(x)$

I.I.D. setting



local comp. free

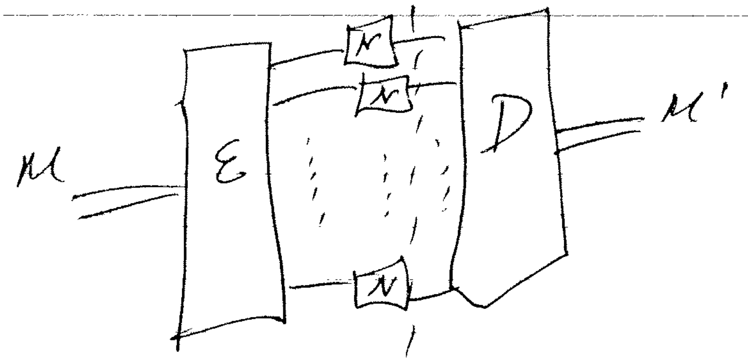
noiseless bit channels ← expensive

What is the rate at which we can comm. error free?

compression rate = $\frac{\#\text{ noiseless channel bits}}{\#\text{ of source symbols}}$

1/4/2016

Data Transmission over a channel



channel is some $P_{Y|X}(y|x) \equiv \mathcal{N}$

What is the rate at which error-free comm. is possible?

Shannon trounced both questions.

* "info. theory is an application of prob. theory"

Uncertainty in info. theory comes about due to lack of knowledge.

(different from "quantum uncertainty")

1/4/2014

QM

Brief History

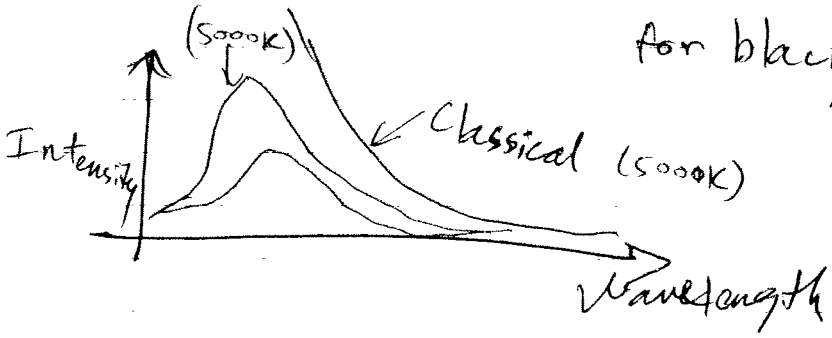
1890 – "In phys., almost everything is already discovered, & all that remains is to fill a few holes."
— Advisor of Planck

Newton, Maxwell, & Boltzmann
(CM) (EM) (SM)
explained everything

Two Clouds (Kelvin)

– first cloud – Michelson & Morley experiment failed to verify the "ether theory". This theory predicted that speed of light should change

– second cloud – ultraviolet catastrophe for blackbody radiation
↑ ideal absorber of light at all frequencies



1/4/2014

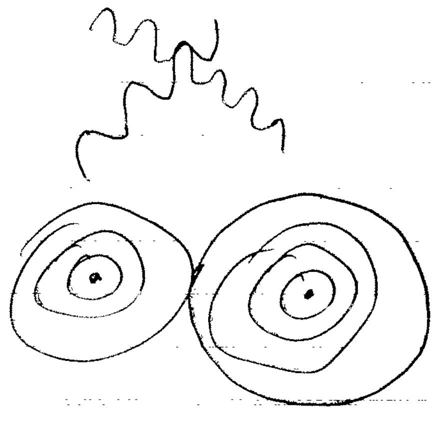
- Planck (1900) explained the curve by making a "quantum" assumption
- Einstein used Planck's assumption to (1905) explain the photoelectric effect
  (current induced in a metal when frequency of light shining on it is above certain frequency)
- de Broglie (1924) every element of matter (photon, atom, or electron, etc.) has both particle & wave behavior (electron diffraction)
- Schrödinger (1926) established a wave equation, that governs evolution of a closed quantum system
  "wave mechanics"
- Heisenberg (1925) "matrix mechanics"
  physicists did not get it
- Dirac (1930) unified these two pictures in his book
  - introduced "Dirac notation"

1/4/2014

Concepts in QM

1. Indeterminism – contrast w/ determinism & Laplace's demon.
   - can occur in a classical theory
   - feature of QM but not unique to it.

2. Interference = another feature of QM



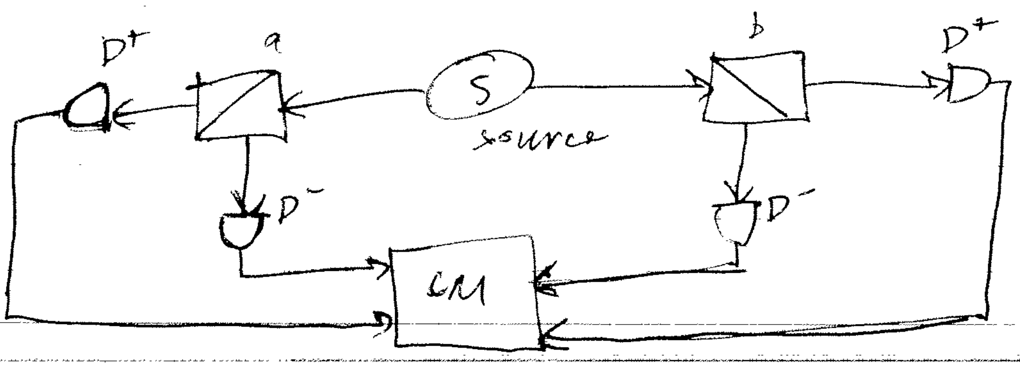
   constr. when crests meet
   destr. when crest meets trough
   - in QM, can occur at the "single-particle" level

3. Uncertainty – (different from indeterminism, but can lead to it)
   - Nature is fundamentally uncertain "weirdness"
   - measure position cannot know anything ~~about~~ momentum & vice versa
   - can exploit in QKD

4. Superposition principle – quantum object can be in a superposition of two allowable states
- due to linearity of Schrödinger eqn
Sps. ψ + ϕ are solutions
then $\alpha\psi + \beta\phi$ is also a solution
- particle is in one location or another.

5. Entanglement – most striking feature
- correlations stronger than any classical correlations
- ~~Bell test~~ most similar to a secret key (but not really)
- now, a resource for q. communication

typical "Bell test"



$$E(a,b) = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N}$$

estimate $\underbrace{E(a,b) - E(a,b') + E(a',b) + E(a',b')}_{\text{Bell quantity } B}$

classically, $|B| \leq 2$

quantumly $|B| \leq 2\sqrt{2}$

Ideas in QST

Physical bit vs. Information Bit

Physical bit ↓ "on" or "off" — light switch, transistor, ...

Information Bit: fair coin — "measure of surprise" upon learning outcome of coin toss; information associated w/ random outcome — Shannon entropy

$H(p) \equiv -p\log_2 p - (1-p)\log_2(1-p)$

Physical Qubit vs. ~~Quantum~~ Information Qubit

Physical Qubit: electron spin, polarization of a photon, atom w/ G & excited state

Information Qubit: ~~someone~~ we prepares as $|\uparrow_z\rangle$ "spin up in z direction"

1/4/2014

- we know its state is $|\uparrow_z\rangle$ & there is no surprise upon learning this
- zero qubits of information

- could also measure in x direction
  will later learn that it becomes
  $|\uparrow_x\rangle$ or $|\downarrow_x\rangle$ w/ equal prob.

  Before performing measurement,
  shannon info. of outcome is 1 bit

Which measure is correct?

one that reveals the least amount of information
we know that the state is $|\uparrow_z\rangle$
so there are zero qubits of information

What if friend prepares

$|\uparrow_z\rangle$ w/ prob. 1/2 or
$|\downarrow_z\rangle$ w/ prob. 1/2

states are distinguishable by measurement in z direction - learn one bit
but turns out that all observations of measurements are the same as if ~~ensemble~~ is

$|\uparrow_x\rangle$ w/ prob 1/2
$|\downarrow_x\rangle$ w/ prob 1/2

measurement in x direction gives
same information

Suppose friend prepares

$|\uparrow_z\rangle$ w/ prob 1/2

$|\uparrow_x\rangle$ w/ prob 1/2

if Bob reveals which state was prepared,
we learn 1 bit of information

Sps. want to learn on our own

could perform measurement in z direction

$|\uparrow_z\rangle$ w/ prob 1/2 } 3/4

→ $|\uparrow_z\rangle$ w/ prob. 1/4

$|\downarrow_z\rangle$ w/ prob. 1/4

action of measurement inevitably disturbs
in this case

.81 bits of info

can perform measurement that learns
least amount of info.

intuitively, ideal b/c requires "fewer questions"

measurement in x+z direction gives

$|\uparrow_{x+z}\rangle$ w/ $\cos^2(\pi/8)$ .6 bits of info

$|\downarrow_{x+z}\rangle$ w/ $\sin^2(\pi/8)$ least info among all measurements

1/4/2014

Operational tasks in QST

- noiseless qubit channel - e.g., free space for photons
- noiseless classical bit channel
- noiseless ebit

protocols - teleportation uses 2 cbits + 1 ebit to make qubit channel

Schumacher compression - compress a quantum state

classical info. over noisy quantum channel

" " " EA quantum channel

private info. over quantum channel

quantum " " " "

progress in this way

trade-off questions

History

1970s - Helstrom, Gordon, Stratonovich, Holevo

Helstrom ↑ detection & estimation

Gordon ↑ conjectured bound on accessible info. in q. system

Holevo ↑ proved it

1/4/2018

Wiesner – "quantum money" 1970
accepted in 1983

Fannes 1973 – continuity property of quantum entropy

1980s – Feynman 1982 – quantum computing

Wooters & Zurek responded to the FLASH w/ no-cloning theorem

1984 – Bennett & Brassard
QKD used Wiesner's "quantum money" idea

1990s –
'91 Ekert entanglement-based QKD

'92 Bennett QKD

'92 – super dense coding
entanglement boosts capacity

'93 – teleportation

'94 – Shor – factoring algorithm

'95 – Shor – quantum error correction
& posed quantum capacity problem

'95 – Schumacher compression

'96 – HSW theorem ~~about thirty years~~

Devetak & Cai, Winter, Yeung
private capacity

2000s

2002 – EA classical capacity Bennett et al.
2005 – interpretation of negative entropy
2008 – Smith & Yard superactivation

2005 and on – network quantum Shannon theory