

Lecture 1

①

Information theory studies the asymptotic performance and resource use of communication tasks.

Resources include noiseless or noisy channel uses, and perhaps other things as well: shared randomness, secret keys, side information, etc.

Communication is assumed to be costly and limited.

Processing information before and after transmission is assumed to be unlimited: no concerns about computational complexity, etc.

Asymptotic: we consider only the limit when messages become very long. Many complications in the finite case (the domain of coding theory) become unimportant asymptotically.

The typical result of an IT calculation is a rate or set of rates for the comm. task.

IT was invented almost single-handedly in 1948 by Claude Shannon, who defined the problem, and developed the core techniques still used today. He proved two fundamental theorems about the two paradigmatic communication problems: noiseless coding (compression) and noisy coding (error correction/channel capacity).

We will look at these two problems in more detail shortly. But the first insight was to treat the message (or source) as an i.i.d. stream of symbols drawn from a finite alphabet. In other words, we ignore the meaning of a message and treat it as a random string of arbitrary letters. ②

The simplest alphabet has just two symbols: 0 and 1. We can choose this wlog. What is a bit? (bit = "binary digit")

- ① A mathematical variable that can take 2 discrete values (e.g., 0 & 1)
- ② A physical system that can represent or store 1 bit (in the sense of ①).
- ③ A unit or measure of information gain.

All 3 of these play a role in IT (and their quantum analogs in QIT). Note that ③ is not an arbitrary measure or mathematical function: it also has an operational meaning, as the rate with which a certain task (Shannon compression) can be performed. This connection between entropic quantities and operational

interpretations will be a running theme
of this course.

More on this shortly. First: what is
quantum IT?

QIT studies the asymptotic performance
and resource use of quantum comm. tasks.

QIT is more complicated than IT (and
includes classical IT as a proper subset),
because it includes of more kinds of resources
(quantum and classical) and a richer array
of communication tasks.

Examples of classical resources:

Bit channels
Shared randomness
Shared secret key } and noisy versions
thereof

Examples of classical comm. tasks:

Transmitting a classical message
Storing a random info. source (compression)

There are some examples of Q resources: ④

(Classical) bit channel

Quantum (qubit) channel

Shared entanglement

Coherent bit ("cubit") channel

} and noisy versions

Moreover, there are many more kinds of quantum noise than classical.

Examples of Q comm. tasks:

Transmitting a classical message

Distributing a secret random key

Transmitting a Q state

Distributing shared entanglement

:

Many kinds of IT tasks (classical or quantum) can be thought of as using one (or more) kinds of resources to produce (or simulate) another.

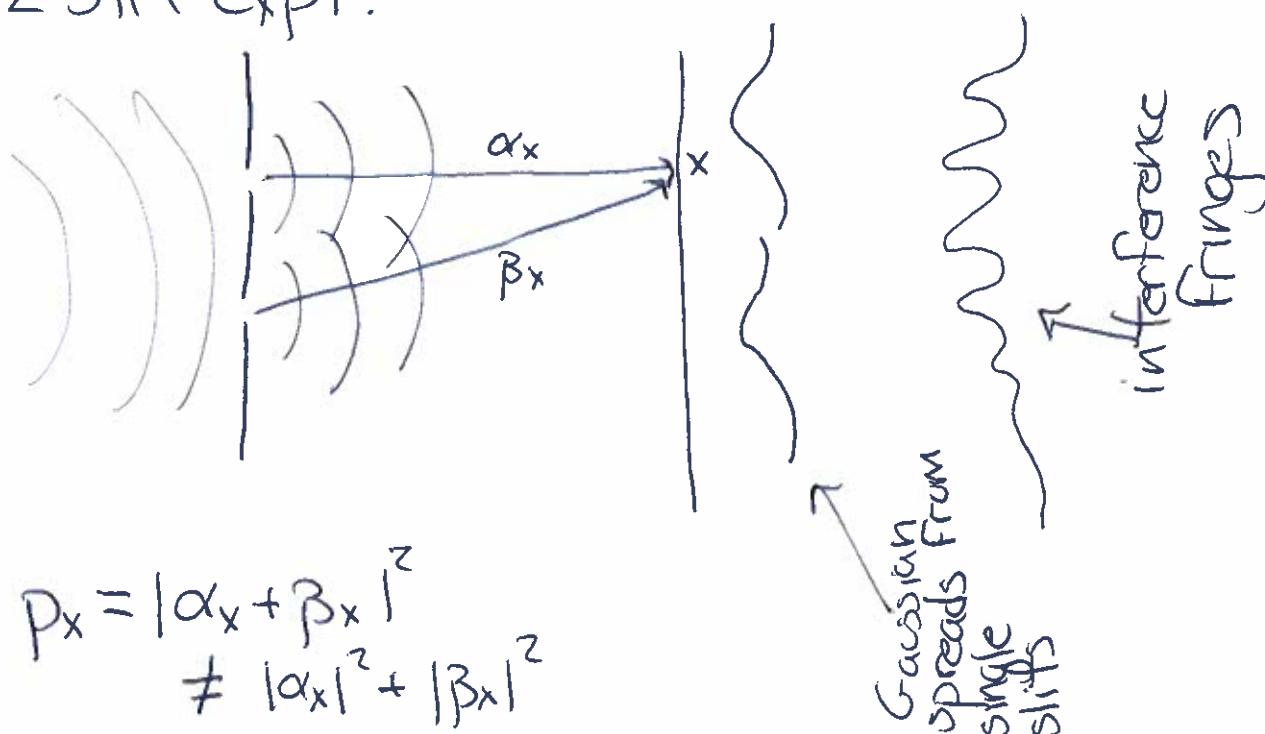
For instance, the noisy channel coding theorem shows that one can simulate a noiseless channel using (more instances of) a noisy channel. These relationships among resources (resource inequalities) and interconversion rates are important conceptual tools in QIT.

Properties of Q systems.

We will define these properties more rigorously next week; but now we will discuss qualitatively.

1. Indeterminism. QM makes only probabilistic predictions about Q systems. In measuring a property of a Q system, the meas. outcome is in general unpredictable, even in principle.
2. Interference. QM is a linear theory - like a classical wave theory - and the quantities it predicts are not probabilities but prob amplitudes: complex numbers or related to probs by $P = |\alpha|^2$.

2 slit expt:



Q computers use interference to design new kinds of algorithms. ⑥

3. Uncertainty and complementarity. Not all properties of a Q system can simultaneously have well-defined values. If one property does have a well-defined value, then measuring an incompatible (complementary) ~~extra~~ quantity will yield a random outcome, and erase (disturb) the value of the original quantity.

e.g., position vs. momentum

different components of spin

Uncertainty is used in Q cryptography to insure the security of key distribution.

4. Superposition. Since QM is linear, linear combinations of solutions are still solutions. If ψ, ϕ are valid states, so is $\alpha\psi + \beta\phi$ (up to normalization).

Superposition is used in Q computing and Q comm. for what is called "quantum parallelism" (somewhat deceptively).

5. Entanglement. This is the least intuitive, and one of the most important for QIT. Q systems with 2 or more subsystems can be prepared in an entangled (correlated) joint state; but, in a certain technical sense, this correlation is stronger than any classical probabilistic correlation could be. One way to see this is to note that shared prob. correlations cannot be used to boost the rate of classical comm., but shared entanglement can (superdense coding). Two systems in ^(e.g., 2 spins) an entangled state can be physically separated and remain entangled; but entanglement cannot be created remotely.

Long history: Schrödinger, EPR, ~~and~~ John Bell. Modern idea of using entanglement as a resource comes from Bennett and collaborators: Q teleportation, superdense coding.

Brief History of QIT

1948 — Shannon's groundbreaking paper. Since all systems are fundamentally quantum, this is the first QIT result.

1970s — Work by Glauber and others led to the question of Q limits on communication using optical states. Work by Glauber, Helstrom, ~~Helstrom~~, Gordon, Stratonovich, Fannes, Levitin, and especially Holevo: Holevo proved a limit (the Holevo bound) that states that a "quantum bit" (qubit) can transmit no more than one classical bit (cbit). Wiesner invented "quantum money."

1980s — Wiesner's idea led Bennett & Brassard to invent Q crypto in 1984: the BB84 protocol. Wootters and Zurek proved the "no-cloning thm," in 1982. Feynman, Mamin and Benioff all independently postulated the Q computer. Deutsch (in 1985) demonstrated the first Q algorithm. ~~Dieks~~ also independently proved "no cloning."

1990s — Ekert devised ~~a~~^a a crypto scheme⁽⁹⁾
(1991) based on entanglement. Bennett and
collaborators invented Q teleportation and
Q superdense coding (1993). Then in 1994, Shor
published his algorithm for factoring and
the field exploded.

A Few highlights:

Schumacher compression 1995

Q error correction (Shor, Steane, Calderbank
and Shor; Laflamme et al., Gottesman, etc., etc.)

1996 and onward

Lloyd defines Q capacity and gives an
intuitive proof (1997); made more
rigorous by Shor (2002) and finally
proven by Devetak (2005).

In the late 1990s and 2000s, the few
scattered results of QIT were made rigorous
and combined into a rich, comprehensive
(but still incomplete) theory. That is
what we will study in this class.