1. Preview of the course:

- Information processing

- Information is physical

- Quantum mechanical consequences on information processing

- Physics is information theoretic

Examples of information processing:

- storage and communication of data

Examples of information processing:

- storage and communication of data

- computation (getting an answer from input data
  e.g. factoring, search, coloring of a graph)

Examples of information processing:

- storage and communication of data

- computation (getting an answer from input data
  e.g. factoring, search, coloring of a graph)

- cryptography (info processing in the presence of
  a malicious adversary)

Examples of information processing:

- storage and communication of data

- computation (getting an answer from input data
  e.g. factoring, search, coloring of a graph)

- cryptography (info processing in the presence of
  a malicious adversary)

- error correction and fault tolerance (combating
  noise)

Examples of information processing:

- storage and communication of data

- computation (getting an answer from input data
  e.g. factoring, search, coloring of a graph)

- cryptography (info processing in the presence of
  a malicious adversary)

- error correction and fault tolerance (combating
  noise)

While formulated in the abstract for full generality, these tasks have to be implemented with physical devices ...

Information is physical (Landauer 1991)

e.g. 1. Church-Turing thesis: what's computable should not depend on the specifics of a physically reasonable model of computation.

Information is physical (Landauer 1991)

e.g. 1. Church-Turing thesis: what's computable should not depend on the specifics of a physically reasonable model of computation.

e.g. 2. Moore's law stating that computing power doubles every year at constant cost must end before transistors and memory reach atomic size.

Information is physical (Landauer 1991)

e.g. 1. Church-Turing thesis: what's computable should not depend on the specifics of a physically reasonable model of computation.

e.g. 2. Moore's law stating that computing power doubles every year at constant cost must end before transistors and memory reach atomic size.

e.g. 3. RSA can be hacked by power analysis -- the value of the private key affects how many elementary operations are needed for decryption.

Information is physical (Landauer 1991)

e.g. 4. Landauer's principle (1961):
The second law of thermodynamics implies that energy is required to erase information.

Does this impose a fundamental energy requirement for computation?

Information is physical (Landauer 1991)

e.g. 4. Landauer's principle (1961):
The second law of thermodynamics implies that energy is required to erase information.

Does this impose a fundamental energy requirement for computation?

Bennett (1973):
Computation can be always be made reversible!

Information is physical (Landauer 1991)

e.g. 4. Landauer's principle (1961):
The second law of thermodynamics implies that energy is required to erase information.

Does this impose a fundamental energy requirement for computation?

Bennett (1973):
Computation can be always be made reversible!

Corollary 1: Energy consumption in computation is unnecessary.

Information is physical (Landauer 1991)

e.g. 4. Landauer's principle (1961):
The second law of thermodynamics implies that energy is required to erase information.

Does this impose a fundamental energy requirement for computation?

Bennett (1973):
Computation can be always be made reversible!

Corollary 1: Energy consumption in computation is unnecessary.

Corollary 2: A quantum computer can do classical computation.

If our computing devices are quantum,
how will information processing change?

1. Computationally:

a. Deutsch 85
Church-Turing thesis must be "quantized"

If our computing devices are quantum, how will information processing change?

1. Computationally:

a. Deutsch 85
Church-Turing thesis must be "quantized"

b. Feynman 85
A quantum computer "may" vastly outperform classical computers if we want to simulate a given quantum system (e.g., q chemistry).

If our computing devices are quantum,
how will information processing change?

1. Computationally:

c. Fast quantum algorithms

Deutsch-Josza (92)
Simon's algorithm (94)
Shor's factoring algorithm (94)
Grover's search algorithm (96)
....

Will see these week 3-6

Modern algorithms in linear programming, semi-definite programming, optimization, machine learning.

If our computing devices are quantum, how will information processing change?

2. Cryptographically:

a. Quantum algorithms break many classical cryptographic scheme (RSA, some elliptic curves). NSA has recommended moving to "post-quantum -crypto" -- classical schemes that may remain quantum safe.

If our computing devices are quantum,
how will information processing change?

2. Cryptographically:

b. Quantum effect provides new methods to detect adversarial behavior.

Wiesner (1970): quantum money.
Bennett, Brassard, Breidbart (1983): key recycling
Bennett, Brassard (1984): quantum key exchange
Ekert (1991): quantum key exchange
...

Will see these end of March.

3. Information theoretically: (fundamental capacities of communication channels to transmit data)

3. Information theoretically: (fundamental capacities of communication channels to transmit data)

(a) There is a continuum of quantum states in a finite dimensional quantum system.

But they are not distiguishable from one another.

3. Information theoretically: (fundamental capacities of communication channels to transmit data)

(a) There is a continuum of quantum states in a finite dimensional quantum system.

But they are not distiguishable from one another.

(b) Holevo (1973) : a d-dim quantum system can only carry d classical messages.

3. Information theoretically: (fundamental capacities of communication channels to transmit data)

(a) There is a continuum of quantum states in a finite dimensional quantum system.

But they are not distiguishable from one another.

(b) Holevo (1973) : a d-dim quantum system can only carry d classical messages.

(c) Bennett-Wiesner (1992): Superdense coding
Entanglement can be used to double the number of bits carried by a quantum channel.

3. Information theoretically: (fundamental capacities of communication channels to transmit data)

(a) There is a continuum of quantum states in a finite dimensional quantum system.

But they are not distiguishable from one another.

(b) Holevo (1973) : a d-dim quantum system can only carry d classical messages.

(c) Bennett-Wiesner (1992): Superdense coding
Entanglement can be used to double the number of bits carried by a quantum channel.

...

My group (2010): we can increasing the number of bits carried perfectly by a noisy classical channel and suppress error using entanglement.

New challenges:

Need to manage quantum noise

a. mixed state quantum mechanics (late Feburary)

b. discretization of quantum computation (January)

c. quantum error correction & fault-tolerance (March)

Quantum information has in turns changed the foundations of the constituent subjects

---

a. Information theory in physical processes gives many physical laws

Quantum information has in turns changed the foundations of the constituent subjects

---

a. Information theory in physical processes gives many physical laws

e.g., Lieb-Robinson bound for speed of communication
entanglement in exotic phases of matter
insights to blackhole information paradox,
interpretations of quantum mechanics
quantum error correcting codes model Anti-deSitter space
...

Quantum information has in turns changed the foundations of the constituent subjects

---

a. Information theory in physical processes gives many physical laws

e.g., Lieb-Robinson bound for speed of communication
entanglement in exotic phases of matter
insights to blackhole information paradox,
interpretations of quantum mechanics
quantum error correcting codes model Anti-deSitter space

b. quantum proofs of classical complexity results

Quantum information has in turns changed the foundations of the constituent subjects

---

a. Information theory in physical processes gives many physical laws

e.g., Lieb-Robinson bound for speed of communication
entanglement in exotic phases of matter
insights to blackhole information paradox,
interpretations of quantum mechanics
quantum error correcting codes model Anti-deSitter space

b. quantum proofs of classical complexity results

c. 2020: MIP*=RE disproves the Connes Embedding conjecture (open problem in operator algebra)