This course is an introduction to the physics of quantum information and quantum computing. The topic is highly interdisciplinary, touching upon many mathematical, scientific and engineering domains. It is assumed that students are mathematically proficient, and know the basics of quantum mechanics at the level of two state systems. We will develop principals of information theory and quantum dynamics leading up to the design and operation operation of quantum gates and algorithms that exploit their novel capabilities. Ultimately we will write simple code to run on an IBM cloud quantum computer.

A course web site at http://euler.phys.cmu.edu/widom/teaching/33-658 contains this syllabus plus links to day-by-day lecture coverage and weekly homework assignments.

Books:
1. Schumacher and Westmoreland, Quantum Processes Systems, and Information
2. Nielsen and Chuang, Quantum Computation and Quantum Information
3. Mermin, Quantum Computer Science
4. Feynman, Lectures on Computation

We mainly use the book by Schumacher and Westmoreland, chapters 1-9 and 18-20. The other books are useful and interesting references. Other papers and notes will be placed on Canvas.

Online Resources:
1. Preskill Lecture notes on quantum computing and quantum information
2. Aaronson Lecture notes! Intro to Quantum Information Science
3. de Wolf Quantum Computing; Lecture Notes
4. Berkeley Qubits,Qubits, Quantum Mechanics, and Computers
5. IBM Q Cloud quantum computing

Grading: Letter grades will be based on homework, a midterm exam on Tuesday October 19, and a final exam (date to be determined), in proportions of 20:30:50. Homework assignments are listed at http://euler.phys.cmu.edu/widom/teaching/33-658/hw.html.

Course Outline:

Note this outline is only approximate. Actual class coverage can be found here.
1. Classical Shannon information, Maxwell's demon and Landauers principle
2-3. Quantum review, cryptography
4. Unitary transformations, entanglement. Quantum key distribution
5. EPR, Bell and GHZ paradoxes. Quantum logic gates
History

- 1970  Stephen Wiesener  Quantum money
- 1982  Richard Feynman  Quantum simulator
- 1984  Charles Bennett  Cryptographic key distribution
- 1985  David Deutsch  Universal quantum computer
- 1992  Deutsch-Josza  Q-Comp > C-Comp
- 1994  Peter Shor  Exponential speedup (factoring)
- 1995  Peter Shor  Quantum error correction
- 1996  Lov Grover  Quadratic speedup (search)
- 2001  IBM factors $N = 15$ by NMR
- 2003  Innsbruck runs Deutsch-Josza on ion trap - bit
- 2007  Yale develops transmon superconducting q
- 2017  China achieves ground-to-satellite teleportation
- 2019  Google claims quantum supremacy
Information - a physical quantity

how to quantify it  how to use it

Probability distribution

\[ P(t) \geq 0 \quad \sum_{t \in T} P(t) = 1 \]

Information \( I(t) = -\log_2 P(t) \)  units bits

- \(-\ln P\)  " nats
- \(-k_B \ln P\)  " Joule/Kelvin

Why \( \log \)? Game of 20 questions  \( P = 1/N \quad N \approx 127,000 \) words

bisection strategy: # yes/no questions = \( \log_2 N \approx 16.9 \)

Proof that \( I = -\log P \)

Let \( P_0 = 1 - S \)

1. \( I(P(t)) \geq 0 \)
2. \( I(P) \downarrow \) as \( P \uparrow \)
3. \( I(1) = 0 \)
4. \( I(P) \) Smooth
5. \( I(P(t_1), P(t_2)) = I(P(t_1)P(t_2)) \)

\[ = I(P(t_1)) + I(P(t_2)) \]
**Improved strategy for 20 questions**

Word usage frequency (http://wordfrequency.info)

Top $N = 5,000$ words

$$\log N = 12.3$$

Shannon (1948)

$$H = - \sum_i P_i \log P_i = 9.3$$

Save 3 questions!

**Correlated variables e.g. dice**

$X = \text{value on top}$

$Y = \text{value on bottom}$ \quad \{ \text{perfectly correlated} \}

$X = \text{value on top} \quad \text{e.g. 1}$

$Y = \text{value on face} \quad \text{e.g. 2, 3, 4, 5}$

$$H(X) = \log 6 \quad H(X,Y) = \log 24$$ \quad \text{joint entropy}

$$H(Y) = \log 6 \quad H(Y|X) = \log 4$$

$$H(X|Y) = \log 4$$ \quad \text{conditional entropy}

**Chain rule**

$$H(Y|X) = H(X,Y) - H(X) = \log 24 - \log 6 = \log 4$$

**Mutual information**

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = \log 32$$

$$\log 6 \quad \log 6 \quad \log 24$$
**Bioinformatics**

**DNA sequence** ACCT \( \cdots \)  
\[ H = \log_2 4 = 2 \]  
Actual is 1.9 - 2.0

**Codons**  
\[ H = \log_2 6^3 = 6 \]  
Actual is 5.2 - 5.8

**Amino acids** ABCEF \( \cdots \)  
\[ \log 2.2 = 1.5 \]  
Actual is 3.6 - 4.2

\[ 4^3 = 64 \Rightarrow \text{codon redundancy} \]

\[ \text{e.g., } CAI = Q, \text{ CAG = Q} \]

**Mutual information after \( k \) base pairs** (Grosse, 2000)

![Graph of mutual information vs. distance](image)

- **Coding DNA**
- **Non-coding "junk" DNA**

**Venn diagram**