CSCI 5370 Quantum Computing

(Spring 2025)

Week 1

Instructor: Xiao Liang

Course homepage: https://xiao-liang.github.io/Resources/Courses/CSCI5370-Spring25.html

About the Instructor:

Why's a cryptographer teaching CSCI 5370 Quantum Computing ?

- Quantum cryptographers know QC very well, sometimes even better than QC experts
- Quantum cryptography is a flagship app. of QC. (You'll see it this semester)
- Boundary between QC and Quantum cryptography is blurred.

Today's Agenda:

① Introduction & administrativa.

② Qubits, One-qubit System.

Motivation.

- What is QC
- Why is QC useful? Applications?
- state-of-the-art quantum computers?
  E.g. IBM's, Google's.

Won't waste time on them...

not in a postgraduate course.

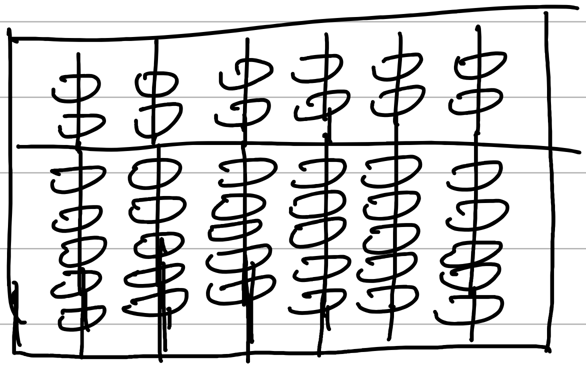
On-line resource:

On-line resources for that:
- The first lecture of Henry Yuen's course: https://www.youtube.com/watch?v=X2vJGA1yFrs

QC in contrast to "Classical" Computing.

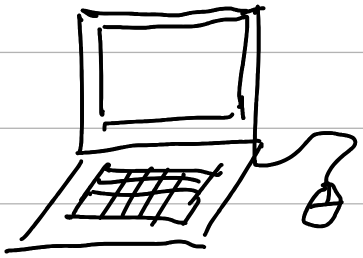
Essence of any computing device:
(E.g. abacus, calculator, laptop ...)

- encoding
- manipulating



mechanical computing device

physics	logic
Classical mechanics $\vec{F} = \frac{d}{dt} \vec{P}$	encoding: ? manipulating: ?



electrical
computing device

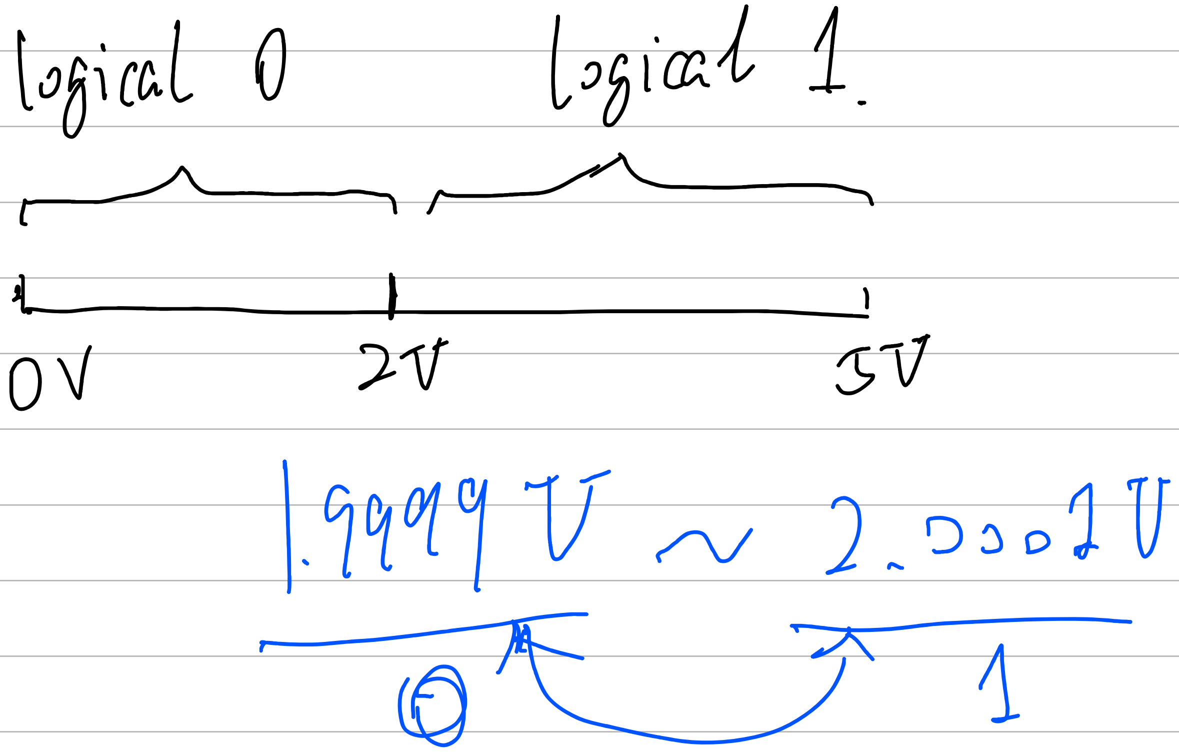
physics	logic
Electrodynamics	encoding : ? binary bits
	manipulating: ? cup

$$\begin{cases} \nabla \cdot \mathbb{E} = \frac{\rho}{\varepsilon_0} \\ \nabla \cdot \mathbb{B} = 0 \\ \nabla \times \mathbb{E} = \frac{\partial}{\partial t} \mathbb{B} \\ \nabla \times \mathbb{B} = \mu_0 \left(J + \varepsilon_0 \frac{\partial}{\partial t} \mathbb{E} \right) \end{cases}$$

Maxwell's equations.

Voltage levels to represent bits:

voltage level:



Error Correcting Code

Summary:

Computing device = A set of rules:
- encoding
- manipulating

\+ The physics implementing the rules

Let's use this formula to approach Quantum Computing!

physics	logic
Quantum Mechanics:	encoding: qubits
$i\hbar \frac{\partial}{\partial t}\|\psi\rangle = \hat{H}\|\psi\rangle$	manipulating: "4 postulates of QM"

Scope of CSCI 5370:

- The "logic" part.
- Use quantum mechanics as axioms.
    - no explanation (cost a 2-semester course of QM)
- Get you familiar with { encoding / manipulating

Do interesting things with them

(Course homepage for topics)

(Conceptual) Learning outcome (See course homepage)

- how QC differs from "classical" comp.
- Get an idea of the SOTA of theoretical QC
- Big questions and research opportunities
- Interdisciplinary.

Who this course is NOT for:

- People who want to learn how to build a quantum computer.
- People who want to learn QM.

Prerequisites:

- "Hard" prerequisites:
  - Linear algebra
  - Probability theory
- "Soft" prerequisites:
  - Algorithm (Design & analysis)
  - Computational Complexity (Theory of Computation)

Administriva:

$$\text{Grading} \begin{cases} \text{homework} & 30\% \\ \text{midterm} & 30\% \\ \text{Project} & 40\% \end{cases}$$

Homework: (30%)

- Weekly (Workload: recall your undergrad Calculus / Linear Algebra / Probability)

- two types:

① Reading Assignments:

- preview of next lecture topics
- supplementary reading materials of lecture topics

(I have no way to check this part)

② "Standard" problem-solving assignments:

- Practice your "quantum calculation" skills
- complete missing steps in lecture proofs.
- Submission MUST be in LaTex code.

Midterm: (30%)

- Same style as Problem-Solving assignments.
- I don't test your memory.

(Necessary formulas will be provided on the exam sheet.

I'm also considering open-book exam)

Project: (40%)

- 4-5 people per group.
- choose a QC-related topic.
  - I'll provide a list of topics.
  - Talk to me if you have your own.
- Write a paper on the chosen topic:
  - Literature survey.
  - Systematization of knowledge (SoK)
  - Pedagogical explanation of a published paper.
  - Anything that convinces me that you've learned something new, related to Q.C.
- If you solve an open problem, you'll get A regardless of your other performance.

- Run a mock Conference:
  - Say we have 10 groups. (thus 10 papers)
  - Each group choose 4-6 papers.
    - Read them
    - Write reviewers' comments
    - Grade them.
  - 3-5 papers with highest scores will win the "Best Paper Award":
    - Bonus points to group members final grades
    - Give a 45-min talk to the class.

[Don't worry. I'll provide step-by-step instructions when the project starts.]

A Project-Oriented Perspective of CSCI 5370

All we learn is for the final Project.

① First half of the course:
  - Basic skills of QC.

② Second half of the course:
  - Examples how other people do their "projects"

③ Final Project of CSCI 5370:
  - Do your own project.

Eventual Goal:

Bring QC skills to your own research / job / project

Textbook:

- No official textbook
- Will assign different chapters from diff. books as reading assigment.
- See course homepage for a recommended reading list.

TA and Office hour:

- Mr. LUO, Robin Bin
- Tue 2:30 - 3:30 pm
  Room 120, Ho Sin Hang Engineer Bldg.

Physics	logic
Quantum Mechanics	Encoding: qubits manipulating: "4 postulates"

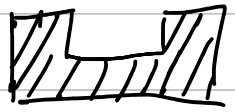
The 4 Postulates for Single-Qubit System.

Classical:

0 or 1 (classical bit)

register position

Quantum:



a quantum register.

A qubit: $|0\rangle$, $|1\rangle$.

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

where $\alpha, \beta \in \mathbb{R}$
and $\alpha^2 + \beta^2 = 1$

(I'm cheating)

The special symbol : $| \ \rangle$ <u>ket</u>.

by mathematician / physicist Paul Dirac

$\Big[$ The other half $\langle \ |$ is <u>bra</u>

so, $\langle \ | \ \rangle$ <u>bra</u><u>cket</u> $\Big]$

Linear Algebra?

$$|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

Is it reminiscent of linear algebra?

- $\{|0\rangle, |1\rangle\}$ are basis "vectors".
  - they are "orthogonal".
  - they are "unit" vectors.
  - natural choice of notation:

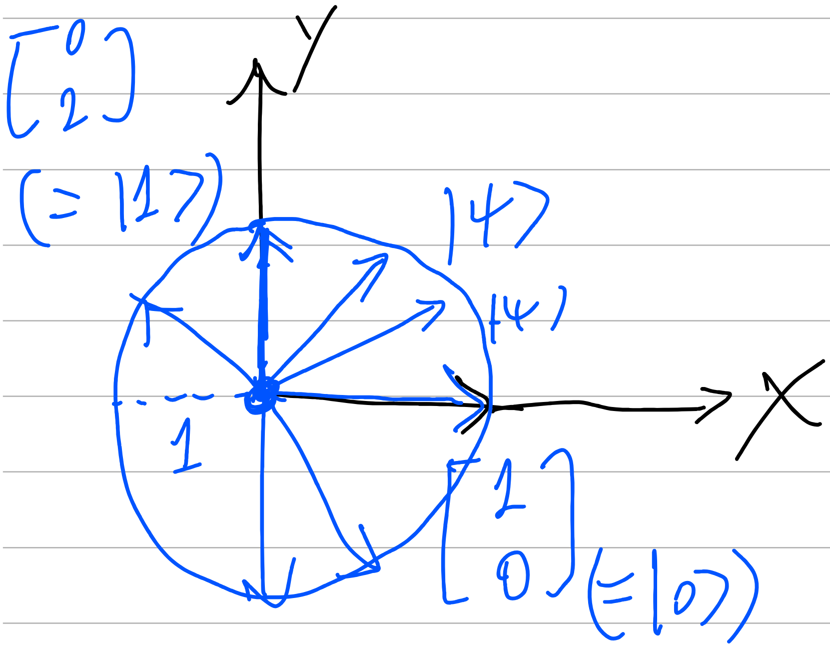
$$\boxed{|0\rangle} \ \underline{\text{rename}} \ \underset{\vec{e}_x}{\begin{bmatrix}1\\0\end{bmatrix}}, \quad \boxed{|1\rangle} \ \underline{\underline{\text{rename}}} \ \underset{\vec{e}_y}{\begin{bmatrix}0\\1\end{bmatrix}}$$

- $|\psi\rangle$ is a linear combination of basis vectors.

$$|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

$$= \alpha \begin{bmatrix}1\\0\end{bmatrix} + \beta \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

- Caveat: α, β have constraints.



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha^2 + \beta^2 = 1$$

$$|0\rangle = 1 \cdot |0\rangle + 0 \cdot |1\rangle$$

Postulate 1: A quantum register encode a "unit vector" $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$.

Measurement:

- a basic operation to qubits.
- no analog in classic computation.

Postulate 2: When we "measure" a qubit $|\psi\rangle = \alpha|0\rangle + \beta\cdot|1\rangle$, it "collapses" to $|0\rangle$ with probability α^2, and "collapses" to $|1\rangle$ with probability β^2.

Evolution (manipulating)

$$|\psi\rangle \xrightarrow{\text{physical procedure}} |\phi\rangle$$

Postulate 3: Evolution of a single qubit must be a 2X2 orthogonal matrix multipled on the left side of the qubit

I.e. $|\phi\rangle = M \cdot |\psi\rangle$, where M is a 2X2 orthogonal matrix

Orthogonal matrix: (with real numbers)

$$\underset{\mathbb{R}}{\underset{\uparrow}{M}} \cdot M^T = 1 \qquad \left(\begin{aligned} &\text{or } M^T \cdot M = 1 \\ &\text{or } \underline{M^T = M^{-1}} \end{aligned} \right)$$

Some rationale behind this choice.

- Orthogonal transforms preserve length.
  (So, being consistent with Postulate 1 and Postulate 2.)

Proof:

$$M \cdot M^T = \underline{1}$$

$$\sqrt{(M\vec{u})^T (M\cdot\vec{u})} = \sqrt{\vec{u}^T \cdot \underbrace{M^T \cdot M}_{1}\vec{u}}$$

$$\underline{= \sqrt{\vec{u}^T \cdot \vec{u}}} \leftarrow$$

$$\vec{u} = \begin{bmatrix}1\\2\\3\end{bmatrix}$$

$$\boxed{\sqrt{\vec{u}^T \cdot \vec{u}}} \qquad \sqrt{\underline{\begin{bmatrix}1 & 2 & 3\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}}}$$

$$= \sqrt{1^2+2^2+3^2}$$