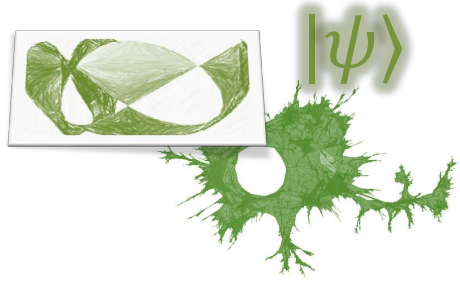
CSE 599Q: Intro to Quantum Computation



Instructor (me): James R. Lee

TAs: Haotian Jiang and Chris Kang

Course info: https://homes.cs.washington.edu/~jrl/teaching/cse599Q/

CSE 599Q: Intro to Quantum Computation

CSE 599Q: Intro to Quantum Computing

PAUL G. ALLEN SCHOOL OF COMPUTER SCIENCE & ENGINEERING

Winter 2022
MW 11:30am-12:50pm in CSE2 G04
Instructor: James R. Lee
Office hours: TBD

Teaching assistant(s):
- Chris Kang (TBD)
- Haotian Jiang (TBD)

Course email list [archives]
Class discussion: CSE 599Q Piazza
Course evaluation: 100% Homework

Reference material:
- Quantum Computer Science: An Introduction (Mermin)
- Quantum Computation and Quantum Information (Nielsen and Chuang)

Related courses:
- Quantum computing (Bacon, UW)
- Quantum computation and quantum information (O'Donnell, CMU)
  A CS theory take
- Qubits, quantum mechanics, and computers (Berkeley)
  More emphasis on the physics perspective
- Quantum computing for the determined (Nielsen, youtube)
  Basics of QC in digestable video snippets
- Quantum algorithms (Childs, UMD)
  Quantum algorithms beyond Shor and Grover
- Quantum complexity theory (Aaronson, MIT)
- Quantum information science (Harrow, MIT)
  Has quantum error-correcting codes

Course description:

An introduction to the field of quantum computing from the perspective of computer science theory.

Quantum computing leverages the revolutionary potential of computers that exploit the parallelism of the quantum mechanical laws of the universe. Topics covered include:

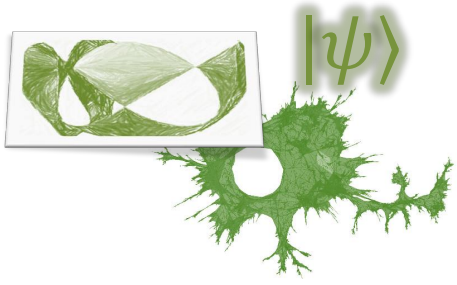
- The axioms of quantum mechanics
- Quantum cryptography (quantum money, quantum key distribution)
- Quantum algorithms (Grover search, Shor's algorithm)
- Quantum information theory (mixed states, measurements, and quantum channels)
- Quantum state tomography (learning and distinguishing quantum states)
- Quantum complexity theory
- Quantum error correction
- Quantum "supremacy"

Prerequisites: A background in undergraduate level linear algebra, probability theory, and CS theory.

Lectures

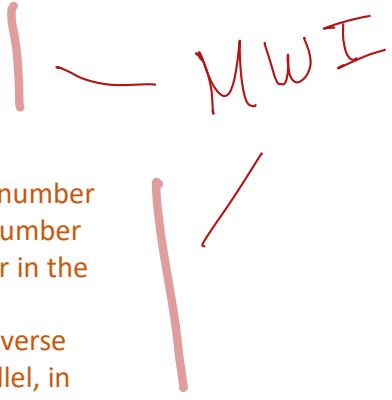
- Jan 05: Computing with parallel universes

Wed, Jan 05 **Computing with parallel universes**	Online lecture: Zoom link
Mon, Jan 10	
Wed, Jan 12	
Wed, Jan 19	
Mon, Jan 24	
Wed, Jan 26	



computing with parallel universes

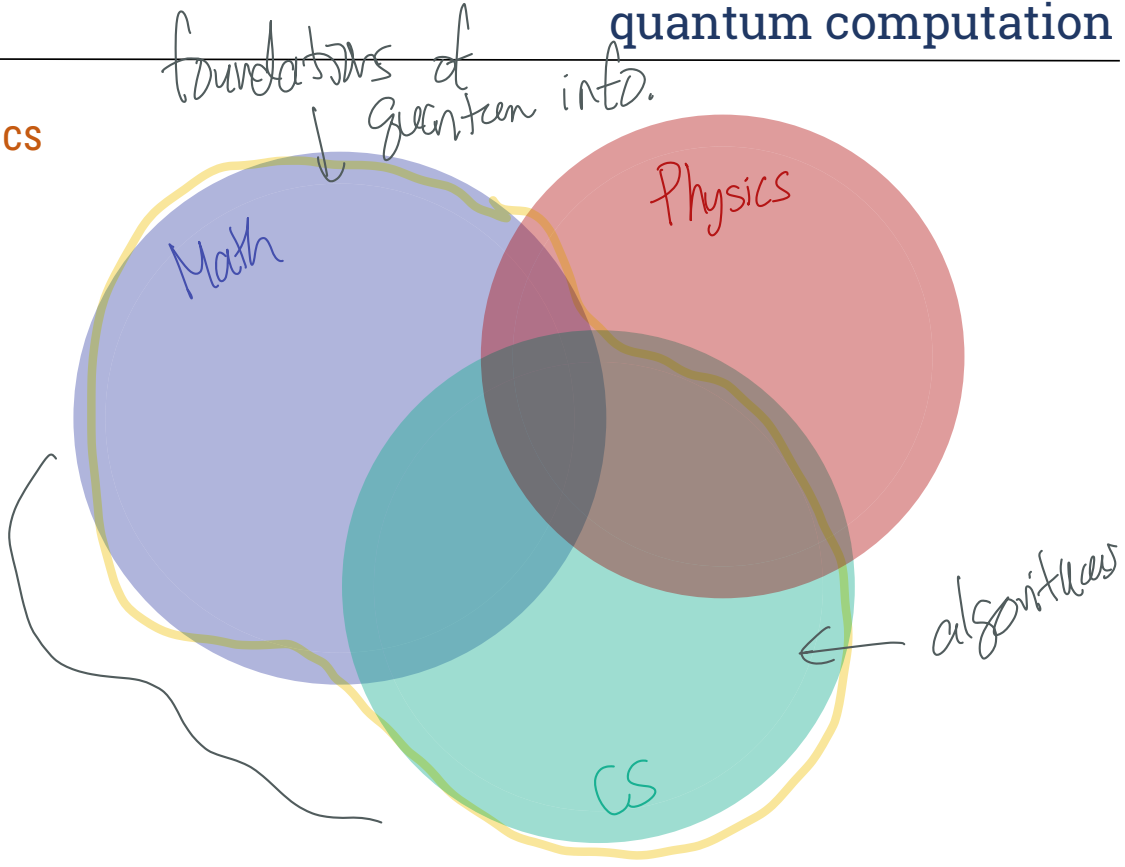
"Quantum computing is… nothing less than a distinctively new way of harnessing nature… it will be the first technology that allows useful tasks to be performed in collaboration between parallel universes."



"When a quantum factorization engine is factorizing a 250-digit number, the number of interfering universes will be of the order of 10^{500}. This staggeringly large number is the reason why Shor's algorithm makes factorization tractable. I said [earlier in the book] that the algorithm requires only a few thousand [or maybe a million] operations. I meant, of course, a few thousand parallel operations in each universe that contributes to the answer. All those computations are performed in parallel, in different universes, and share their results through interference."

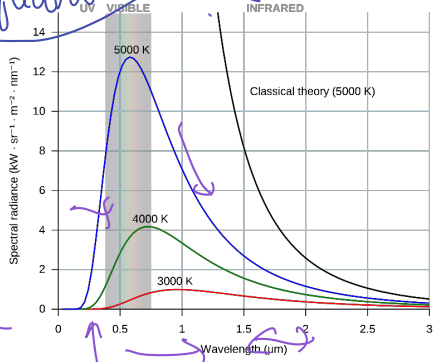
Quotes from David Deutsch (cofounder of quantum computing)

Math ∩ CS ∩ Physics



quantum mechanics arose from observations

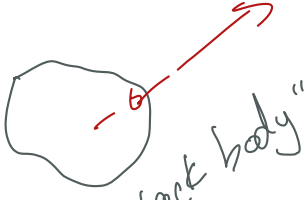
Quantum



Blackbody radiation problem

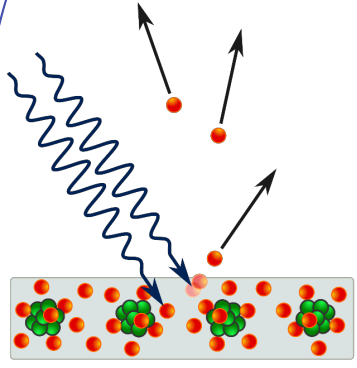
"ultraviolet catastrophe"

1/ε

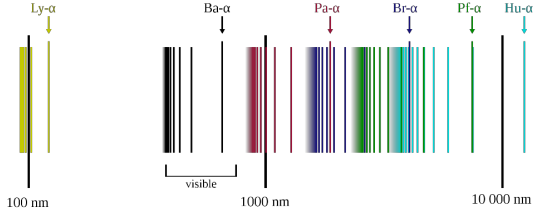


"Black body"

Photoelectric effect



Superposition



Spectral lines

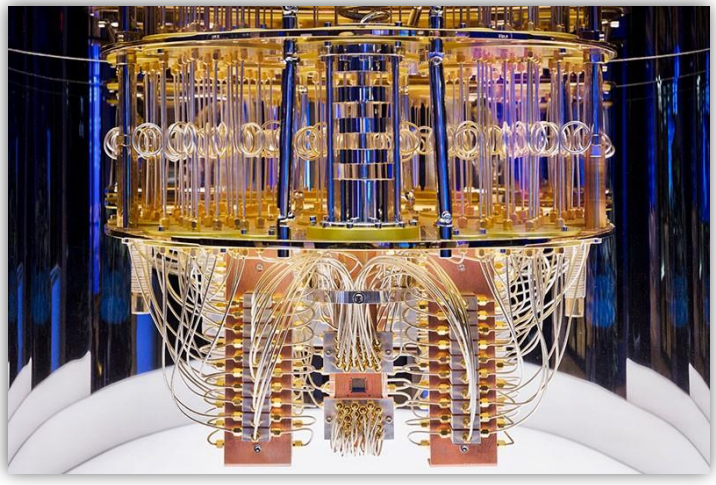
Rydberg formula

Foundations of quantum mechanics: 1900–1925

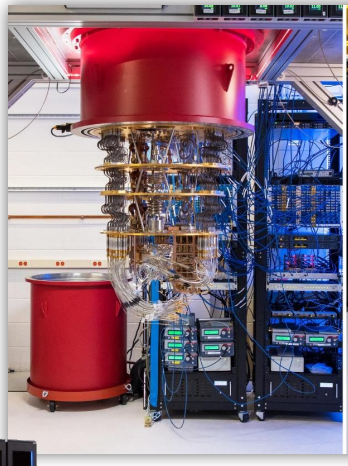
Copenhagen interp. of quantum mech

Quantum computation: 1980+

(Benioff, Feynman, Manin, Deutsch, …)



all aboard the hype train



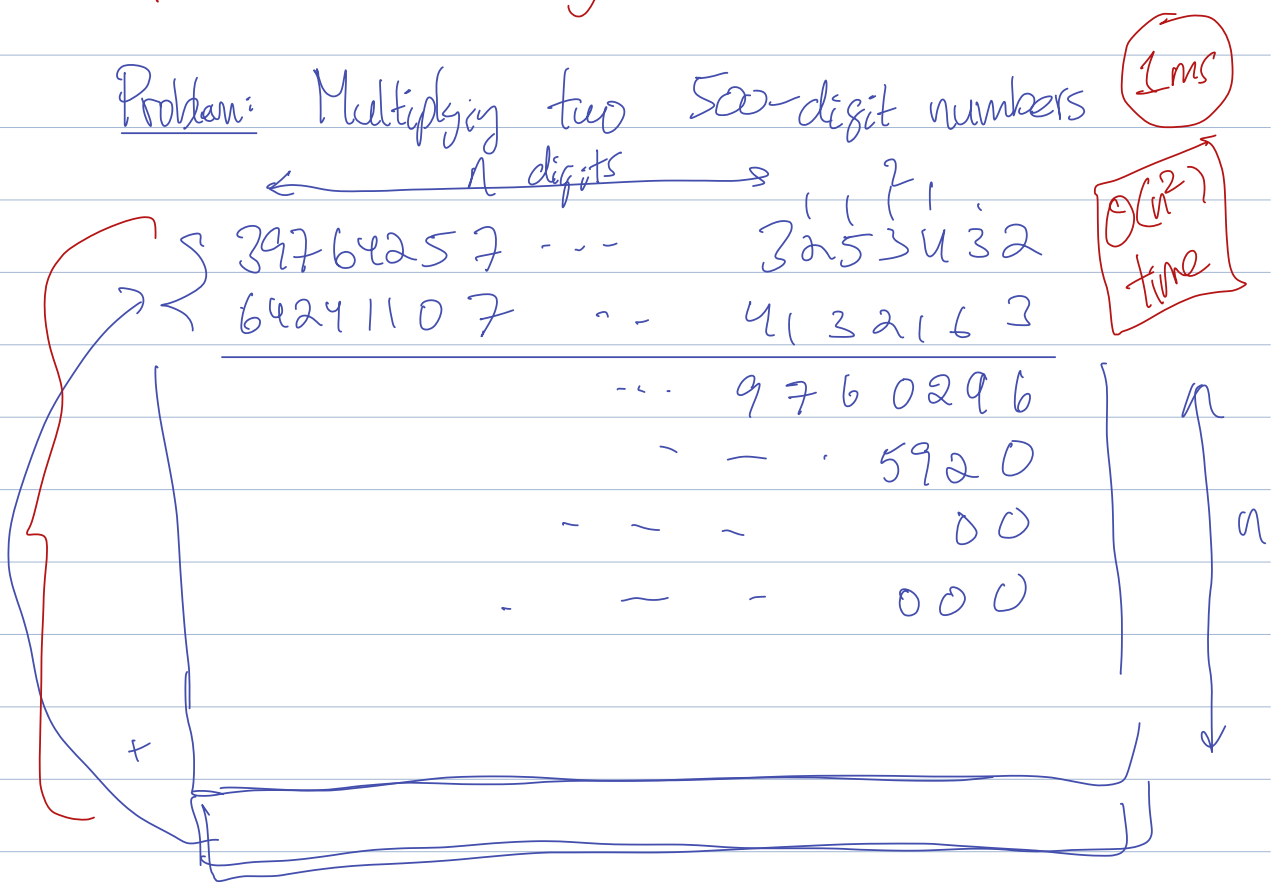
SPAC

Questions:

- Are quantum computers more powerful than classical computers?
- For what problems?
- Near-term prospects for demonstrating this? (“quantum supremacy”)

Computational efficiency

Problem: Multiplying two 500-digit numbers



FFT-based algorithm: $O(n \log n)$ time

(e.g. mult. two 1,000,000-digit #s on a PS4 in ~ 1 μs)

Problem: Primality testing ("~~Probabilistic supremacy~~")

Given an n-digit number, say whether it's prime.

→ Miller-Rabin test (Randomized)

ERH

P[alg. outputs the correct answer] ≥ $1 - 10^{-20}$

0.00000000001

PSU can check primality of a 500-digit # n < 1 μs. = 0.999999999999

{ Agrawal-Kayal-Saxena 2002:
Efficient deterministic alg. for primality testing }

Problem: Factoring n-digit numbers

Given an n-digit N, find a nontrivial factor.

$n = 500$

Does 2 divide it?
3 ...
5 ... ?
7 ... ?
⋮
$\sqrt{N}$

$\sqrt{N} \approx \sqrt{10^n} \approx \boxed{3^n}$

Pollard '96: $O(10^{6 \cdot n^{1/3}})$ time for an n-digit #

RSA-2048 ← 10^6
bits

RSA-2048
factored a 2048-digit #

RSA cryptosystem

Shor '1994: Quantum computers can factor n-digit numbers in $O(n^2)$ steps

Quantum cell phone: Solve $n = 500$ in < 1ms.

$15 = 5 \cdot 3$ ✓ (Quantum computer)