

LECTURE 1

COURSE LOGISTICS AND MOTIVATION

CS785: Theoretical Computer Science Toolkit

Sruthi Sekar

IITB



Course Objectives, Pre-requisite, Webpage

- **Course Objective:**

- Introduce you to mathematical tools that arise in theoretical computer science research.
- More breadth in topics and less depth (will follow [Ryan O'Donnell's CS Theory Toolkit course](#)).
- Train you and get you into TCS research through the course and in general talks and papers.

- **Recommendations:**

- Be active in class, take a few notes, and refer to the handwritten notes (sometimes slides) and scribes that your classmates write. I will upload references per lecture on the webpage, with the main reference being the handwritten notes uploaded (and the link above).
- All questions are important, so ask as many questions as possible in class. I will try to either answer them right away or get back to you with an answer.
- Solve the assignments (whether they are graded or not).

Pre-requisites: Basic discrete mathematics and mathematical maturity

COURSE HOMEPAGE (for references/notes/announcements/assignments): [link](#)

MOODLE: additional discussions, grades

Course Logistics

- **Grading Policy:**
 - 30% -Final Exam
 - 25% -Mid Sem Exam
 - 20% -Best 2 out of 3 quizzes (will happen in 1-hour quiz slots Wed/Fri (8:30-9:30 AM))
 - Some questions from assignments (not graded). Will have doubt-solving TA hours.
 - 15% -Chalk and talk (if the class strength permits it)
 - One presentation of 30 mins (groups of 2 (maybe more), will decide this based on class strength)
 - During lectures, some topics will be given (up for grabs on a **first come first serve** basis)
 - Presentations will be in last couple of lectures before mid-sem and before end-sem (date will be mentioned when topic announced).
Email me as soon as you decide to fix the topic!
 - 5% -Class participation (2%) + attending seminar talks and writing a short report summarizing any one talk (3 %) (talk announcements will be posted on Moodle or they can be of your choice)
 - 5 % -Scribing the lectures ([scribe template](#)):
 - Decide and let me know at the beginning of each lecture about who wants to scribe it (meaning type out detailed notes of the lecture, with all missing proofs and exercises discussed in class)
 - Each lecture will be scribed by two people separately. Each person has to scribe at least one lecture in the course. If you scribe more, I will grade the best one.

Syllabus

MODULE 1 Asymptotics and Probability

Some probability basics,
concentration
inequalities, basic
asymptotics, etc..

MODULE 2 Fourier Transforms

Properties of discrete
fourier transforms,
integer multiplication,
analysis of boolean
functions, etc..

MODULE 3 Algebra and Applications

Number theory, Fields
and polynomials,
Schwartz-Zippel Lemma,
Error correcting Codes,
other applications..

MODULE 4 Linear Algebra and Graphs

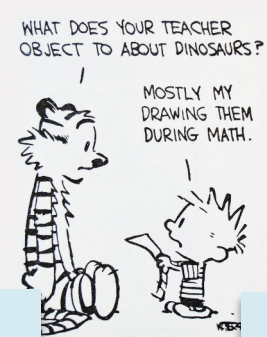
Some linear algebra
basics, eigenvalues,
eigenvectors, expanders,
random walks, etc..

MODULE 5 Information Theory and Pseudorandomness

Basics of communication
complexity, entropy,
mutual information,
information complexity,...

MODULE 6 Hardness

Lattices, Average case vs
worst case hardness, PCP
theorem, alternative
assumptions in
Cryptography



Use linear algebra to find
the identity of superman.

Let $A =$ 
superman

Then $AA^{-1} =$ 
clark kent



Contact Hours and TAs

- **Meet me after class**, or **email me** to set up an appointment (sruthi@cse.iitb.ac.in).
- **Teaching Assistant:** Nilabha Saha (210260037@iitb.ac.in), Krishna N Agaram (210051003@iitb.ac.in)
(There will be TA hours for clearing doubts. Discuss on Moodle)
- **Temporary Class Rep:** the goal is to find a TA discussion time for assignment solving.
(form a group, add Nilabha to it, and figure out a slot to meet weekly).
Mail me the TA hour by Monday, 13th January at the latest! Volunteer(s)?

TCS Philosophy

- It is a cool area where you see many abstract concepts in math actually being used. You can choose anything to work on, from algorithms of different kinds, quantum computing, cryptography, complexity theory, game theory, etc. Anything you pick, you will apply various math tools!

“I work in theoretical computer science: a field that doesn’t itself win Fields Medals (at least not yet), but that has occasions **to use parts of math that have won Fields Medals**. Yes, there’s plenty of math that strikes even me as boutique scholasticism: a way to signal the brilliance of the people doing it, by solving problems that require years just to understand their statements, and whose “motivations” are about 5,000 steps removed from anything Caplan or Bostrom would recognize as motivation. But where I part ways is that there’s also math that looked to me like boutique scholasticism, until Greg Kuperberg or Ketan Mulmuley or someone else finally managed to explain it to me, and I said: “ah, so that’s why Mumford or Connes or Witten cared so much about this. **It seems ... almost like an ordinary applied engineering question, albeit one from the year 2130 or something, being impatiently studied by people a few moves ahead of everyone else in humanity’s chess game against reality.** It will be pretty sweet once the rest of the world catches up to this.”

--Scott Aaronson

- You often make gradual progress in TCS research, and you learn more and more as you make mistakes.
- Keep reading, writing, working out the math, watching online talks, and attending in-person seminars.

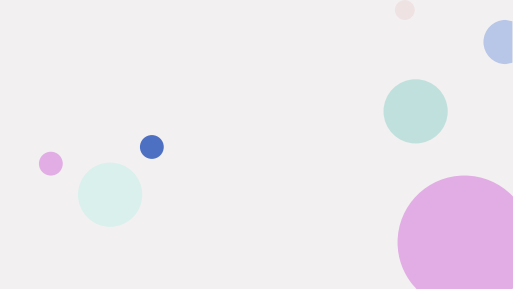
A good source of videos and talks: [Simons Berkeley](#)

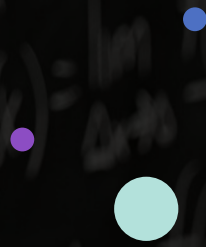
Conceptual understanding in an innovative way: [3Blue1Brown](#)



INTRODUCE YOURSELF

(Fair warning: I am bad with names, so will slowly know them through the course.)

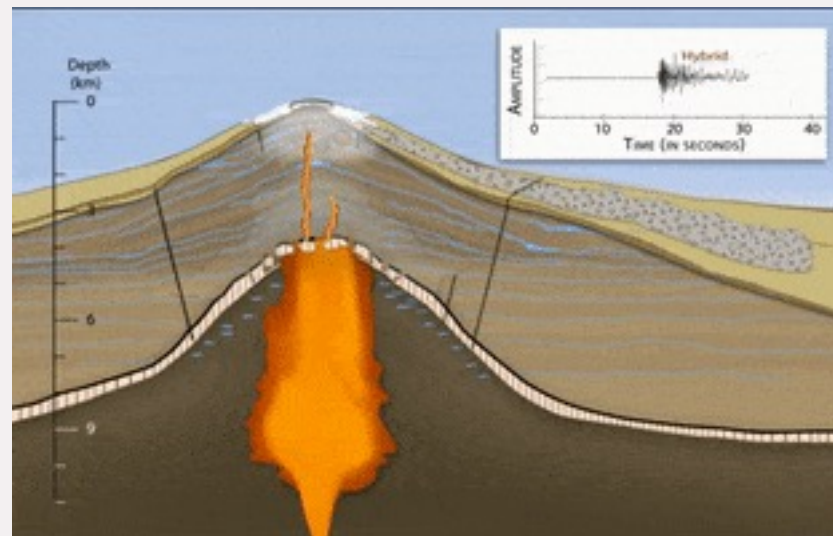
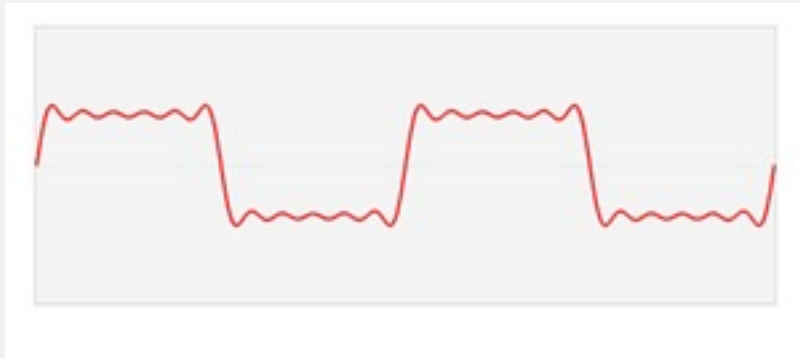
- Your name and what degree you are pursuing?
 - Why you decided to take this course and what you expect?
- 

- 
- 
- 
- Some interesting applications of the Math we will learn through the course..

Fast Fourier Transform

History of how FFT was discovered: FFT was discovered by scientists trying to detect covert nuclear weapons tests, and if they had done it sooner, it may have put a stop to the nuclear arms race.

To detect, they used seismometer, and scientists wanted a method to reliably determine whether a given signal was a bomb or an earthquake and if it was a bomb, then how big it was, and how deep it was buried. To do this, they needed to know how much which frequency was present, which required them to take a fourier transform!

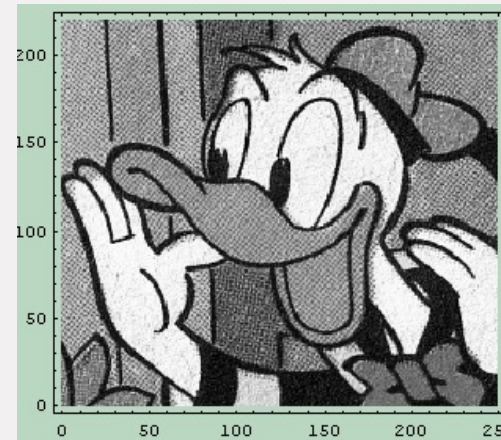
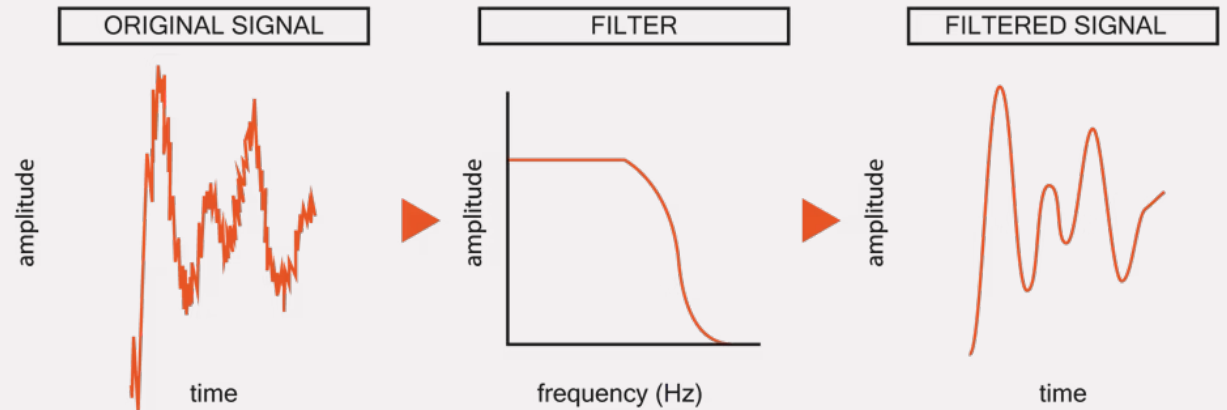


Discrete Fourier Transform: Applications

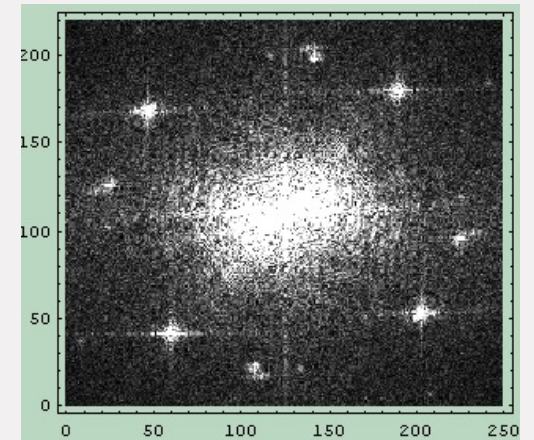
Audio Processing: Discrete Fourier Transforms (DFTs) are used to analyze sound signals, enabling applications like noise reduction, audio compression (e.g., MP3), and audio effects.

Image Processing: DFTs also help in image analysis and compression. It helps in transforming the image to the frequency domain for filtering and enhancement.

Many other applications of DFTs: telecommunications, medical imaging, seismology, economics and finance, machine learning, cryptography, etc..



Donald Duck



DFT of Donald Duck

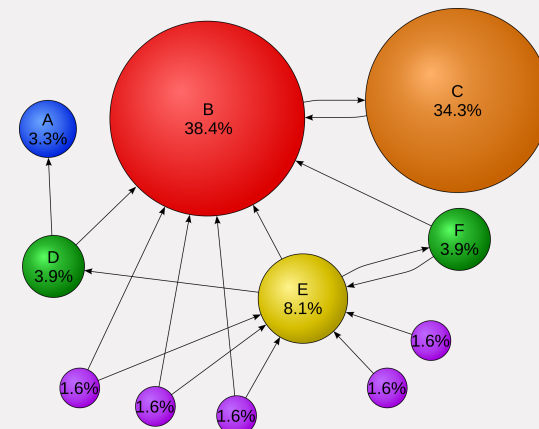
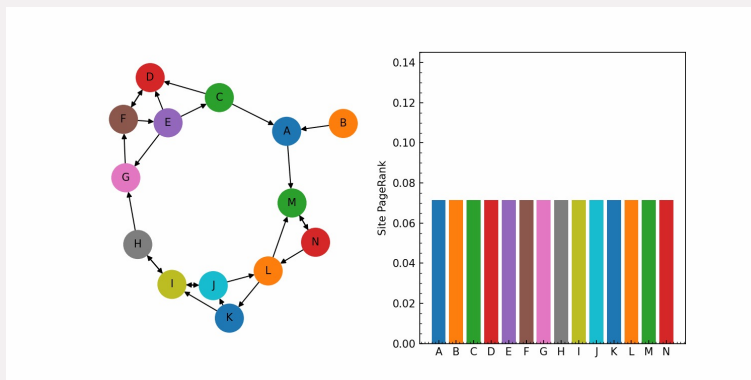
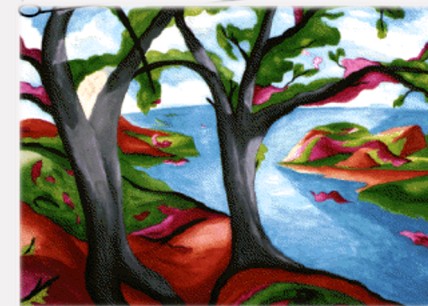
Linear Algebra and Graphs: Applications

Image/Video Editing: Performing rotation, scaling, translation, compression, etc are all matrix operations. Compression uses singular value decompositions.

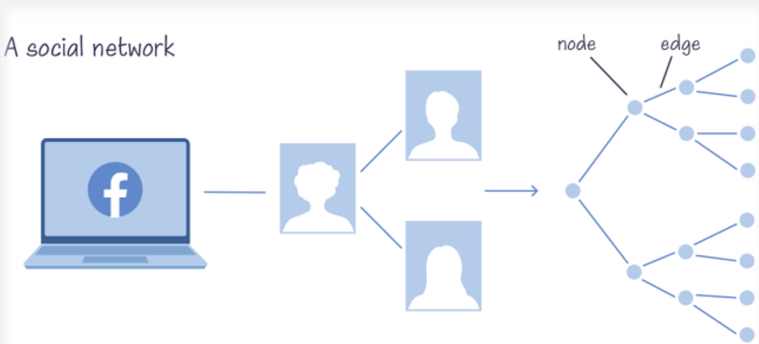
Network Analysis: Graphs and linear algebra used in analyzing networks, including social networks, transportation networks, neural networks, and communication networks (through adjacency matrices and eigenvalues).

Page Rank Algorithm: The ranking of pages when you search on google uses this algorithm. It uses Markov chains (probability), eigenvalues, eigenvectors (very interesting and simple algorithm)!

0.2235	0.1294	Blue	0.4196	0.2235
0.5804	0.2902	0.0627	0.2902	0.2902
0.5804	0.0627	0.0627	0.0627	0.2235
0.5176	0.1922	0.0627	Green	0.1922
0.5176	0.1294	0.1608	0.1294	0.2588
0.5176	0.1608	0.0627	0.1608	0.1922
0.5490	0.2235	0.5490	Red	0.7412
0.3882	0.5176	0.5804	0.5804	0.7765
0.2588	0.2902	0.2588	0.2235	0.4824
0.2235	0.1608	0.2588	0.2588	0.1608
0.1608	0.2588	0.2588	0.2588	0.2588



A social network

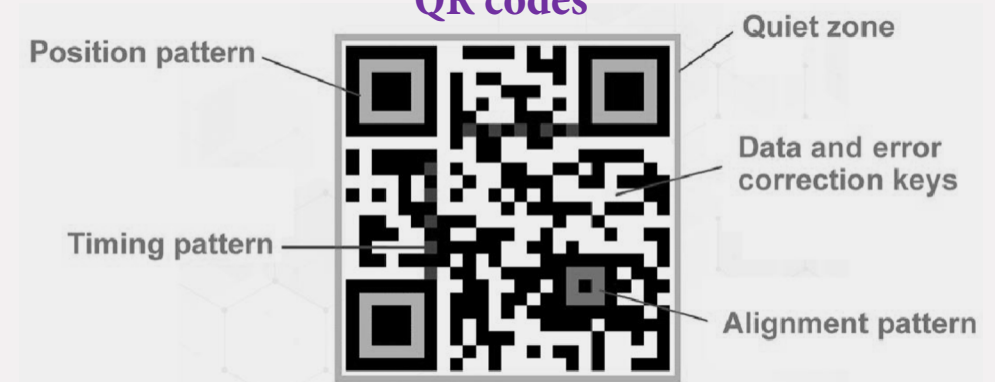


Algebra and Coding Theory: Applications

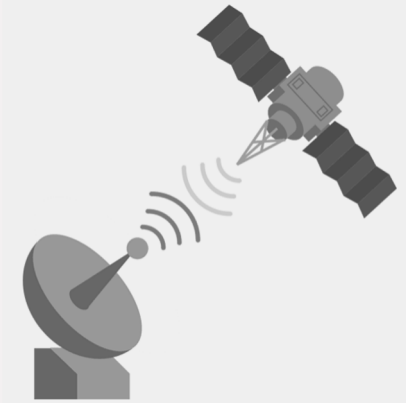
Storage Devices: CDs, DVDs, Blu-rays



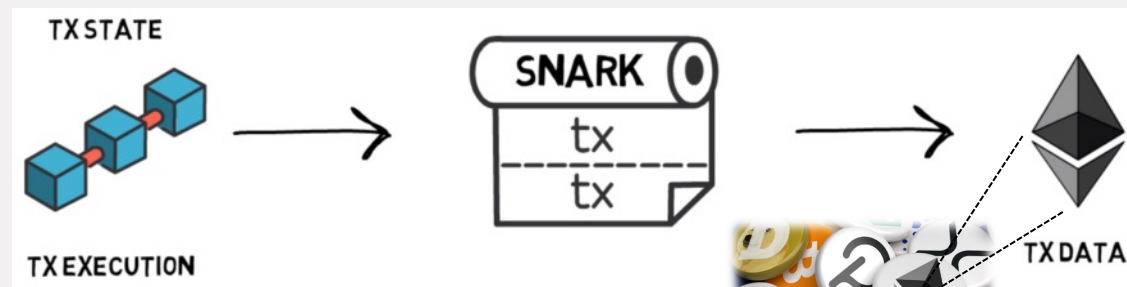
QR codes



Reed-Solomon Encoding: uses polynomial algebra, and FFT for decoding



Satellite communications
and Digital television



Blockchains and Cryptocurrencies
(uses Hardness, Polynomial encodings,
Expanders, and in general Algebra)

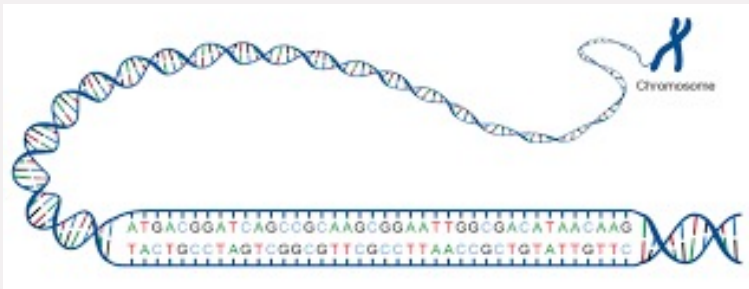


High-speed Modems

Algebra, Number theory, Hardness: Applications

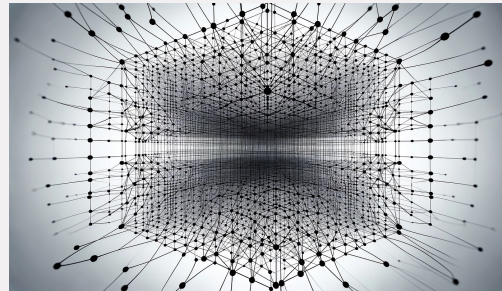


Phylogenetics: algebraic methods help model evolutionary relationships

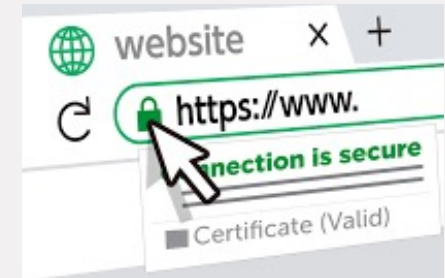


Reconstruct DNA sequences (uses algebraic graph theory)

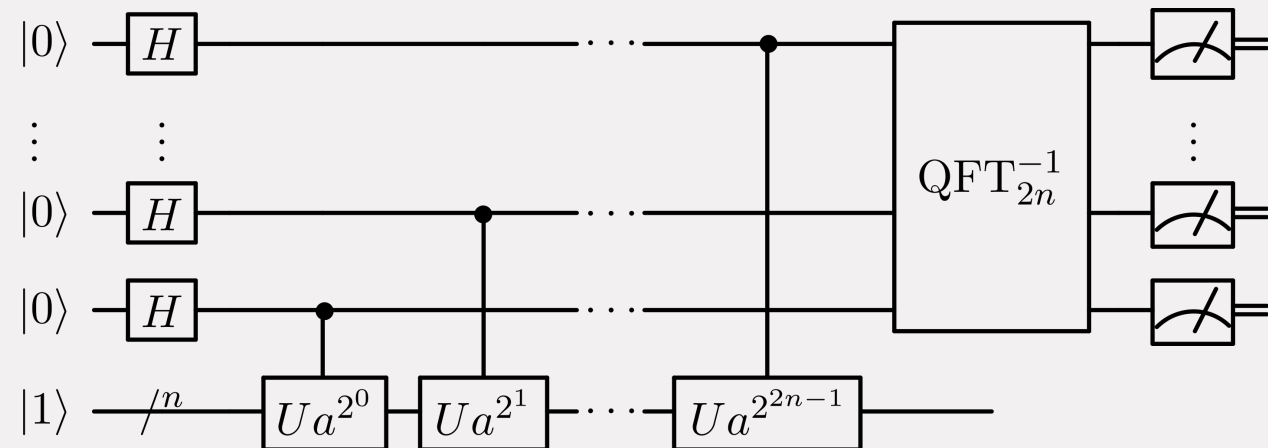
Post-quantum cryptography uses lattices



5G: uses Polar codes and LDPC codes



Cryptography: SSL/TLS (uses Hardness and Algebra)



Shor's Algorithm (Quantum): uses number theory, algebra and Quantum Fourier Transform

Coupon Collector Problem



Suppose there are n different kinds of coupons (say pokemons) and we want to collect at least one coupon (pokemon) of each kind. We start with nothing, and at each step, we get a new random coupon, equally likely to be any of the n kinds, and independent of the previous coupons.

Question: What is the expected time T when we're done collecting?
Can you bound the probability that T deviates from this expected value?

DISCUSS



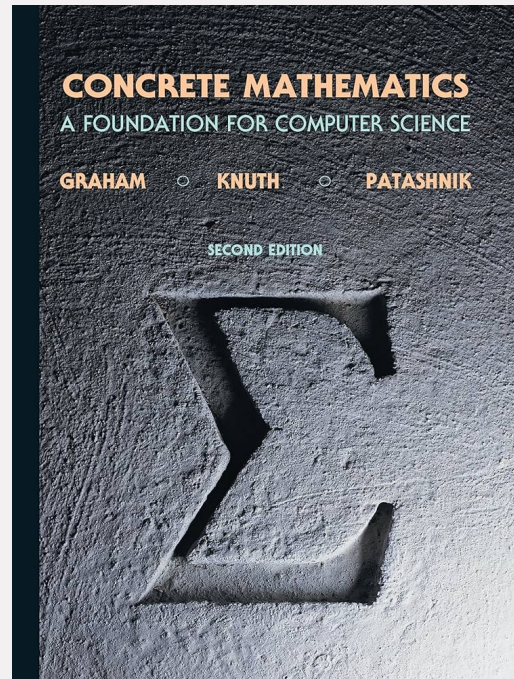
To Do's for you all

- **Brush-up basic probability:** sample space, probability distribution, random variable, basic conditional probability, Bayes' rule, law of total probability, union bound, expectation and variance. I can define some of the terms in class, as we progress through, if someone asks me for these basic definitions. Here is a [link](#) of my slides from CS409 for your quick reference to these definitions. **HW0 will be sent soon.**
- Take a look at the scribe template that you need to use along with LaTeX primers (links for your use on the webpage). If you have never used LaTeX, you should start learning to do so.
- Watch out for some interesting talks that are happening this month. I will post interesting talk announcements on Moodle. Starting getting into the habit of attending talks. It's a great way to learn and start thinking about research.
- Volunteer for CR? Tell me a TA hour slot that works for everyone, including Nilabha, by Monday the 13th.

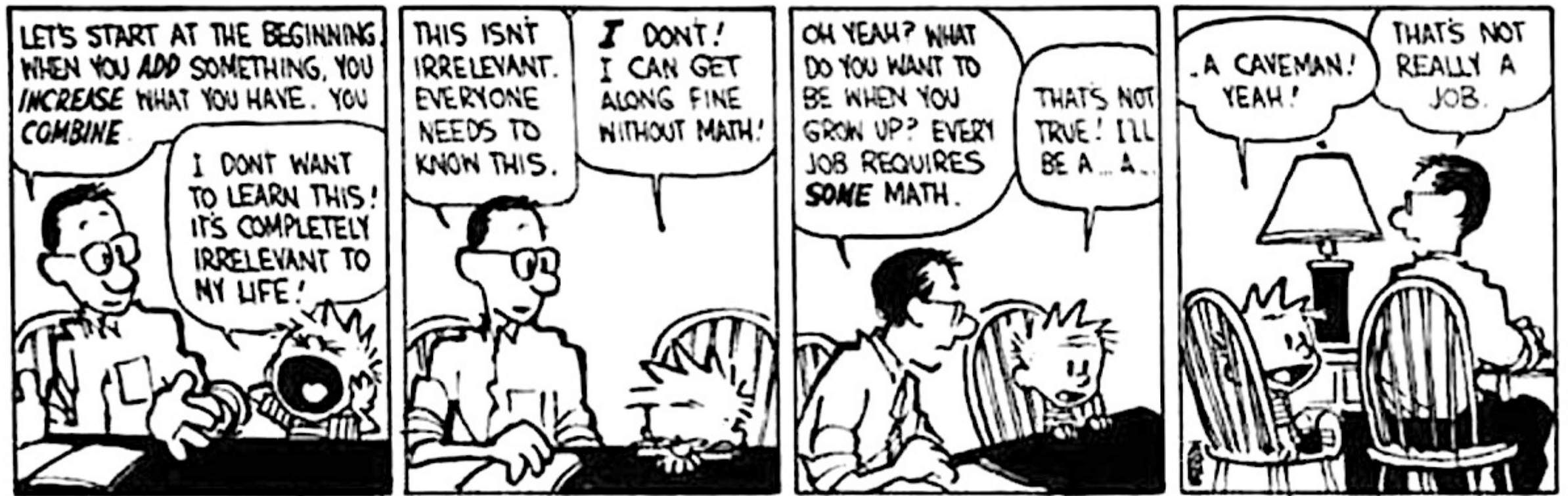
Next Class

- Introducing Asymptotic notations to you
- Some important approximations that you often use
- Some example applications

You can also refer to this book to brush up probability basics!



Will refer to
this book



THANK YOU

Questions?