Lecture 00: Introduction Mathematical Toolkit in CS CS–59000–MTK

Course Content

- Introduce Foundational Topics in Mathematics and Computer Science
  - Mathematical tools and techniques useful in computer science
  - Gems of Mathematics and Computer Science
  - Glimpse of relevant big Open Problems

About Me

- Hi! I am Hemanta K. Maji and I am a Theoretical Cryptographer

Learning Goals

- Understand Intuition
- Learn to Conjecture
- Create Atomic Conceptual Building Blocks
  - Intuitively Reason about *your* Research Problems
  - Formulate *your* Research Problems in these terminologies
- Lot of Supplementary Materials (links to lecture notes and videos)

Grading

- 75% Homeworks
  - Collaborations are Encouraged
  - All resources must be cited
  - Homework needs to be LaTeX-ed
- 20% Midterm in the class
- 5% Class Participation

Logistics

- Lectures: Tuesday and Thursday, 4:30 p.m. to 5:45 p.m. at LWSN B134
- Office Hours: Appointment by Email
- Office: LWSN 1177

Similar Courses

- "Toolkit Courses" and "Gems in CS Courses"
- Representative Examples
  - MIT: Topics in theoretical computer science: An algorithmist's toolkit
  - Princeton: Advanced topics in computer science: A theorist's toolkit
  - CMU: A theorist's toolkit
  - TTI: Mathematical toolkit
  - IAS: Algebraic Gems of Theoretical Computer Science
  - North Eastern: Gems of Theoretical Computer Science
  - EPFL: Theory Gems

Tentative Topics (1)

- Crash Course in Counting and Probability: Generating Functions, Ball and Bins problems, Power of two choices Problem

Tentative Topics (1)

- Crash Course in Counting and Probability: Generating Functions, Ball and Bins problems, Power of two choices Problem
- Probabilistic Proofs: Lovász Local Lemma and its Algorithmic versions (Moser-Tardos and others)

Tentative Topics (1)

- Crash Course in Counting and Probability: Generating Functions, Ball and Bins problems, Power of two choices Problem
- Probabilistic Proofs: Lovász Local Lemma and its Algorithmic versions (Moser-Tardos and others)
- Concentration Bounds: Markov Inequality, Chebyshev Inequality, Chernoff Bounds, Bounds for Hypergeometric distributions, t-wise Independent Variables, Azuma's Inequality, Talagrand Inequality, Tightness of Chernoff, Anti-concentration Inequalities (Littlewood-Offord)

Tentative Topics (1)

- Crash Course in Counting and Probability: Generating Functions, Ball and Bins problems, Power of two choices Problem
- Probabilistic Proofs: Lovász Local Lemma and its Algorithmic versions (Moser-Tardos and others)
- Concentration Bounds: Markov Inequality, Chebyshev Inequality, Chernoff Bounds, Bounds for Hypergeometric distributions, t-wise Independent Variables, Azuma's Inequality, Talagrand Inequality, Tightness of Chernoff, Anti-concentration Inequalities (Littlewood-Offord)
- Spectral Graph Theory: Expanders, Random walk on Expanders (Gillman), Zig-zag Products, SL = L Result

Tentative Topics (2)

- "Vector Space"-esque Objects: Lattices, Linear Error-correcting Codes and their properties

Tentative Topics (2)

- "Vector Space"-esque Objects: Lattices, Linear Error-correcting Codes and their properties
- Information Theory: Entropy, Mutual Information, Fano's Inequality, Channel Capacity, Shannon's Capacity Theorem and its converse

Tentative Topics (2)

- "Vector Space"-esque Objects: Lattices, Linear Error-correcting Codes and their properties
- Information Theory: Entropy, Mutual Information, Fano's Inequality, Channel Capacity, Shannon's Capacity Theorem and its converse
- Fourier Analysis on boolean hypercube: BLR Linearity Testing, Convolution, Left-over Hash Lemma, Min-entropy Extraction by eps-biased masking, XOR-lemma, Hypercontractivity, Kahn-Kalai-Linial Theorem, Goldreich-Levin Hardcore-predicate, PCPs

Concluding Remarks

- What I expect of you: Knowledge of "Algorithms"-equivalent course, some Mathematical Maturity and Class Participation
- We will collaboratively learn from each other