The most important questions of life are, for the most part, really only problems of probability. Strictly speaking one may even say that nearly all our knowledge is problematical; and in the small number of things which we are able to know with certainty, even in the mathematical sciences themselves, induction and analogy, the principal means for discovering truth, are based on probabilities, so that the entire system of human knowledge is connected with this theory.

Pierre-Simon Laplace. Introduction to Theorie Analytique des Probabilities. Oeuvres, t. 7. Paris, 1886, p. 5.

0.1 Preliminary Syllabus

Class time: MWF10:00-11:00 in Annenberg 314.

Office hours will normally be in my office, Annenberg 317. Just email to schedule an appointment. I'll soon schedule a regular weekly hour but even then, write if you want to meet at another time, and I'll do my best.

TA: Jenish Mehta, jenishc@gmail.com. Office Hours TBA

There will be problem sets, normally due on Fridays; there will not be an exam. You may collaborate with other students on the sets; just make a note of that. This is assuming it's a collaboration and doesn't regularly become one-way; if you feel that happening, (a) focus on doing a decent fraction of the problems on your own or with consultation with me or the TA, (b) don't collaborate until after you've already spent some time thinking about the problem yourself.

Lecture notes will be handed out after the fact. A full set from two years ago has been posted.

There will be no class on Monday Oct. 1; the first day of classes will be Oct. 3.

This syllabus is rough in its estimates of the time we'll spend on each topic.

$\sim$ 1 week: Discrete probability: examples and basics. The probabilistic method and combinatorial applications. Randomized algorithms, derandomization by conditional expectations.

$\sim$ 2 weeks: "Fingerprinting", polynomial identity testing. Applications: file comparison, verifying matrix multiplication, verifying associativity. Perfect matchings (decision and search versions).

$\sim$ 3 weeks: Concentration of measure for fully or partially independent rvs. Fully and pairwise independent rvs. Chor-Goldreich error amplification. CLT, Large deviation bound (Chernoff / Bernstein), Chebychev bound. MIS and derandomization. Shannon coding theorem. Concentration of the number of prime factors of a random number. Set discrepancy. Gale-Berlekamp (unbalancing lights): upper and lower bounds. Expander graphs. Johnson-Lindenstrauss metric embedding. k-wise independence and error-correcting codes. 4-wise independence and metric embedding. Bourgain metric embedding?

$\sim$ 2 weeks: Lovasz Local Lemma. Applications: Ramsey numbers, van der Waerden. Moser-Tardos algorithm.

$\sim$ 2 weeks: Randomized vs. Distributional Complexity. Game tree evaluation: upper and lower bounds. Karger's min-cut algorithm.

$\sim$ Desirable but unlikely to be reached during the quarter: Hashing, AKS dictionary hashing, cuckoo hashing. Talagrand concentration inequality. Linial-Saks graph partitioning. A. Kalai's sampling random factored numbers. Feige leader election. Approximation of the permanent and self-reducibility. Equivalence of approximate counting and approximate sampling. ε-biased k-wise independent spaces. #DNF-approximation. Shamir secret sharing. An interactive proof for a problem only known to be in coNP: graph non-isomorphism. Searching for the first spot where two sequences disagree. Weighted sampling (e.g., Karger network reliability). Markov Chain Monte Carlo.

Notes. (1) This course can be only an exposure to probability and its role in the theory of algorithms. We will stay focused on key ideas and examples; we will not be overconcerned with best bounds. (2) I assume this is not your first exposure to probability. Likewise I'll assume you have some familiarity with algorithms. However, the first lecture will start out with some basic examples and definitions.

Books. There will be no assigned book, but I recommend the following references:

On reserve at SFL:

- Mitzenmacher & Upfal, Probability and Computing, Cambridge 2005
- Motwani & Raghavan, Randomized Algorithms, Cambridge 1995
- Williams, Probability with Martingales, Cambridge 1991
- Alon & Spencer, The Probabilistic Method, 3rd ed., Wiley 2008

Not on reserve:

- Adams & Guillemin, Measure Theory and Probability, Birkhäuser 1996
- Billingsley, Probability and Measure, 3rd ed., Wiley 1995