LECTURE 1
Randomness in Computing

- Course information
- Verifying polynomial identities (on the blackboard)
- Probability Amplification (on the blackboard)
- Probability Review

Sofya Raskhodnikova
Course information

1. Course staff
2. Course website(s)
3. Piazza bonus
4. Prerequisites
5. Textbook(s)
6. Syllabus
7. Homework logistics
8. Collaboration policy
9. Exams and grading
Tips for the course

• Concepts in this course take some time to sink in: be careful not to fall behind.
• Do the assigned reading on each topic before the corresponding lecture.
• Attend the lectures: most of the material in lectures will be presented on the blackboard (and some of it is not in the book).
• Take advantage of office hours.
• Be active in lectures and on piazza.
• Allocate lots of time for the course: comparable to a project course, but spread more evenly.
Tips for the course: HW

• Start working on HW early.
• Spread your HW time over multiple days.
• You can work in groups (up to 4 people), but spend 1-2 hours thinking about it on your own before your group meeting.
Tips: learning problem solving

To learn problem solving, you have to do it:

• Try to think how you would solve any presented problem before you read/hear the answer.
• Do exercises in addition to HW.
Tips: how to read a math text

• Not like reading a mystery novel.
• The goal is not to get the answers, but to learn the techniques.
• Always try to foresee what is coming next.
• Always think how you would approach a problem before reading the solution.
• This applies to things that are not explicitly labeled as problems.
Skills we will work on

• Mathematical reasoning
• Expressing your ideas
  – abstractly (suppress inessential details)
  – precisely (rigorously)
• Probabilistic thinking
• Algorithmic thinking
• Problem solving
• Having **FUN** with all of the above!!!
Could they ask me questions about CS 537 material on job interviews?

- You bet.
Uses of Randomness in Computing

• To speed up algorithms.

• To enable new applications:
  – Symmetry breaking in distributed algorithms, cryptography, privacy, online games and gambling.

• To simulate real world events in physical systems: model them as happening randomly.

• To analyze algorithms when data is generated from some distribution:
  – learning theory, data compression.

• To analyze algorithms when errors happen randomly
  – error-correcting codes.

• Analyzing statistics from sampling.
Probability space has three components

- Sample space $\Omega$
- Family of allowable events $E \subseteq \Omega$
- A probability function $\Pr$ that maps events $E$ to $\mathbb{R}$ such that
  - $\Pr(E) \in [0,1]$ for any event $E$;
  - $\Pr(\Omega) = 1$;
  - For any finite or countable sequence of pairwise disjoint events $E_1, E_2, \ldots$, $E = \bigcup_{i \geq 1} E_i$,
    
    $\Pr\left( \bigcup_{i \geq 1} E_i \right) = \sum_{i \geq 1} \Pr(E_i)$.  

Sofya Raskhodnikova; Randomness in Computing
Review: Inclusion-Exclusion Principle

For any two events $E_1$ and $E_2,$

$$\Pr(E_1 \cup E_2) = \Pr(E_1) + \Pr(E_2) - \Pr(E_1 \cap E_2).$$

For any three events $E_1$, $E_2$ and $E_3$,

$$\Pr(E_1 \cup E_2 \cup E_3) = \Pr(E_1) + \Pr(E_2) + \Pr(E_3)$$
$$- \Pr(E_1 \cap E_2) - \Pr(E_1 \cap E_3) - \Pr(E_2 \cap E_3)$$
$$+ \Pr(E_1 \cap E_2 \cap E_3)$$

For any $n$ events $E_1, E_2, \ldots, E_n$,

$$\Pr\left(\bigcup_{i \in [n]} E_i\right) = \sum_{i \in [n]} \Pr(E_i) - \sum_{i < j} \Pr(E_i \cap E_j)$$
$$+ \sum_{i < j < k} \Pr(E_i \cap E_j \cup E_k) - \cdots + (-1)^{n+1} \Pr\left(\bigcap_{i \in [n]} E_i\right).$$
Union Bound

For finite or countable sequence of events $E_1, E_2, \ldots,$

$$\Pr\left( \bigcup_{i \geq 1} E_i \right) \leq \sum_{i \geq 1} \Pr(E_i).$$
Independent events

- Two events $E_1$ and $E_2$ are independent if
  \[ \Pr(E_1 \cap E_2) = \Pr(E_1) \cdot \Pr(E_2). \]
- Events $E_1, \ldots, E_k$ are mutually independent if, for every subset $I \subseteq [k],$
  \[ \Pr\left(\bigcap_{i \in I} E_i\right) = \prod_{i \in I} \Pr(E_i). \]
Conditional Probability

The conditional probability of event $E$ given event $F$ is

$$\Pr(E \mid F) = \frac{\Pr(E \cap F)}{\Pr(F)}.$$ 

- When $E$ and $F$ are independent,

$$\Pr(E \mid F) = \frac{\Pr(E \cap F)}{\Pr(F)} = \frac{\Pr(E) \cdot \Pr(F)}{\Pr(F)} = \Pr(E).$$