COS 522: Complexity Theory : Boaz Barak

Handout 1 : Administrative details, introduction, Turing machines and Boolean circuits.

Reading: Chapters 1, 6.1

Administration My email is **boaz(at)cs.princeton.edu** — please do not hesitate to contact me for any question or to schedule a meeting (in fact, it's mandatory — see below).

If you're taking the course for credit your responsibilities are: **(1)** submit all homework assignments the next class after they are given - there are no optional assignments but most will have bonus questions to make up for those you could not or did not have time to solve, **(2)** grade two assignments - a schedule of whose grading when will be on the web and **(3)** submit the take home final exam.

Textbook The textbook for the course is "Computational Complexity: A modern Approach" by Sanjeev Arora and myself. It is available as a course packet from the university store (it's also available on the web but please do not print it on the department's printers).

Background The main background I assume is mathematical maturity: ability to read, write and even enjoy (!) mathematical proofs. Other than that, we will use some basic concepts from discrete mathematics, especially **elementary finite probability** (random variables, expectation, independence, Chernoff bounds, etc..). Some lectures will also use basic notions from **linear algebra** (linear spaces, dimension, basis, eigenvalues, etc..). If you feel you need more background in this area take a look at lecture notes for UC Berkeley discrete math courses by **Umesh Vazirani** (joint with Papadimitriou) and by **Luca Trevisan** available through their homepages. You can also contact me for a more personalized reading list. You might also find the textbook's appendix useful.

I do not explicitly assume background in **algorithms** (O notations, basic data structures etc..) and **computability theory** (Turing machines, NP and NP completeness), but we will go through this material fairly rapidly. If you have not taken an algorithms and theory of computation course, you might should carefully read Chapters 1 and 2 of the textbook, and ask me if there are any questions.

Introduction What is complexity theory, what are its goals - why it's the coolest field ever.

Turing machines Our main model of computation, some basic features.

Machines as strings Representing TM's by strings and the universal Turing machine.

The class P Our formalization of "efficiently computable decision problems"

Boolean circuits The class $\mathbf{P_{/poly}}$, $\mathbf{P} \subseteq \mathbf{P_{/poly}}$.

Hard functions Existence of $f \notin \mathbf{P_{/poly}}$, probabilistic method.

Notes:

- Please write proofs *clearly* but *succinctly* without any logical gaps or superfluous complications or formalities. I prefer that, if possible, you type up your solutions using LaTeX . To make this easier, I will post the LaTeX source file of all handouts on the web.
- In all exercises below, random variables are over a *finite sample space* - that is a finite set Ω where we associate with any $\omega \in \Omega$ a number p_ω (the probability that ω is chosen) in $[0,1]$ such that $\sum_{\omega\in\Omega} p_\omega = 1$. If it makes your life easier, in all the exercises below you may assume that the distribution is the *uniform distribution* over the sample space: that is $p_\omega = 1/|\Omega|$ for every $\omega \in \Omega$.

  Recall that an *event* A over the space Ω is a subset of Ω, where $\Pr[A] = \sum_{\omega\in A} p_\omega$. A *random variable* X over the space is a function that maps Ω to the real numbers $\mathbb{R}$, where $\mathsf{E}[X] = \sum_{\omega\in\Omega} X(\omega)p_\omega$. We say that two events A,B are *independent* if $\Pr[A \cap B] = \Pr[A]\Pr[B]$, and that two random variables X, Y are independent if for every $x, y \in \mathbb{R}$, the events "$X = x$" and "$Y = y$" are independent.

Homework Assignments

§1 (10 points) Please send me an email by **next Monday, Feburary 12th** to say the times you are available for a 10-15 minute meeting on Tuesday or Thursday of next week.

§2 (30 points) Prove that if two random variables X, Y are independent then

$$\mathsf{E}[XY] = \mathsf{E}[X]\mathsf{E}[Y].$$

§3 (30 points) If $A_1, \ldots, A_m$ are events over a sample space Ω then

$$\Pr[\cup_{i\in[m]} A_i] \geq \sum_{i\in[m]} \Pr[A_i] - \sum_{i<j\in[m]} \Pr[A_i \cap A_j].$$

§4 (30 points) We say that a function $f : \mathbb{R} \to \mathbb{R}$ is *convex* if for every $x, y \in \mathbb{R}$ and $p \in [0,1]$, $f(px + (1-p)y) \leq pf(x) + (1-p)f(y)$ (i.e., if we draw a straight line between every two points on f's graph, then this line will be above this graph). Prove that if f is convex and X is a random variable then

$$\mathsf{E}[f(X)] \geq f(\mathsf{E}[X]).$$

§5 (15 points) We showed in class that there exist functions that cannot be computed even by very large circuits. **(a)** Show that there are functions that cannot even be *approximated* by large circuits: that is, show that for any sufficiently large n, there exists a function $f : \{0,1\}^n \to \{0,1\}$ such that for every circuit C of size at most $2^{n/10}$, $f(x) \neq C(x)$ for at least a 0.49 fraction of the inputs x in $\{0,1\}^n$. See footnote for hint[1] **(b)** Show that for every function $f : \{0,1\}^n \to \{0,1\}$, there exists a circuit C of size at most $10n$ such that $C(x) = f(x)$ for at least a $1/2$ fraction of the inputs x in $\{0,1\}^n$.

§6 (No points) Please read and make sure you understand Section 3.1 in the textbook - the Time Hierarchy Theorem. I will assume this is known next week, when we'll see some more clever diagonalizations. Please do not hesitate to email me if any clarifications are needed.

[1] **Hint:** use the Chernoff bound.