COS 522 Complexity — Homework 1.

Boaz Barak

Total of 125 points. Due February 20, 2006

Important note: In all the exercises where you are asked to prove something you need to give a *clearly written* and *rigorous* proof. If a proof is made up of several steps, consider encapsulating each step as a separate claim or lemma. While the proof should be rigorous, remember that it will be read by a human and not a computer. So while you should be accurate and convincing, intuition and simplicity are preferred to excessive formality and verboseness. Use your common sense to decide which points are clear and obvious, and which deserve more elaboration and explanations.

You can use results from class, but not results from the text that were not proven (or at least stated) in class. If you're not sure whether you can or can not use a particular result, please do not hesitate to email me.

The recommended way to submit the exercises is to type them up using LaTeX. To make this simpler, I will supply the LaTeX source of the exercises so you can simply copy and paste the questions.

Exercise 0. Read the assumed knowledge handout. Skim Chapters 1 through 6 of the textbook. Read (or at least skim) Goldreich's text on computational tasks and models.

Exercise 1 (25 points)**.** The search problem CSAT is defined as follows: let C be a Boolean circuit with n-bit input and one-bit (i.e., binary) output, $\mathsf{CSAT}(C)$ is the set of inputs $x \in \{0,1\}^n$ such that $C(x) = 1$. Prove that CSAT is an $\mathbf{NP}$-complete search problem via a Karp/Levin reduction.

Exercise 2 (25 points)**.** Prove that the Hamiltonian cycle search problem is an $\mathbf{NP}$-complete search problem via a Karp/Levin reduction. (You can use the variant for *directed* graphs if that is easier for you.)

Exercise 3 (25 points)**.** Suppose that $\mathbf{P} = \mathbf{NP}$. Prove that under this assumption the decision problem Σ_2-$\mathsf{3SAT}$ can be solved in polynomial time. This decision problem is defined in the following way: the input is a statement of the following form:

$$\exists_{x \in \{0,1\}^n} \forall_{y \in \{0,1\}^m} \phi(x,y) = 1$$

where ϕ is a $3CNF$-formula of size polynomial in n, m. The output is 1 if and only if this statement is true.

Exercise 4 (25 points)**.** If $f : \{0,1\}^* \to \{0,1\}^*$ is a function, we denote by f_n the restriction of f to $\{0,1\}^n$. Recall that a Boolean circuit is a labeled bounded in-degree graph. We define the *size* of such a circuit to be the number of vertices in the graph. We say that $f \in \mathbf{P_{/poly}}$ if there are constants c, d such that for every n, f_n is computable by a circuit of size cn^d.

Show that $\mathbf{P} \subsetneq \mathbf{P_{/poly}}$. That is, that every language in $\mathbf{P}$ is in $\mathbf{P_{/poly}}$ but there exists a language in $\mathbf{P_{/poly}}$ that is not in $\mathbf{P}$.

Exercise 5 (25 points)**.**

1. Show that there exists a function $f : \{0,1\}^\ell \to \{0,1\}$ that can not be computed by a circuit of size $2^{\ell/5}$ (under the definition of size from above).
2. Give a hierarchy theorem for circuits: show that there exists a function $f : \{0,1\}^* \to \{0,1\}$ such that for every n, f_n can be computed by an n^{100}-sized circuit, but not by an n^2-sized circuit.

See footnote for hint[1]

[1] **Hint:** You might find it easier to first work with a definition of size of a circuit as the number of bits to represent the circuit as a string (say, in adjacency-list format), and then use the fact that the two definitions are related up to a logarithmic factor.