Lecturer: Thomas Rothvoss Due date: Friday, Feb 2, 2024, 11pm, on GradeScope

Problem Set 4

CSE 531 - Computational Complexity

Winter 2024

Exercise 2.30 (slightly modified from Arora and Barak; 10pts)
A language B is called *unary* if $B \subseteq \{1^n : n \in \mathbb{N}\}$. Show that if there exists an **NP**-complete unary language B, then $\mathbf{P} = \mathbf{NP}$.
Hint. Assume for the sake of contradiction that $\texttt{3SAT} \leq_p B$. Then there is a polynomial time computable function $f : \{0,1\}^* \to \mathbb{N}$ with $\psi \in \texttt{3SAT} \Leftrightarrow 1^{f(\psi)} \in B$ and $f(\psi) \leq n^c$ for some constant $c > 0$ where n is the number of variables in ψ. You may use this function polynomially many times in order to decide whether a given 3CNF ψ is satisfiable. Given a 3CNF ψ, if we select some variable x_i and a value $a \in \{0,1\}$, then $\psi' := \psi_{|x_i=a}$ is the 3CNF *obtained by substitution*, meaning we replace literal x_i by constant a and literal $\neg x_i$ by $1-a$ and either shorten the clauses or throw out satisfied clauses. For example, if $\psi := (x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3)$ then $\psi_{|x_1=0} = (x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3)$. Now, given a 3CNF ψ, design a polynomial time algorithm that maintains a set

$$L = \{(\psi_1, f(\psi_1)), \dots, (\psi_m, f(\psi_m))\}$$

where we have the invariant that each ψ_i is obtained by repeated substitution and $\psi \in \texttt{3SAT} \Leftrightarrow \bigvee_{i=1,\dots,m}(\psi_i \in \texttt{3SAT})$.
Remark. The claim is also known as Berman's Theorem.

Exercise 3.8 (rephrased from Arora and Barak; 10pts)
For a language $B \subseteq \{0,1\}^*$, we write $B_n := \{x \in B : |x| = n\}$ as all the strings of length n. Suppose we pick a random language B in the following way: for each n, with probability 1/2 one has $B_n = \emptyset$ and with probability 1/2 one has $B_n = \{y_n\}$ where y_n is a uniform random string from $\{0,1\}^n$. Prove that with high probability[1] $\mathbf{P}^B \neq \mathbf{NP}^B$.

[1] Your argument will most likely be able to show that the probability of $\mathbf{P}^B \neq \mathbf{NP}^B$ is arbitrarily close to 1. Then actually that probability must be equal to 1.