COS 522 Complexity — Homework 7.

Benny Applebaum

Total of 140 points

Exercise 1 (30 points)**.** In class we proved that the Nissan-Wigderson construction gives a $2^{\delta n}$ PRG from a $2^{\epsilon n}$ hard on average function in **E**. Please read Theorem 20.6 which generalizes this statement and its proof in pages 407–413 of the book, and then solve Exercise 20.6. (In the terminology we used in class, the notation $H_{\text{avg}}(f) \geq S$ says that f is S average-case hard.)

Exercise 2 (20 points)**.** Do Exercise 20.2

Exercise 3 (20 points)**.** Do Exercise 20.9

The notion of pseudorandomness is also central in *cryptography*. A polynomial-time computable function[1] $G : \{0,1\}^n \to \{0,1\}^{m(n)}$ is a cryptographic pseudorandom generator (PRG) if: (1) $m(n) > n$; and (2) the distribution $G(U_n)$ is $(S(n), 1/S(n))$ pseudorandom for some super-polynomial function $S(n) > n^{\omega(1)}$. I.e., for every circuit C of size at most $S(n)$

$$|\Pr[C(G(U_n)) = 1] - \Pr[C(U_{m(n)}) = 1]| < 1/S(n).$$

Note that in this setting G, which is computable in some fixed polynomial time n^c, fools adversaries that have much *more* computational resources (as $S(n)$ is super-polynomial).

In the following questions the term PRG stands for "cryptographic PRG".

Exercise 4 (20 points)**.** Prove that the existence of a PRG implies that $\mathbf{P} \neq \mathbf{NP}$.

Exercise 5 (30 points)**.** Suppose that there exists a PRG with one bit-stretch $G : \{0,1\}^n \to \{0,1\}^{n+1}$. Show that for every polynomial $m(n)$ there exists a PRG $G' : \{0,1\}^n \to \{0,1\}^{m(n)}$. Specifically, prove that the following algorithm G' is a PRG.

- Input: $x \in \{0,1\}^n$.
- Let $y^{(0)} = x$.
- For $i = 1$ to $m(n) - n$ set $y^{(i)} = G(y^{i-1})$.
- Output $y^{(m(n)-n)}$.

Hint: Use a hybrid argument where the i-th hybrid H_i is the output of G' where the value of $y^{(i)}$ is chosen randomly at uniform from $\{0,1\}^{n+i}$. (Can you see why simple induction on i does not work?)

Exercise 6 (20 points)**.** Prove that the existence of a PRG implies that $\mathbf{BPP} \subseteq \bigcap_{\epsilon>0} \text{DTIME}(2^{n^\epsilon})$. You may use the statement of the previous question even if you haven't solved it.

[1] We think of G as a function family which is defined for every input length n.