You are encouraged to collaborate on the homework and ask for assistance. You are required to write your own solutions, list your collaborators, acknowledge all sources of help, and cite all external references.

Question 1

One method for gauging how hard it is to prove a conjecture C is to investigate if NOT C is true under the assumption that P equals NP. If P = NP implies NOT C then proving C would also prove that P $\neq$ NP, so a proof of C (if true) is likely out of reach. Show that the following statements are true assuming P = NP:

(a) The problem "Given a circuit C as input, all assignments are satisfying for C" is in P.

(b) Polynomial Identity Testing is in P. (**Hint:** Think of the randomness as a potential NP certificate.)

(c) There is no polynomial-time computable family $G_n\colon \{0,1\}^n \to \{0,1\}^{n+1}$ of $(2^{n/10}, 1/4)$-pseudorandom generators. (**Hint:** The problem "On input y, does there exists x such that $G_{|x|}(x) = y$?" is in NP.)

Question 2

Assume $f\colon \{0,1\}^n \to \{0,1\}$ is 0.01-unpredictable against size n^2. Which of these constructions is an $(n^2/10, 0.1)$-pseudorandom generator? If you answer no describe a distinguisher for G. If you answer yes show how to convert a distinguisher for G into a predictor for f (possibly using results from class). Addition denotes (bitwise) xor.

(a) $G\colon \{0,1\}^{2n} \to \{0,1\}^{2n+2}$ given by $G(x,y) = (x, f(x), y, f(x) + f(y))$.

(b) $G\colon \{0,1\}^{nm} \to \{0,1\}^{\binom{m}{2}}$ (one output for every pair of inputs), with $m = 3n$, given by

$$G(x_1, \ldots, x_m) = \big(f(x_1) + f(x_2), \ldots, f(x_1) + f(x_n), f(x_2) + f(x_3), \ldots, f(x_{m-1}) + f(x_m)\big)$$

(c) **(Optional)** $G\colon \{0,1\}^{3n} \to \{0,1\}^{3n+3}$ given by $G(x,y,z) = (x, y, z, f(x+y), f(x+z), f(y+z))$.

Question 3

In Lecture 3 we showed that the following property of functions $f\colon \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ separates *EQUALITY* (when $m = n$) from width 2^n read-once branching programs:

`diffext`(f): For every pair $x \neq x' \in \{0,1\}^n$ there exists a $y \in \{0,1\}^m$ such that $f(x,y) \neq f(x',y)$.

(a) Argue that `diffext` is $2^{O(n+m)}$-constructive, namely describe an efficient algorithm that deciders `diffext`(f) using oracle access to f and analyze its running time.

(b) Show that the probability that `diffext`(R) holds for a random function R is at least $1 - 2^{2n-m-1}$.
(**Hint:** Calculate the probability $R(x,y) = R(x',y)$ for fixed $x \neq x'$ and all y and take a union bound.)

(c) Use part (b) to show that `diffext`(f) is 1/2-large (and therefore natural) when $m \geq 2n$.