Problem Set #2

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Sep. 14, noon (before start of class)

General instructions: If you collaborate or use any outside resources, remember to cite them in your solutions.

Problem #1. Big-O Notation and Negligible Functions (40 points)

For parts a-c, you need only give your answers, but if you explain your reasoning, you may qualify for partial credit in cases where your answer is incorrect. Parts a-c refer to the following five functions of n:

$$f_1(n) = 3n + 15 \tag{1}$$
$$f_2(n) = \frac{1}{2}(n^3 + n^{-3}) \tag{2}$$
$$f_3(n) = \frac{n^{-11}}{18} \tag{3}$$
$$f_4(n) = \left(\frac{3}{2}\right)^{\sqrt{n}} \tag{4}$$
$$f_5(n) = \left(\frac{2}{3}\right)^{\sqrt{n}} \tag{5}$$

a) (10 points) For each of the five functions $f_i(n)$, say if it is $O(n^3)$.

b) (10 points) For each of the five functions $f_i(n)$, say if it is $O(1)$. (I.e., if it is $O(g(n))$, where $g(n) = 1$ is a constant function.)

c) (10 points) For each of the five functions $f_i(n)$, say if it is negligible.

d) (10 points) Let $\epsilon(s)$ be a negligible function of s and let $p(s)$ be a polynomial function of s. Show that there exists s_1 such that for any $s > s_1$, $p(s)\epsilon(2s) < 1$.
Hint: Let $t = 2s$ and find another polynomial function $q(t)$ such that by applying the definition of negligible to $\epsilon(t)$, you get the desired result.
Comment: This result is the main step to proving that if $\epsilon(s)$ is negligible then $\epsilon(2s)$ is also negligible.

Problem #2. Combining Pseudorandom Generators (80 points)

For this problem, let $G(y)$ and $H(y)$ be two efficiently computable pseudorandom generators with $\ell(s) = 2s$. Recall that G (or H) takes inputs of arbitrary length s and outputs bit strings of length $\ell(s)$.

a) (20 points) Let $|$ represent concatenation, so if m and n are two bit strings of length $2s$, then $m|n$ is the string of length $4s$ formed by bits of m followed by the bits of n. Then let $K_1(y) = G(y)|G(y)$ (which takes inputs of length s and outputs bit strings of length $4s$) and find an attack that shows that $K(y)$ is *not* a pseudorandom generator.

b) (20 points) Is $K_2(y) = G(y)|H(y)$ a pseudorandom generator for all pairs of functions $G(y)$ and $H(y)$ such that $G(y) \neq H(y)$ for all y? Why or why not?

c) (20 points) Let $K_3(y) = H(G(y))$, which also takes inputs of size s and outputs bit strings of length $4s$. ($G(y)$ and $H(y)$ do not always have to be different here.) Explain how to create a reduction which turns an efficient attack on $K_3(y)$ into an efficient attack on $G(y)$. (In fact, this reduction shows that $K_3(y)$ is a pseudorandom generator but you don't need to go through all the other details. In particular, you don't need to calculate the success probability of the attack on $G(y)$, merely set up the reduction.)
Hint: This reduction will look similar to the one showing the security of the pseudo one-time pad.

d) (5 points) Let $G^{(k)} = G^{(k-1)}(G(y))$ for $k \geq 2$, where $G^{(1)}(y) = G(y)$. If the input to $G^{(k)}$ is a bit string of length s, how long is the output?

e) (15 points) Define $G^{(k)}$ as in part d. Let $K_4(y) = G^{(s)}(y)$ when the length of y is s. Which of these two arguments is correct?

1. $K_4(y)$ is a pseudorandom generator, because the reduction in part c shows that if $H(y) = G^{(k-1)}(y)$, then $G^{(k)}(y)$ is also a pseudorandom generator.
2. $K_4(y)$ is *not* a pseudorandom generator, because Eve can do a brute force attack by trying all possible inputs y to distinguish $K_4(y)$ from a random string.