

## Homework 2

*Due: February 22, 2026 (11:59 PM)*

## 1 Negligible/Non-Negligible Functions

For each  $n \in \mathbb{N}$ , determine whether the following functions are negligible, non-negligible, or neither. Write a proof for your conclusion in each case.

1. **(10 points)**  $f(n) = n^5 \cdot g(n)$ , where  $g : \mathbb{N} \rightarrow \mathbb{R}$  is a negligible function.
2. **(10 points)**  $f(n) = n^{-1000000000} + 40^{-n}$
3. **(10 points)**  $f(n) = g(n)^{-h(n)}$ , where  $g, h : \mathbb{N} \rightarrow \mathbb{R}$  are negligible functions.

## 2 Hybrid Lemma

**(10 points)** Recall the hybrid lemma discussed in class: let  $\mathcal{D}_1, \dots, \mathcal{D}_m$  be distributions such that, for every  $1 \leq i \leq m-1$ , the adjacent distributions  $\mathcal{D}_i$  and  $\mathcal{D}_{i+1}$  are computationally indistinguishable. If  $m = \text{poly}(n)$ , then  $\mathcal{D}_1$  and  $\mathcal{D}_m$  are also computationally indistinguishable.

**Explain why  $\mathcal{D}_1$  and  $\mathcal{D}_m$  are not guaranteed to be computationally indistinguishable if  $m = 2^n$ .**

## 3 Pseudorandom Generator

Let  $G_1 : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  and  $G_2 : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$  be two (possibly different) pseudorandom generators (PRGs). Define a function  $G : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{4n}$  by

$$G(s_1 \| s_2) = G_1(s_1) \| G_2(s_2).$$

In this problem, we will prove that  $G$  is also a pseudorandom generator.

**Proof.** The function  $G$  is clearly deterministic and expands its input from  $2n$  bits to  $4n$  bits. To show that  $G$  is a PRG, it therefore suffices to prove that its output is pseudorandom. Equivalently, we must show that the following distributions are computationally indistinguishable:

- $\{G(s_1 \| s_2) \mid s_1 \leftarrow \$ \{0, 1\}^n, s_2 \leftarrow \$ \{0, 1\}^n\}$
- $\{r \leftarrow \$ \{0, 1\}^{4n}\}$

We prove this using a hybrid argument. Consider the hybrids:

- $\mathcal{H}_0 := \{G(s_1 \| s_2) \mid s_1 \leftarrow \$ \{0, 1\}^n, s_2 \leftarrow \$ \{0, 1\}^n\}$
- $\mathcal{H}_1 := \{G_1(s_1) \| r_2 \mid s_1 \leftarrow \$ \{0, 1\}^n, r_2 \leftarrow \$ \{0, 1\}^{2n}\}$
- $\mathcal{H}_2 := \{r \leftarrow \$ \{0, 1\}^{4n}\}$

By the hybrid lemma, it suffices to prove that

$$\mathcal{H}_0 \approx_c \mathcal{H}_1 \quad \text{and} \quad \mathcal{H}_1 \approx_c \mathcal{H}_2.$$

1. **(10 points) Explain how the pseudorandomness of  $G_1$  and  $G_2$  implies that  $\mathcal{H}_0 \approx_c \mathcal{H}_1$  and  $\mathcal{H}_1 \approx_c \mathcal{H}_2$ .**
2. **(10 points) Prove via a reduction that  $\mathcal{H}_0 \approx_c \mathcal{H}_1$ .**  
**Hint:** Assume toward contradiction that  $\mathcal{H}_0$  and  $\mathcal{H}_1$  are distinguishable; that is, there exists a non-uniform PPT adversary  $\mathcal{A}$  with non-negligible advantage in distinguishing them. Construct a PPT adversary  $\mathcal{B}$  that uses  $\mathcal{A}$  as a subroutine to break the pseudorandomness of  $G_1$ , thereby deriving a contradiction.
3. **(10 points) Prove via a reduction that  $\mathcal{H}_1 \approx_c \mathcal{H}_2$ .**