CS178 Assignment 2

Jonas Chen

February 20, 2025

Problem 1

> Let $f : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}$ be a pseudorandom function. Show that there exists a pseudorandom generator $G : \{0,1\}^\lambda \times \{0,1\}^{n'} \to \{0,1\}^m$,
> where $m > n' + \lambda$ and $n' = n - \lceil \log_2(m) \rceil$ and $n \geq \lceil \log_2(m) \rceil$

Solution

Define G over any choice of λ, n', m such that $m > n' + \lambda$ as follows:

On input ($k \in \{0,1\}^\lambda$,$z \in \{0,1\}^{n'}$)

1: Compute $n = n' + \lceil \log_2(m) \rceil$

2: Generate the first m strings of length n and denote them to be $x_1, x_2, ..., x_m = 0000, 0001, ..., 1111$ etc.

Note that $m \leq 2^{\lceil \log_2(m) \rceil} \leq 2^n$ (by the last condition in the problem statement) so that there are always sufficient amount of strings of length n generated by the above

3: output $f(k \parallel x_1) \parallel f(k \parallel x_2) \parallel ... \parallel f(k \parallel x_m)$

Then G is guaranteed to generate m bits of output.

Also, the third condition that $n \geq \lceil \log_2(m) \rceil$ is satisfied based on the computation of n above. (note that n' can be 0)

G will run in a time polynomial in m and is determinstic since f is determinstic

We need to show that G is a function that satisifes the definition of pesudorandom generators

Let $G_{n,m} = \{g : \{0,1\}^n \to \{0,1\}^m\}$ and let $g_{n,m} \xleftarrow{\$} G_{n,m}$ be the family of random functions as defined in class.

By definition of pesudorandom functions we have that dist$\{f\} \underset{c}{\approx} \left\{g_{n,1}\right\} \underset{c}{\approx} \left\{U_{\{0,1\}^1}\right\}$ since the random function $g : \{0,1\}^n \to \{0,1\}$ simply samples from uniform distribution over the bits $\{0,1\}$

This means that each bit from the output of G is computationally indistinguishable from a random bit, which further means that $\left\{y = G(z) \mid z \xleftarrow{\$} \{0,1\}^n\right\} \underset{c}{\approx} \left\{y \xleftarrow{\$} \{0,1\}^m\right\}$

Therefore G as constructed above is a pesudorandom generator $\square$

Importantly, each call to f is on a different input, if any two of the inputs are identical then those two bits would be distinguishable from uniform 2 bits (we showed this is important in class today (feb 19))

Problem 2

> Let $f : \{0,1\}^n \to \{0,1\}^m$
>
> Suppose there is a binary string $y \in \{0,1\}^m$ such that
>
> $$\Pr\left[f(x) = y : x \xleftarrow{\$} \{0,1\}^n\right] \geq \frac{1}{\text{poly}(n)}$$
>
> Note that the probability is taken over choice of x. Show that f is not a one-way function.

Solution

Fix $x \xleftarrow{\$} \{0,1\}^n$ and also fix $f(x) \in \{0,1\}^m$

Consider an adversary A which on input $f(x)$ outputs s where $s \xleftarrow{\$} \{0,1\}^n$

Then $A(f(x))$ is sampled uniformly from $\{0,1\}^n$ and since we know there exists y such that $f(x) = y$,

$$\Pr[f(A(f(x))) = y] \geq \frac{1}{\text{poly}(n)} \text{ and}$$

$$\Pr[f(x) = y] \geq \frac{1}{\text{poly(n)}} \text{ means that}$$

$$\Pr[f(x) = f(A(f(x)))]$$

$$= \Pr[f(x) = y] \cdot \Pr[f(A(f(x))) = y] \geq \frac{1}{\text{poly}(n)^2} \geq \text{negl}(n)$$

which shows that A outputs a preimage of $f(x)$ with non-negligilble probability. (thus f is not a one-way function.)

□

Problem 3

> Let PRG: $\{0,1\}^n \to \{0,1\}^{2n}$ be a pesudorandom generator. Let $s \xleftarrow{\$} \{0,1\}^n, r \xleftarrow{\$} \{0,1\}^{m=2n}$ and $y = \text{PRG}(s)$ Consider the following program $P_{r,y}$:
>
> 1: On input $x \in \{0,1\}^n$ check that $\text{PRG}(x) \oplus r = y$
>
> 2: If true; output 1 else output 0
>
> Show that there is no PPT adversary that, given (r,y) outputs $x \in \{0,1\}^n$ such that $P_{r,y}(x) = 1$ with non-negligilble probability.
>
> You have to show that for all PPT adversary A with input (r,y) and output $x \in \{0,1\}^n$ that
>
> $$\Pr\left[P_{r,y}(x) = 1 \mid x \leftarrow A(r,y)\right] = \text{negl}(n)$$

Solution

Suppose that there $\exists A$ such that $\Pr\left[P_{r,y}(x) = 1 \mid x \leftarrow A(r,y)\right] > \text{negl}(n)$

Note that $\Pr\left[P_{r,y}(x) = 1\right] = \Pr[\text{PRG}(x) \oplus r = y] = \Pr[\text{PRG}(x) = r \oplus y]$

Note that all pesudorandom generators are one way functions (we will prove this later)

Consider another adversary B, which is defined as follows:

B on input $r \oplus y$:

1: Set $\text{PRG}(x) := r \oplus y$

2: Outputs $x' \leftarrow A(r,y)$

Then $\Pr[\text{PRG}(x) = \text{PRG}(x') = r \oplus y] = \Pr\left[P_{r,y}(x') = 1\right] > \text{negl}(n)$ due to the initial assumption

Which contradicts the fact that PRG is a one way function. (For any r, y we have that an adversary that can generate an x' such that $\text{PRG}(x') = r \oplus y$, note that $r \oplus y$ is a uniformly sampled string from $\{0,1\}^{2n}$)

Therefore A cannot exist, as desired $\square$

Proof that pesudorandom generators are one-way functions:

Assume that $G : \{0,1\}^n \to \{0,1\}^{n+1}$ is a pesudorandom generator and is not a one way function i.e.

$\Pr\left[G(x) = G(x') \mid x' \leftarrow A(G(x)); x \xleftarrow{\$} \{0,1\}^n\right] > \text{negl}(n)$

Then consider a distinguisher D that does the following:

On input z, run $A(z)$ to try to generate an x' such that $G(x') = z$

If A runs sucessfully, output 1, else output 0

$\Pr[1 \leftarrow D(z_1) \mid z_1 \leftarrow \{G(x)\}] > \text{negl}(n)$ by assumption, and

$\Pr\left[1 \leftarrow D(z_2) \mid z_2 \xleftarrow{\$} \{0,1\}^n\right] = \text{negl}(n)$ since G is a pesudorandom generator

Then $\left|\ \Pr[1 \leftarrow D(z_1) \mid z_1 \leftarrow \{G(x)\}] - \Pr\left[1 \leftarrow D(z_2) \mid z_2 \xleftarrow{\$} \{0,1\}^n\right]\ \right| > \text{negl}(n)$

This leads to a contradiction that G is not a pesudorandom generator. therefore G must be a one-way function $\square$