CS178 F21 Homework 2

Michael Glushchenko, 9403890

October 26, 2021

1 Negligible or Non-negligible?

1.1

$$f_1(n) = \mu(n) * n^{2021} \text{ for some negligible function } \mu(n)$$

$$\mu(n) \text{ is negligible } \Rightarrow (\forall c > 0)(\exists n_0 > 0)(\forall n > n_0)(\mu(n) \leq \frac{1}{n^c})$$

$$\mu(n) \leq \frac{1}{n^c} \Rightarrow \mu(n) * n^{2021} \leq \frac{1}{n^c} * n^{2021} = \frac{1}{n^{c+2021}} \Rightarrow f_1(n) \leq \frac{1}{n^{c+2021}}$$

$$\text{Define a very conservative } n_0' := n_0^{2022} \text{ and we have}$$

$$(\forall c > 0)(\exists n_0' > 0)(\forall n > n_0')(f_1(n) \leq \frac{1}{n^c}) \Rightarrow f_1(n) \text{ is negligible.}$$

1.2

$$f_2(n) = (log(n))^{-log(log(n))}$$

$$\text{Define } m := log(n) \rightarrow f_2(n) = m^{-log(m)} = \frac{1}{m^{log(m)}}$$

$$\text{We want to know if } (\forall c > 0)(\exists m_0 > 0)(\forall m > m_0)(\frac{1}{m^{log(m)}} \leq \frac{1}{m^c})$$

$$\text{Suppose not; } \Rightarrow \frac{1}{m^{log(m)}} > \frac{1}{m^c} \Rightarrow m^{log(m)} < m^c \Rightarrow log(m) < c$$

A contradiction, $log(m)$ is not bounded by a constant $\Rightarrow f_2(n)$ is negligible.

2 Product of Two Non-negligible Functions

$$\text{Define } f_1(n) := \begin{cases} 1 & \forall n \mod 2 = 0 \\ 0 & \text{otherwise} \end{cases}$$

$$\text{Define } f_2(n) := \begin{cases} 1 & \forall n \mod 2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$f_1(n) \text{ and } f_2(n) \text{ are both discontinuous, and thus non-negligible}$$

$$\text{Define } f_3(n) := f_1(n) * f_2(n) = \begin{cases} 0 & \forall n \mod 2 = 0 \\ 1 & \forall n \mod 2 = 0 \end{cases} = 0 \quad \forall n$$

$$f_3(n) \text{ is a negligible function, as it's always 0.}$$

3 Closure of Computational Indistinguishability

3.1 Given

$$X_n,\ Y_n \in \{0,1\}^{\text{poly}(n)}$$

3.2 Claim

$$\{X_n\} \approx_c \{Y_n\} \Rightarrow \{f(X_n)\} \approx_c \{f(Y_n)\}$$

3.3 Proof

$$\{X_n\} \approx_c \{Y_n\} \text{ implies } (\forall \text{PPT } \mathcal{D})(\exists v()) \text{ s.t.:}$$

$$|\mathcal{P}[\mathcal{D}(x); x \leftarrow X_n] - \mathcal{P}[\mathcal{D}(x); x \leftarrow Y_n]| \leq v(n)$$

We want to know if $\{f(X_n)\} \approx_c \{f(Y_n)\}$.
Suppose not $\Rightarrow \exists$PPT Distinguisher $\mathcal{D}$ that distinguishes $\{f(X_n)\}$ and $\{f(Y_n)\}$ with some non-negligible probability $\epsilon(n)$:

$$|\mathcal{P}[\mathcal{D}(x); x \leftarrow f(X_n)] - \mathcal{P}[\mathcal{D}(x); x \leftarrow f(Y_n)]| > \epsilon(n)$$

But because f can be computed in polynomial time, we can build $\mathcal{D}' = \mathcal{D}(f(x))$, that can distinguish X_n and Y_n with the same non-negligible probability $\epsilon(n)$:

$$|\mathcal{P}[\mathcal{D}(f(x)); x \leftarrow X_n] - \mathcal{P}[\mathcal{D}(f(x)); x \leftarrow Y_n]| > \epsilon(n)$$

$$\Rightarrow \{X_n\} \not\approx_c \{Y_n\} \Rightarrow \text{a contradiction.}$$

Thus, we have

$$\{f(X_n)\} \approx_c \{f(Y_n)\}.$$

4 Pseudorandom Generator Security

Given:

$$G : \{0,1\}^n \to \{0,1\}^{3n} \text{ is a secure PRG,}$$

meaning $\forall$ PPT Distinguishers $\mathcal{D}, , \exists$ a negligible $v(n)$ s.t.:

$$|\mathcal{P}[\mathcal{D}(x) : x \leftarrow G] - \mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}] \leq v(n)$$

4.1

$$G_1(s) : \{0,1\}^n \to \{0,1\}^{3n}, \quad G_1(s) = (G(s)_{[2n],r}), \text{ where } r \overset{\$}{\leftarrow} \{0,1\}^n$$

Want to show that $G_1(s)$ is a secure pseudorandom generator.
Suppose not $\Rightarrow \exists$ a PPT $\mathcal{D}$ that can distinguish the output of $G_1(s)$ from the output of a uniformly-random distribution with some non-negligible probability $\epsilon(n)$:

$$|\mathcal{P}[\mathcal{D}(x) : x \leftarrow (G(x)_{[2n],r}), r \overset{\$}{\leftarrow} \{0,1\}^n] - \mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}] \geq \epsilon(n)$$

We construct the following hybrid distributions:

$$\mathcal{H}_1 := \{x||y : x \overset{\$}{\leftarrow} \{0,1\}^{2n},\ y \overset{\$}{\leftarrow} \{0,1\}^n\}$$

$$\mathcal{H}_2 := \{x : x \overset{\$}{\leftarrow} \{0,1\}^{3n}\}$$

The concatenation of two uniform distributions gives us another uniform distribution $\mathcal{H}_2$ over $\{0,1\}^{3n}$. That is precisely what $\mathcal{H}_4$ is $\Rightarrow \mathcal{H}_1 \equiv \mathcal{H}_2$.
By hybrid lemma, the above probability expression is equivalent to:

$$|\mathcal{P}[\mathcal{D}(x) : x \leftarrow (G(x)_{[2n],r}), r \overset{\$}{\leftarrow} \{0,1\}^n] - \mathcal{P}[\mathcal{D}(x||y) : x \overset{\$}{\leftarrow} \{0,1\}^{2n},\ y \overset{\$}{\leftarrow} \{0,1\}^n]|,$$

which is $\geq \epsilon(n)$.
Here, the last n bits for both ciphertexts x and $x||y$ are chosen from an identical uniformly-random distribution over $\{0,1\}^n$, so, again, by hybrid lemma:

$$|\mathcal{P}[\mathcal{D}(x) : x \leftarrow (G(x)_{[2n]})] - \mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{2n}]| \geq \epsilon(n),$$

A truncation $t : \{0,1\}^{3n} \to \{0,1\}^{2n}$ is a polynomial-time function $\Rightarrow$ by closure property, since $\{x : x \leftarrow G(x)\} \approx_c \{x : x \overset{\$}{\leftarrow} \{0,1\}^{3n}\}$, it must be true that $\{t(x) : x \leftarrow G(x)\} \approx_c \{t(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}\}$. But the above is equivalent to:

$$|\mathcal{P}[\mathcal{D}(x) : x \leftarrow t(G(x))] - \mathcal{P}[\mathcal{D}(x) : x \leftarrow t(y), y \overset{\$}{\leftarrow} \{0,1\}^{3n}]| \geq \epsilon(n),$$

for some non-negligible probability $\epsilon(n)$. This is a contradiciton breaking the closure property of computational indistinguishability $\Rightarrow G_1(s)$ is a secure PRG.

Given:

$$G : \{0,1\}^n \to \{0,1\}^{3n} \text{ is a secure PRG,}$$

meaning $\forall$ PPT Distinguishers $\mathcal{D}$, , $\exists$ a negligible $v(n)$ s.t.:

$$|\mathcal{P}[\mathcal{D}(x) : x \leftarrow G] - \mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}] \leq v(n)$$

4.2

$$G_2(s) : \{0,1\}^{2n} \to \{0,1\}^{6n}, \quad G_2(r,s) = (G(r), G(s)), \text{ where } r, s \overset{\$}{\leftarrow} \{0,1\}^n$$

Want to show that $G_2(s)$ is a secure pseudorandom generator.
Suppose not $\Rightarrow$ $\exists$PPT $\mathcal{D}$ that can distinguish the output of $G_2(s)$ from the output of a uniform distribution with some non-negligible probability $\epsilon(n)$:

$$|\mathcal{P}[\mathcal{D}(x||y) : x \leftarrow G(r), y \leftarrow G(s)] - \mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{6n}]| \geq \epsilon(n)$$

But the average of identical uniform distributions is still uniform, so the uniform distribution $\{x : x \overset{\$}{\leftarrow} \{0,1\}^{6n}\}$ is identical to the uniform distribution $\{(x||y) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}, y \overset{\$}{\leftarrow} \{0,1\}^{3n}\}$. This means we can write

$$|\mathcal{P}[\mathcal{D}(x||y) : x \leftarrow G(r), y \leftarrow G(s)] - \mathcal{P}[\mathcal{D}(x||y) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}, y \overset{\$}{\leftarrow} \{0,1\}^{3n}]| \geq \epsilon(n)$$

Using the union bound method, we know that the following statements are true

$$\mathcal{P}[\mathcal{D}(x||y) : x \leftarrow G(r), y \leftarrow G(s)] \leq \mathcal{P}[\mathcal{D}(x) : x \leftarrow G(r)] + \mathcal{P}[\mathcal{D}(y) : y \leftarrow G(s)]$$

$$\mathcal{P}[\mathcal{D}(x||y) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}, y \overset{\$}{\leftarrow} \{0,1\}^{3n}] \leq 2\mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}]$$

We know that G is deterministic, and thus the probability of distinguishing one output of G from a uniform distribution is the same as the probability of distinguishing another output of G from a uniform distribution:

$$\mathcal{P}[\mathcal{D}(x) : x \leftarrow G(r)] = \mathcal{P}[\mathcal{D}(y) : y \leftarrow G(s)] \text{for a given distinguisher } \mathcal{D}.$$

$$\Rightarrow |2\mathcal{P}[\mathcal{D}(x) : x \leftarrow G(r)] - 2\mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}]| \geq \epsilon(n)$$

$$\Rightarrow 2|\mathcal{P}[\mathcal{D}(x) : x \leftarrow G(r)] - \mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}]| \geq \epsilon(n)$$

$$\Rightarrow |\mathcal{P}[\mathcal{D}(x) : x \leftarrow G(r)] - \mathcal{P}[\mathcal{D}(x) : x \overset{\$}{\leftarrow} \{0,1\}^{3n}]| \geq \frac{\epsilon(n)}{2},$$

But if $\epsilon(n)$ is a non-negligible probability, then $\frac{\epsilon(n)}{2}$ is also non-negligible. This breaks our assumption that G cannot be distinguished from a uniform distribution with non-negligible probability $\Rightarrow$ $G_2(s)$ is a secure PRG.

5 One-Way Functions

5.1 No, it's not

$$f(x) \equiv x + 2021 \pmod{2^n}, \forall x \in \mathbb{Z}_{2^n}$$

To show it's not one-way, we simply need to find an existing adversary that has a non-negligible probability of inverting f (meaning if the adversary can invert f for a some classified portion of the input values of n, i.e. all even values, or all values greater than some number, etc, then we are done).
We know that for some constant c,

$$c * 2^n + f(x) - 2021 = x$$

But since n is the number of bits in x, we know that $x \leq 2^n - 1$ (need $n+1$ bits to represent 2^n). So, the c in the following expression

$$f(x) - 2021 = x$$

is either 1 or 0. We can now construct an adversary $\mathcal{A}$ that simply outputs $f(x) - 2021$. This is enough: $\mathcal{A}$ successfully inverts f with non-negligible probability for some n with $2^n >> 2021$, where 12th bit of $f(x)$ is 0. This is because the 12th bit being 0 ensures we don't overflow when adding the 11-bit decimal 2021, while $2^n >> 2021$ ensures that $\pmod{2^n}$ doesn't change the output of $x+2021$. So we can always output $x + 2021$, and for every given n, have a non-negligible probability of correctly inverting the function.

We can come up with other adversaries (one that uses $c = 1$, for example), that have non-negligible probability of inverting $f(x)$ for some portion of values of x, but the above is enough to show

$$\exists \text{PPT } \mathcal{A} \text{ and a negligible function } \epsilon(n) \text{ such that } \mathcal{P}[\mathcal{A} \text{ inverts f(x)}] \geq \epsilon(n).$$

5.2 Yes, we can

Yes. If we set $f'(x_1 \cdots x_n) = f(x_1 \cdots x_n)$ concatennated with 1 at the end, i.e. $f'(|x_1| \cdots |x_n|) = f(|x_1| \cdots |x_n||1|)$ then we have that f' is still a one-way function (the probability of a distinguisher correctly **inverting** f' is the same as that of it **inverting** f, (knowing the last bit does not help us invert f) and thus negligible; however, f' is not a secure PRG: the next bit unpredictibility test fails here, and we can use the hybrid lemma to prove the PRG is not secure if we related it to some other PRG.