Lecture 7.2: Pseudorandom Functions

Oracle Algorithms

- A binary-output oracle O maps a query $q \in \{0,1\}^n$ to an answer $a \in \{0,1\}$

Oracle Algorithms

- A binary-output oracle O maps a query $q \in \{0,1\}^n$ to an answer $a \in \{0,1\}$
- Querying and receiving an answer from the oracle takes unit time

Oracle Algorithms

- A binary-output oracle O maps a query $q \in \{0,1\}^n$ to an answer $a \in \{0,1\}$
- Querying and receiving an answer from the oracle takes unit time
- An oracle algorithm $\mathcal{A}$ with oracle access to oracle O is written as $\mathcal{A}^O$

Oracle Algorithms

- A binary-output oracle O maps a query $q \in \{0,1\}^n$ to an answer $a \in \{0,1\}$
- Querying and receiving an answer from the oracle takes unit time
- An oracle algorithm $\mathcal{A}$ with oracle access to oracle O is written as $\mathcal{A}^O$
- Think: Definition of PPT and n.u. PPT in this context

Random Functions

- Let $\mathcal{F}_n$ be the set of all functions which map inputs in $\{0,1\}^n$ to $\{0,1\}$

Random Functions

- Let $\mathcal{F}_n$ be the set of all functions which map inputs in $\{0,1\}^n$ to $\{0,1\}$
- What is $|\mathcal{F}_n|$?

Random Functions

- Let $\mathcal{F}_n$ be the set of all functions which map inputs in $\{0,1\}^n$ to $\{0,1\}$
- What is $|\mathcal{F}_n|$? Ans: 2^{2^n}

Random Functions

- Let $\mathcal{F}_n$ be the set of all functions which map inputs in $\{0,1\}^n$ to $\{0,1\}$
- What is $|\mathcal{F}_n|$? Ans: 2^{2^n}
- A random function is: $f \xleftarrow{\$} \mathcal{F}_n$

Oracle Indistinguishability

Definition (Oracle Ensemble)

An oracle ensemble $\{O_n\}$ is a probability distribution over the set of all functions $f : \{0,1\}^n \to \{0,1\}^{\ell(n)}$.

Oracle Indistinguishability

Definition (Oracle Ensemble)

An oracle ensemble $\{O_n\}$ is a probability distribution over the set of all functions $f : \{0,1\}^n \to \{0,1\}^{\ell(n)}$.

Mostly we will have $\ell(n) = n$

Oracle Indistinguishability

Definition (Oracle Ensemble)

An oracle ensemble $\{O_n\}$ is a probability distribution over the set of all functions $f : \{0,1\}^n \to \{0,1\}^{\ell(n)}$.

Mostly we will have $\ell(n) = n$

Definition (Oracle Indistinguishability)

Two oracle ensembles $\{O_n\}$ and $\{O'_n\}$ are computationally indistinguishable if for all n.u. PPT oracle machines D, there exists a negligible function $\varepsilon(\cdot)$ such that:

$$\left|\Pr[f \leftarrow O_n : D^f(1^n) = 1] - \Pr[f \leftarrow O'_n : D^f(1^n) = 1]\right| \leqslant \varepsilon(n)$$

Pseudo-random Functions

Definition (Pseudo-random Functions)

A family of functions $\{f_s : \{0,1\}^n \to \{0,1\}^n\}$ is a pseudo-random function if:

- There exists a PPT F such that $F(s,x)$ efficiently computes the function $f_s(x)$, and

Pseudo-random Functions

Definition (Pseudo-random Functions)

A family of functions $\{f_s : \{0,1\}^n \to \{0,1\}^n\}$ is a pseudo-random function if:

- There exists a PPT F such that $F(s,x)$ efficiently computes the function $f_s(x)$, and
- $\{s \xleftarrow{\$} \{0,1\}^n : f_s\} \approx \{f \xleftarrow{\$} \mathcal{F}_n : f\}$