Lecture 11: Random Function

In this lecture we will learn about a few properties to expect from a Random Function

Representing Functions I

- Let $f : \mathcal{D} \to \mathcal{R}$ be a function from the domain $\mathcal{D}$ to the range $\mathcal{R}$
- Suppose $\mathcal{D} = \{x_1, x_2, \dots, x_N\}$ be a domain of finite size
- And, suppose that $\mathcal{R} = \{y_1, y_2, \dots, y_M\}$ be a range of finite size
- A function can be equivalently expressed as a table of entries

x_1	$f(x_1)$
x_2	$f(x_2)$
$\vdots$	$\vdots$
x_N	$f(x_N)$

Representing Functions II

- Now, this table can be expressed, equivalently, as the list

$$\left(\ f(x_1), f(x_2), \ldots, f(x_N)\ \right)$$

- So, every function f can be written as the list mentioned above

Equivalence of Functions

- Let $f, g \colon \mathcal{D} \to \mathcal{R}$ be two functions
- We say that the functions f and g are equivalent if they have identical input-output behavior, i.e., $f(x) = g(x)$, for all $x \in \mathcal{D}$

Counting Functions

- Let $\mathcal{D}$ and $\mathcal{R}$ be of size N and M, respectively
- To count the number of unique functions from the domain $\mathcal{D}$ to the range $\mathcal{R}$, we need to count the number of distinct lists

$$(y_1, y_2, \dots, y_N),$$

  where each $y_i \in \mathcal{R}$
- Note that there are M possibilities of choosing y_1
- Conditioned on choosing y_1, there are M possibilities of choosing y_2
- Conditioned on choosing y_1 and y_2, there are M possibilities of choosing y_3
- And so on ...
- So, we have the following result

Claim (Number of Functions)

There are a total of M^N distinct functions with domain-size N and range-size M

Example

- Suppose $\mathcal{D} = \{0, 1, 2\}$ and $\mathcal{R} = \{0, 1\}$
- The list $(1, 0, 1)$ corresponds to the function f such that $f(0) = 1$, $f(1) = 0$, and $f(2) = 1$
- There are $2^3 = 8$ different functions
- The eight functions correspond to the lists $(0, 0, 0)$, $(0, 0, 1)$, $(0, 1, 0)$, $(0, 1, 1)$, $(1, 0, 0)$, $(1, 0, 1)$, $(1, 1, 0)$, and $(1, 1, 1)$

- We have seen that there are a total of M^N distinct functions with domain-size N and range-size M
- Let us represent the set of all these functions $\mathcal{F}_{N,M} := \{F_1, F_2, \ldots, F_{M^N}\}$

Definition (Random Function)

A function f chosen uniformly at random from the set $\mathcal{F}_{N,M}$ is referred to as the *random function*

-
- We represent this as $f \xleftarrow{\$} \mathcal{F}_{N,M}$

Property: Consistent Answers

- Once $f \xleftarrow{\$} \mathcal{F}_{N,M}$ has been sampled it always has the same value y as the value of $f(x)$
- So, this is what a random function <u>does not</u> do. Every time you query the random function at the <u>same</u> x it provides a random answer.

Property: Unpredictability I

- Suppose we sample $f \xleftarrow{\$} \mathcal{F}_{N,M}$
- For any input x_1, the output $f(x_1)$ is distributed uniformly at random over the range $\mathcal{R}$. That is, for any $x_1 \in \mathcal{D}$ and any $y_1 \in \mathcal{R}$, we have:

$$\mathbb{P}_{f \xleftarrow{\$} \mathcal{F}_{N,M}} \left[f(x_1) = y_1 \right] = \frac{1}{M}$$

- Conditioned on the answer x_1 and $f(x_1) = y_1$, for any (different) input x_2, the output $f(x_2)$ is distributed uniformly at random over the range $\mathcal{R}$. That is, for any distinct $x_1, x_2 \in \mathcal{D}$ and any $y_1, y_2 \in \mathcal{R}$, we have:

$$\mathbb{P}_{f \xleftarrow{\$} \mathcal{F}_{N,M}} \left[f(x_2) = y_2 | f(x_1) = y_1 \right] = \frac{1}{M}$$

Property: Unpredictability II

- So, in general, for $1 \leqslant k \leqslant N$, any distinct $x_1, x_2, \ldots, x_k \in \mathcal{D}$ and any $y_1, y_2, \ldots, y_k \in \mathcal{R}$, we have:

$$\mathbb{P}_{f \xleftarrow{\$} \mathcal{F}_{N,M}} \left[f(x_k) = y_k | f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_{k-1}) = y_{k-1} \right] = \frac{1}{M}$$

Bounded Unpredictability

- Note that a random function has the property that all distinct inputs (up to N) are answered independently and uniformly at random
- Suppose we need this requirement only for the first 5 inputs
- Suppose $\mathcal{D} = \mathcal{R}$ be a field $\mathbb{F}$
- Exercise: Think how the set of polynomials with coefficients in $\mathbb{F}$ and of degree $< t$ ensures t-bounded unpredictability
- Exercise: Suppose Alice and Bob want to perform private-key encryption for t messages. How to use t-bounded unpredictability to design a secure private-key encryption scheme for t messages.