CS 276 – Cryptography Sept 8, 2014

Lecture 1: One-Way Functions

Instructor: Sanjam Garg *Scribe: Rohin Shah*

1 Noticeable and Negligible Functions

Noticeable and negligible functions are used to characterize how "large" a function representing a probability is. Intuitively, a noticeable function is one which is at most polynomially small, whereas a negligible function must be exponentially small (more accurately, it must be smaller than any polynomial function).

1.1 Definitions and Examples

Definition 1 (Negligible Function) *A function μ is negligible iff $\forall c \in N\ \exists n_0 \in N$ such that $\forall n \geq n_0,\ \mu(n) < n^{-c}$.*

Definition 2 (Noticeable Function) *A function μ is noticeable iff $\exists c \in N, n_0 \in N$ such that $\forall n \geq n_0,\ \mu(n) \geq n^{-c}$.*

As an example, since $\mu(n) = 2^{-n}$ is exponentially small, it is a negligible function (proof in the appendix). On the other hand $\mu(n) = n^{-3}$ is only polynomially small and so is noticeable. (The proof is simple - just set $c = 3, n_0 = 1$ in the definition of a noticeable function.)

1.2 Difference between Noticeable and Non-Negligible

Note that a non-negligible function is not necessarily a noticeable function. A non-negligible function $\mu(n)$ would satisfy the following:
$\exists c \in N$ such that $\forall n_0 \in N$, $\exists n \geq n_0$ such that $\mu(n) \geq n^{-c}$.

Note the key difference from a noticeable function - a non-negligible function only needs to have one $n \geq n_0$ for which $\mu(n) \geq n^{-c}$, whereas a noticeable function must satisfy this for *any* $n \geq n_0$.

For example, if we take any noticeable function and any negligible function and interleave them, then the resulting function will be non-negligible and non-noticeable. A concrete example is:

$$\mu(n) = \begin{cases} 2^{-n} & : x \texttt{ is even} \\ n^{-3} & : x \texttt{ is odd} \end{cases}$$

The function cannot be negligible, because for any odd integer, the function is only polynomially small, but it is not noticeable either, because for any even integer, it is exponentially small.

1.3 Sum of Negligible Functions

The sum of two negligible functions f and g is still negligible. Intuitively, even if you add two functions that are exponentially small, that cannot give a function that is polynomially small, and so the sum is still negligible.

Theorem 1 *If $f(n)$ and $g(n)$ are two negligible functions, then their sum $h(n) = f(n) + g(n)$ is also negligible.*

Main Idea: To show that $h(n) \leq n^{-c}$, we make use of the fact that $f(n), g(n) \leq n^{-(c+1)}$ since they are negligible. Adding two things that are $\leq n^{-(c+1)}$ must be smaller than n^{-c}.

Proof. We need to show that for any $c \in N$, we can find n_0 such that $\forall n \geq n_0$, $h(n) \leq n^{-c}$. So, consider an arbitrary $c \in N$.

Then, since $c + 1 \in N$, and since f and g are negligible, there exists n_f and n_g such that:
$\forall n \geq n_f$, $f(n) \leq n^{-(c+1)}$ and $\forall n \geq n_g$, $g(n) \leq n^{-(c+1)}$.

Choose $n_0 = \max(n_f, n_g, 2)$. Then, for any $n \geq n_0$, we have
$h(n) = f(n) + g(n) \leq n^{-(c+1)} + n^{-(c+1)} = 2n^{-(c+1)} \leq n \cdot n^{-(c+1)}$ (since $n \geq n_0 \geq 2$).
Thus $h(n) \leq n^{-c}$ and $h(n)$ is negligible. ■

Corollary 2 *If $f(n)$ is non-negligible and $g(n)$ is negligible, then $h(n) = f(n) - g(n)$ is non-negligible.*

Proof. If $h(n)$ was negligible, then $f(n) = g(n)+h(n)$ would be the sum of two negligible functions, but would be non-negligible, which is a contradiction. ■

2 Probabilistic Polynomial Time

A polynomial time Turing machine is one which halts in polynomial time for any input. A probabilistic Turing machine is allowed to make random choices in its execution.

Definition 3 (Probabilistic Polynomial Time) *A Turing machine M is a PPT (Probabilistic Polynomial Time) Turing Machine if $\exists c \in N$ such that $\forall x$, $M(x)$ halts in n^c steps.*

A *non-uniform* PPT Turing Machine is allowed to specify different machines for different input lengths, as opposed a single machine that must work for any input length:

Definition 4 (Non-uniform PPT) *A nu-PPT (non-uniform PPT) Machine is a sequence of probabilistic Turing Machines $\{M_1, M_2, \cdots\}$ such that $\exists c \in N$ such that $\forall x$, $M_{|x|}(x)$ halts in $(|x|)^c$ steps.*

3 One-way Function

3.1 An Attempt at a Definition

Intuitively, a one-way function is a function f that is easy to compute, but hard to invert. We formalize this by saying that there *cannot* exist a machine that can invert f in polynomial time.

Consider the following potential definition of a one-way function:

A function $f : \{0,1\}^n \to \{0,1\}^m$ is one-way if and only if $\exists$ PPT M such that $\forall x$ $M(x) = f(x)$, and $\forall$ non-uniform PPT A we have that $\underset{x \overset{\$}{\leftarrow} \{0,1\}^n}{Pr} [A(f(x)) \in f^{-1}(f(x))] = neg(|x|) = neg(n)$.

Note that in this definition, $f^{-1}(y)$ is the set of all values of x such that $f(x) = y$. The notation $x \overset{\$}{\leftarrow} \{0,1\}^n$ means that x is drawn uniformly at random from the set $\{0,1\}^n$.

x must have been drawn uniformly at random because otherwise the adversary could optimize the machine A to work for those values of x that are common. In the extreme case where x is not random and is always a specific value x_0, the machine A would be a machine that always outputs x_0, which would then always break the function f (regardless of what f is).

3.2 Problem - What if $m << n$?

This definition has a problem - the adversary A is given $f(x)$ as an input, which is only m bits long. So, the adversary only gets time polynomial in m in order to invert f to recover an n bit value of x. This is especially problematic if m is exponentially smaller than n.

As a concrete example, consider the function $f(x) = |x|$. In this example, we have $m = \log_2 n$, or $n = 2^m$. Obviously f should not be considered a one-way function, because it is very easy to invert f - given a value y, any x of length y would satisfy $x \in f^{-1}(y)$. (For example, `00000` $\in f^{-1}($`101`$)$.) However, the adversary gets an input of size m bits, and so only gets time polynomial in m to find a valid x. But since each possible x is of size $n = 2^m$, the adversary doesn't even have enough time to write down the answer! Thus, according to the flawed definition above, f would be a one-way function.

3.3 A Better Definition

We can fix this by providing the attacker 1^n (n repetitions of the 1 bit) as input. This means that the attacker gets $f(x)$ and 1^n as input for a total of $m + n$ bits. So, the attacker gets time polynomial in $m + n$ in order to invert $f(x)$, which prevents the issue above.

Definition 5 (One-way Function) *A function $f : \{0,1\}^n \to \{0,1\}^m$ is one-way if and only if $\exists$ polynomial-time M such that $\forall x$ $M(x) = f(x)$, and $\forall$ non-uniform PPT A we have that* $\underset{x \overset{\$}{\leftarrow} \{0,1\}^n}{Pr} [A(f(x), 1^n) \in f^{-1}(f(x))] = neg(|x|) = neg(n)$

3.4 A Potential One-way Function

It is not known whether one-way functions exist. The existence of one-way functions would imply that $P \neq NP$, and so of course we do not know of any concrete functions that have been proved to be one-way.

However, there are candidates for functions that could be one-way functions. One example is based on the hardness of factoring. Multiplication can be done easily in $O(n^2)$ time, but so far no polynomial time algorithm is known for factoring.

One candidate might be to say that given an input x, split x into its left and right halves x_1 and x_2, and then output $x_1 \times x_2$. However, this is not a one-way function, because with probability $\frac{3}{4}$, 2 will be a factor of $x_1 \times x_2$, and in general the factors are small often enough that a non-negligible number of the outputs could be factored in polynomial time.

To improve this, we again split x into x_1 and x_2, and use x_1 and x_2 as seeds in order to generate large primes p and q, and then output pq. Since p and q are primes, it is hard to factor pq, and so it is hard to retrieve x_1 and x_2. This function is believed to be one-way.

4 Modifying One-way Functions

4.1 Fixing Certain Values of a One-way Function

Consider having a one-way function f. Can we use this function f in order to make a one-way function g such that $g(x_0) = y_0$ for some constants x_0, y_0, or would this make the function no longer be one-way?

Intuitively, the answer is yes - we can specially set $g(x_0) = y_0$, and otherwise have $g(x) = f(x)$. In this case, the adversary gains the knowledge of how to invert y_0, but that will only happen with negligible probability, and so the function is still one-way.

Theorem 3 *Given a one-way function $f : \{0,1\}^n \to \{0,1\}^m$ and constants $x_0 \in \{0,1\}^n$, $y_0 \in \{0,1\}^m$, $\exists g : \{0,1\}^n \to \{0,1\}^m$ such that $g(x_0) = y_0$ where g is a one-way function.*

The proof is given in the appendix.

However, this raises an apparent contradiction - according to this theorem, given a one-way function f, we could keep fixing each of its values to 0, and it would continue to be a one-way function. If we kept doing this, we would eventually end up with a function which outputs 0 for *all* of the possible values of x. How could this still be one-way?

The resolution of this apparent paradox is by noticing that a one-way function is only required to be one-way in the limit where n grows very large. So, no matter how many times we fix the values of f to be 0, we are still only setting a finite number of x values to 0. However, this will still satisfy the definition of a one-way function - it is just that we will have to use larger and larger values of n_0 in order to prove that the probability of breaking the one-way function is negligible.

4.2 Composing One-way Functions

We might ask, given a one-way function $f : \{0,1\}^n \to \{0,1\}^n$, is the function $f^2(x) = f(f(x))$ also a one-way function? Intuitively, it seems that if it is hard to invert $f(x)$, then it would be just as hard to invert $f(f(x))$. However, this is actually wrong - it is possible that $f(f(x))$ actually can be inverted.

Proof. In order to demonstrate this, we first show the following lemma:

Lemma 4 *If $f : \{0,1\}^n \to \{0,1\}^n$ is a one-way function, then $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined as $g(x) = 0^n \mid\mid f(x_{[1:n]})$ is also one-way.*

Proof. Assume towards contradiction that g is not one-way, and so there is an adversary A_g that inverts g with probability $\mu(2n)$ that is non-negligible.

Note that $\mu(2n)$ is also non-negligible with respect to inputs of size n.

Then we can define an adversary A_f such that $A_f(y) = (A_g(0^n \mid\mid y))_{[1:n]}$. Note that A_g breaks g on input $0^n \mid\mid y \implies A_f$ breaks f on input y, and so A_f breaks f with at least non-negligible probability $\mu(2n)$. Contradiction.

Thus, g is also one-way. ■

Now, given a function $f : \{0,1\}^n \to \{0,1\}^n$, we can construct a new one-way function $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$. From g, we can construct another one-way function $h : \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined by:

$$h(x) = \begin{cases} 0^{2n} & : x_{[1:n]} = 0^n \\ g(x) & : otherwise \end{cases}$$

A generalization of the previous theorem (fixing values in a one-way function) shows that h is also a one-way function. (In short, we are only fixing the values of $\frac{2^n}{2^{2n}} = \frac{1}{2^n}$ of all of the possible values of x. Since we are only fixing a negligible fraction of the possible values of x, the same proof with slight modifications still applies.)

So, h is a one-way function. However, $h^2(x) = h(h(x)) = 0^{2n}$, and so h^2 is clearly not a one-way function. Thus, composing one-way functions is not guaranteed to give another one-way function. ■

5 Appendix

5.1 Proof: 2^{-n} is negligible

Main Idea: Just use the definition of a negligible function. As long as we choose a large enough n_0 given a specific c, 2^{-n} will be sufficiently small since exponentials drop off faster than polynomials.

Proof. Consider the function $\mu(n) = 2^{-n}$ and an arbitrary $c \in N$.

Then we can choose $n_0 = c^2$.

Then, for any $n \geq n_0$, we have $2^{-n} = (2^{\log_2 n})^{-\frac{n}{\log_2 n}} = n^{-\frac{n}{\log_2 n}}$

Since $n \geq n_0$, we know $\frac{n}{\log_2 n} \geq \frac{n_0}{\log_2 n_0} \geq \frac{n_0}{\sqrt{n_0}} = \sqrt{n_0} = c$ (since $n_0 = c^2$).

Thus $\mu(n) = 2^{-n} = n^{-\frac{n}{\log_2 n}} \leq n^{-c}$.

So, we have proved that for any $c \in N$, there exists $n_0 \in N$ such that for any $n \geq n_0$, $\mu(n) \leq n^{-c}$.

Hence, $\mu(n) = 2^{-n}$ is negligible. ■

5.2 Proof: Fixing a Value in a One-way Function

Theorem 5 *Given a one-way function $f : \{0,1\}^n \to \{0,1\}^m$ and constants $x_0 \in \{0,1\}^n$, $y_0 \in \{0,1\}^m$, $\exists g : \{0,1\}^n \to \{0,1\}^m$ such that $g(x_0) = y_0$ where g is a one-way function.*

Main Idea: Set g to be f, except at x_0, where $g(x_0) = y_0$. If there exists an adversary that can break g, then that adversary will also break f, because the adversary can only know negligibly more information about g than f.

Proof. Define the function g as follows:
$g(x) = \begin{cases} y_0 & : x = x_0 \\ f(x) & : x \neq x_0 \end{cases}$
Suppose there is an adversary A that can break g with non-negligible probability $\mu(n)$.

So, we have $\mu(n) = \underset{x \overset{\$}{\leftarrow} \{0,1\}^n}{Pr}[A(g(x)) \in g^{-1}(g(x))] = \sum\limits_{x \in \{0,1\}^n} Pr(X = x)Pr[A(g(x)) \in g^{-1}(g(x))]$

Since x is uniformly distributed, $Pr[X = x] = \frac{1}{2^n}$. We can split it into the cases $x : g(x) = y_0$ and $x : g(x) \neq y_0$:

$$\mu(n) = \left[\frac{1}{2^n} \sum_{x \in \{0,1\}^n, g(x) = y_0} Pr[A(y_0) \in g^{-1}(y_0))]\right] + \left[\frac{1}{2^n} \sum_{x \in \{0,1\}^n, g(x) \neq y_0} Pr[A(g(x)) \in g^{-1}(g(x))]\right].$$

Let $p = |\{x : g(x) = y_0\}|$. Consider the adversary M where $M(y) = x_1$ for any y, where x_1 is a value of x where $f(x_1) = y_0$. Thus, M breaks f for any input where $f(x) = y_0$, of which there are $p - 1$ or p (depending on whether $f(x_0) = y_0$). So, the probability with which M breaks f is $\frac{p-1}{2^n}$ or $\frac{p}{2^n}$. Either way, since f is a one-way function, this implies that $\frac{p}{2^n}$ is a negligible function.

Now, since $Pr[A(y_0) \in g^{-1}(g(x_0))] \leq 1$, we have:

$$\mu(n) \leq \frac{p}{2^n} + \sum_{x \in \{0,1\}^n, g(x) \neq y_0} Pr[A(g(x)) \in g^{-1}(g(x))]$$

Notice that for any x such that $g(x) \neq y_0$, we have $f(x) = g(x)$ and $f^{-1}(f(x)) = g^{-1}(g(x))$.

So $\mu(n) \leq \frac{p}{2^n} + \frac{1}{2^n} \sum\limits_{x \in \{0,1\}^n, g(x) \neq y_0} Pr[A(f(x)) \in f^{-1}(f(x))]$

Thus, if we consider A as an adversary for f, then we get:

$$\underset{x \overset{\$}{\leftarrow} \{0,1\}^n}{Pr}[A(f(x)) \in f^{-1}(f(x))] \geq \frac{1}{2^n} \sum_{x \in \{0,1\}^n, g(x) \neq y_0} Pr[A(f(x)) \in f^{-1}(f(x))] \geq \mu(n) - \frac{p}{2^n}$$

$\mu(n)$ is non-negligible and $\frac{p}{2^n}$ is negligible, and so, $\mu(n) - \frac{p}{2^n}$ is non-negligible. Thus A is an adversary that breaks f with non-negligible probability. ■