CS 687 Cryptography February 19, 2008

Lecture 8: Pseudo Randomness and the Next-bit test

Instructor: Rafael Pass *Scribe: Anuradha Patil*

1 Review

In the last lecture we learnt about Computational Indistinguishability and the Next Bit test. Let us now put down the informal definitions :

Definition 1 *An ensemble* $\{X_n\}$ *is pseudorandom* $\iff \{X_n\} \approx \{Uniform\ Distribution\}$.

Definition 2 *An ensemble* $\{X_n\}$ *passes the Next Bit test* $\iff \forall$ *PPT A,* $\exists$ *a negligible function* ϵ *such that for every* $n \in N$*,*

$$\Pr[t \leftarrow X_n : A(t_{1\to i}) = t_{i+1}] \le \frac{1}{2} + \epsilon(n) \tag{1}$$

2 Pseudorandomness and Next Bit test

Theorem 1 $\{X_n\}$ *is pseudorandom* $\iff \{X_n\}$ *passes the Next Bit test.*

Proof.

One direction is simple. If $\{X_n\}$ is pseudorandom, then by definition itself it passes the Next Bit test. We have to now prove the other direction.

Assume that $\{X_n\}$ passes the next Bit test but is not pseudorandom. This implies that $\exists$ a distinguisher D, a polynomial $p(n)$ such that for infinitely many n,

$$|\Pr[t \leftarrow X_n : D(t) = 1] - \Pr[t \leftarrow U_n : D(t) = 1]| \ge \frac{1}{p(n)} \tag{2}$$

Let $\mathrm{H}_i = \{l \leftarrow X_n; r \leftarrow \{0,1\}^n : l_{1\to i}||r_{i+1\to n}\}$

Then, $H_0 = U_n$ and $H_n = X_n$

$\implies$ there exist H_i and H_{i+1} such that

$$|\Pr[t \leftarrow H_i : D(t) = 1] - \Pr[t \leftarrow H_{i+1} : D(t) = 1]| \ge \frac{1}{nq(n)} \tag{3}$$

Let $H'_{i+1} = \left\{t \leftarrow X_n; r \leftarrow \{0,1\}^n : l_{1\to i}||l'_{1\to i}||r_{i+2\to n}\right\}$

The intuition behind this is that if $H_i \not\approx H_{i+1}$ then $H_{i+1} \not\approx H'_{i+1}$

$\Longrightarrow$ Distinguisher D can guess the right bit (at the $i+1^{th}$) position more often than not. We now construct a machine A such that it distinguishes between these two bits.

$A(y)$

- Pick $r \leftarrow \{0,1\}^n$
- If D $(y||r_{i+1\to n})$, output r_{i+1}
- Otherise output r'_{i+1}

Now,

$\Pr[t \leftarrow X_n : A(\mathrm{t}_{i+1}) = t_{i+1}]$ = Probability that A guessed bit correctly + Probability that A didn't guess correctly

$= \left(\frac{1}{2}\right) \Pr[t \leftarrow \mathrm{H}_{i+1}\text{:D(t)=1}] + \left(\frac{1}{2}\right) \Pr[t \leftarrow \mathrm{H}'_{i+1}\text{:D(t)} \neq 1]$

$= \left(\frac{1}{2}\right) \Pr[t \leftarrow \mathrm{H}_{i+1}\text{:D(t)=1}] + \left(\frac{1}{2}\right) (1 - \Pr[t \leftarrow \mathrm{H}'_{i+1}\text{:D(t)=1}]\ )$

$= (\frac{1}{2})+(\frac{1}{2})(\Pr[t \leftarrow \mathrm{H}_{i+1}\text{:D(t)=1}] - \Pr[t \leftarrow \mathrm{H}'_{i+1}\text{:D(t)=1}]\ )$

$\leq \Pr[[t \leftarrow \mathrm{H}_{i+1}\text{:D(t)=1}] - \Pr[t \leftarrow \mathrm{H}_i\text{:D(t)=1}]$

Definition 3 $G : \{0,1\}^* \to \{0,1\}^*$ *is a Pseudorandom generator iff*

- *G is a PPT.*
- *Expansion :* $|G(x)| > |x|$
- $\{x \leftarrow \{0,1\}^n : G(x)\} \approx \left\{U^{|G(x)|}\right\}$

Definition 4 *A predicate* $b : \{0,1\}^* \to \{0,1\}$ *is a hard-core with respect to function f if and only if*

- *b is a PPT.*
- $\forall$ *PPT A,* $\exists$ *a negligible function* ϵ *such that*

$$\Pr[x \leftarrow \{0,1\}^n : A(f(x), 1^n) = b(x)] \leq \frac{1}{2} + \epsilon(n) \tag{4}$$

Claim 1 *f is a One Way Permutation and b is the hard-core bit of f. G(s) = f(s)b(s) is a PRG.*

Proof.

From its definition, we can see that G(s) is efficient. It can be computed in PPT. Also, the output of G(s) is greater than the input, by atleast one bit, b(s), i.e., $|G(s)| > |s|$.

Also, $\{s \leftarrow \{0,1\}^n : f(s)\} = U^{|f(s)|}$ And, b(s) passes the Next bit test by definition, and is hence random.

Thus, $\{s \leftarrow \{0,1\}^n : f(s)||b(s)\} \approx \left\{U^{|f(s)|}\right\}$ Hence, G is a PRG.