Foundations of Cryptography

Oded Goldreich and Shafi Goldwasser

Exercise 2: Pseudorandom generators and pseudorandom functions

Due date: 10 Jan. 2002

1. Let $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ be two ensembles that are polynomial-time indistinguishable.
   (a) For any probabilistic polynomial-time algorithm A, prove that the ensembles $\{A(X_n)\}_{n\in\mathbb{N}}$ and $\{A(Y_n)\}_{n\in\mathbb{N}}$ are polynomial-time indistinguishable. That is, computational indistinguishability is preserved under efficient transformations.
   (b) Show that if A is not polynomial-time then $\{A(X_n)\}_{n\in\mathbb{N}}$ and $\{A(Y_n)\}_{n\in\mathbb{N}}$ are NOT necessarily polynomial-time indistinguishable.
   (c) Prove that for every $L \in \mathcal{BPP}$, the function
   $$\Delta_L(n) \stackrel{\text{def}}{=} |\Pr[X_n \in L] - \Pr[Y_n \in L]|$$
   is negligible in n.

2. (a) Assuming that one-way permutation exist, prove that there exists a pseudorandom generator G and an efficiently computable function h such that $h \circ G$ is one-to-one and length-preserving (where $(h \circ G)(x) = h(G(x))$).
   Hint: Recall the construction of pseudorandom generators from one-way permutations.
   (b) Show that if pseudorandom generators exists then there exists a pseudorandom generators G such that the mapping $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is NOT one-to-one.

3. (a) Prove that for every pseudorandom generator G, the set $L_G = \{G(s) : s \in \{0,1\}^*\}$ is in NP.
   (b) Does there exist a pseudorandom generator G such that L_G is in co-NP, under reasonable assumptions?
   Hint: Use part 2a.

continued...

4. (a) Prove that one-way functions assign a negligible probability mass to any string. That is, if f is a one-way function then for every positive polynomial p and all sufficiently large n and α, $\Pr[f(U_n)=\alpha] < 1/p(n)$.

   (b) Prove that pseudorandom generators assign a negligible probability mass to any string. That is, if G is a pseudorandom generator then for every positive polynomial p and all sufficiently large n and α, $\Pr[G(U_n)=\alpha] < 1/p(n)$.

   (c) Prove that pseudorandom functions ensembles assign a negligible probability to functions that assign a non-negligible probability to some string. That is, if $\{f_s\}_s$ is an ensemble of pseudorandom functions then for every positive polynomial p and all sufficiently large s:

$$\Pr_{s\in\{0,1\}^n}\left[\exists\alpha \text{ s.t. } \Pr_{x\in\{0,1\}^{\ell(n)}}[f_s(x)=\alpha] > 1/p(n)\right] < 1/p(n)$$

5. *Failure of an alternative construction of pseudorandom functions from pseudorandom generators*: Let G be a pseudorandom generator with an expansion function $\ell(n)=2n$. Consider a construction of a function ensemble where the functions in F_n are defined as follows. For every $s\in\{0,1\}^n$, the function f_s is defined so that

$$f_s(x) \stackrel{\text{def}}{=} G_{\sigma_n}(\cdots(G_{\sigma_2}(G_{\sigma_1}(x))\cdots)$$

   where $s=\sigma_1\cdots\sigma_n$ and G_σ is as in the construction shown in class. Namely, the roles of x and s are switched compared to the construction shown in class (i.e., the root of the tree is labeled by x, and the value of f_s on x is obtained by following the path corresponding to the index s). Prove that the resulting function ensemble is not necessarily pseudorandom.

   Hint: Show, first, that if pseudorandom generators exist then there exists a pseudorandom generator G satisfying $G(0^n)=0^{2n}$.

Questions may be directed to Oded Goldreich `<oded@wisdom.weizmann.ac.il>` or Eran Tromer `<tromer@wisdom.weizmann.ac.il>`.