Introduction to Computational Complexity - Assignment 5

To be submitted by 18/5/2008

We recall some definitions from class.

Definition 1. For any string $x \in \{0,1\}^n$ we denote by $F_i(x)$ the length i prefix of x, that is, $F_i(x) = x_1x_2\ldots x_i$.

Definition 2. The probability ensemble $\{X_n\}_n$ is polynomial-time samplable if there exists a probabilistic polynomial time A such that for every n, the output distribution of $A(1^n)$ is exactly the same distribution as X_n.

Definition 3. The probability ensemble $\{X_n\}_n$ is unpredictable if for every probabilistic polynomial-time algorithm P, every positive polynomial p and all sufficiently large n it holds that

$$\Pr_{i\in[n]}\left[P\left(n, F_{i-1}(X_n)\right) = (X_n)_i\right] \leq \frac{1}{2} + \frac{1}{p(n)}$$

Finally, recall that in class, Zvika suggested the following definition for unpredictability:

Definition 4. The probability ensemble $\{X_n\}_n$ is Zvika-unpredictable if for every probabilistic polynomial-time algorithm P, every positive polynomial p , all sufficiently large n and all $i \in [n]$ it holds that

$$\Pr\left[P\left(n, F_{i-1}(X_n)\right) = (X_n)_i\right] \leq \frac{1}{2} + \frac{1}{p(n)}$$

1 Indistinguishability versus Unpredictability

Recall that in class we started to show the proof that if an ensemble $\{X_n\}_n$ is unpredictable then it is pseudorandom. The goal of this question is to complete the proof. Suppose that $\{X_n\}_n$ is not pseudorandom, that is, there exists some probabilistic polynomial-time algorithm D and some positive polynomial p such that for infinitely many n's:

$$\Pr\left[D\left(X_n\right) = 1\right] - \Pr\left[D\left(U_n\right) = 1\right] \geq \frac{1}{p(n)}$$

where U_n is the uniform ensemble. Then, we showed, using an hybrid argument, that for infinitely many n's:

$$\Pr_{i\in[n]}\left[D\left(F_i\left(X_n\right) \circ U_{n-i}\right) = 1\right] - \Pr_{i\in[n]}\left[D\left(F_{i-1}(X_n) \circ U_{n-i+1}\right) = 1\right] \geq \frac{1}{n \cdot p(n)}$$

Finally, we defined the following predictor P for X_n: When given as input $n \in \mathbb{N}$ and a string x of length $i-1$ (where $i \in [n]$), the predictor P chooses a bit $\sigma \in \{0,1\}$ and another string $u \in \{0,1\}^{n-i}$ uniformly at random. Then, P outputs σ if $D(x \circ \sigma \circ u) = 1$ and outsputs $\overline{\sigma}$ otherwise (where $\overline{\sigma}$ is the complement of σ).

The exercise is to prove that P is a good predictor for X_n, that is, for infinitely many n's it holds that

$$\Pr_{i\in[n]}\left[P\left(n, F_{i-1}(X_n)\right) = (X_n)_i\right] \geq \frac{1}{2} + \frac{1}{n \cdot p(n)}$$

2 Unpredictability versus Zvika-Unpredictability

In this part of the exercise we will examine the relations between unpredictability and Zvika-unpredictability.

1. Prove that if an ensemble $\{X_n\}_n$ is Zvika-unpredictable then it is also unpredictable.

2. Prove that if an ensemble $\{X_n\}_n$ is unpredictable with respect to *polynomial-size circuits* (rather than probabilistic polynomial-time algorithms) then it is also Zvika-unpredictable with respect to polynomial-size circuits.
   Note that the other direction can be proved using exactly the same proof as the previous question.

3. Prove that if an ensemble $\{X_n\}_n$ is *polynomial-time samplable* and unpredictable then it is also Zvika-unpredictable.

   Hint The argument is somewhat related to the analysis we have shown in class two weeks ago, of the algorithm A_G which combines a probabilistic algorithm A and a pseudorandom generator G.

Bonus Prove that there exists an ensemble $\{X_n\}_n$ which is unpredictable but not Zvika-unpredictable. You may use the fact that, for any unbounded and monotonically non-decreasing function f (e.g. $f(n) = \log n$), there exists a pseudorandom ensemble $\{Z_n\}_n$ (which is not polynomial-time samplable), such that for every n the distribution Z_n has support of size at most $f(n)$.