Summary of Recitation, and New Homework

November 21, 2012

In class we discussed the following problem:

> Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a prg. Denote by $G_L(x)$ the n left bits of $G(x)$, and by $G_R(x)$ the n right bits of n. Then $G'(x) = G_L(x) \mid G(G_R(x))$ is a prg that expands an n bit seed to a $3n$ bit output.

The proof uses the following hybrids:

- $f_0 = z$, where z is sampled uniformly at random from $\{0,1\}^{3n}$.
- $f_1 = x \mid G(y)$, where x and y are each sampled uniformly at random from $\{0,1\}^n$.
- $f_2 = G_L(x) \mid G(G_R(x))$, where x is sampled uniformly at random from $\{0,1\}^n$.

Note that $f_0(x)$ is uniformly random, whereas f_2 has the same distribution as the output of $G'()$. The proof must show that if there is a polynomial time distinguisher D' which distinguishes between f_0 and f_2 then there is a polynomial time distinguisher D that distinguishes between the output of G and a random string of length $2n$.

We showed in class that if there exists such a D' distinguishing between f_0 and f_2, then at least one of the following two distinguishers exists

- A distinguisher D_{01} which distinguishes between f_0 and f_1.
- A distinguisher D_{12} which distinguishes between f_1 and f_2.

Homework:

1. Show that if D_{01} exists then there is a distinguisher D that distinguishes between the output of G and a uniformly random string of length $2n$.
2. Show the same with relation to D_{12}. That is, show that if D_{12} exists then there is a distinguisher D that distinguishes between the output of G and a uniformly random string of length $2n$.