Homework 2

February 2, 2004

This problem set is due in class on **Monday, February 9.**

1 Indistinguishability and guessing

Recall that the distributions D_0, D_1 are said to be (t, ϵ)-indistinguishable (for $0 \leq \epsilon \leq 1$) if

$$|\Pr[A(x_0) = 1] - \Pr[A(x_1) = 1]| \leq \epsilon$$

holds for all adversaries A running in time at most t, where the random variable x_0 is distributed according to D_0 and x_1 is distributed like D_1.

Now, let's call the distributions D_0, D_1 (t, ϵ)-*inseparable* just if

$$\frac{1}{2} - \frac{\epsilon}{2} \leq \Pr_{b,x}[A(x) = b] \leq \frac{1}{2} + \frac{\epsilon}{2}$$

holds for all adversaries A running in time at most t, where the random variable b is a uniformly random bit and where the random variable x is distributed according to D_b. This is a very natural notion, because it talks about our chances of guessing correctly which distribution x came from, and whether we can do much better than simply flipping a coin.

Prove: D_0, D_1 are (t, ϵ)-indistinguishable if and only if they are (t, ϵ)-inseparable. (Hence the notion of inseparability is redundant.)

2 Bigger PRG's

Let $G^{(1)} : \{0,1\}^k \to \{0,1\}^{2k}$ be a length-doubling PRG. Define $G^{(2)} : \{0,1\}^k \to \{0,1\}^{4k}$ by $G^{(2)}(x) = (G^{(1)}(y), G^{(1)}(z))$ where $(y, z) = G^{(1)}(x)$, $G^{(3)} : \{0,1\}^k \to \{0,1\}^{8k}$ by $G^{(3)}(x) = (G^{(2)}(y), G^{(2)}(z))$ where $(y, z) = G^{(1)}(x)$, and so on.

Fill in the blanks to make the following a true statement, and then prove it: If $G^{(1)}$ is a (t, ϵ)-PRG, then $G^{(n)}$ is a $(\_\_\_, \_\_\_)$-PRG.