Composition of Two PRGs

Somesh Jha

October 20, 2020

Let G and F be psuedorandom generators (PRGs) with expansion factor $l(n) = 2n$. We will sketch a proof that $F \circ G$ (composition of F and G is a PRG). Note that $F \circ G$ has expansion factor $4n$). You will complete the proof in the homework, but I will sketch it here.

Let us consider the two worlds.

World 0: We generate a n-bit random seed s and are given $F(G(s))$ (note that this has length $4n$, which is the length of the string r in world 1.)

World 1: We are given a uniform bit string r of length $4n$.

Let D be a PPTA distinguisher, which outputs 1 if it thinks it is in world 0.

Intermediate world: We will create an intermediate world, called *world I*. In this world, we generate a $2n$-bit random string z and provide $F(z)$ to the distinguisher, which is again a $4n$-bit string.

Step 1 (difference between world 1 and I): Argue the following (where negl_1) is a negligible function).

$$|P(D(r) = 1) - P(D(F(z)) = 1)| \quad \leq \quad \text{negl}_1(n)$$

Step 2 (difference between world I and 0: Argue the following (where negl_2) is a negligible function).

$$|P(D(F(z)) = 1) - P(D(F(G(s))) = 1)| \quad \leq \quad \text{negl}_2(n)$$

Step 3: Recall the triangle inequality $|a - c| + |c - b| \;\geq\; |a - b|$. Use what you proved in steps 1 and 2 and prove the following:

$$|P(D(r) = 1) - P(D(F(G(s))) = 1)| \quad \leq \quad \text{negl}_1(n) + \text{negl}_2(n)$$

Since the sum of two negligible functions is negligible, we just proved that $F \circ G$ is a PRG.

Note: This technique of creating ”intermediate” worlds and then using the triangle inequality to bound the probability is called the *hybrid argument* in cryptography (I guess because we are creating hybrid “intermediate” worlds, but I am not sure).