CS59200-PRS: Pseudorandomness

Assignment 3 *Due: Dec 1*

Problem 1 (Pseudo-entropy Generator) [10 pts]. In this problem we examine a key component of Håstad-Impagliazzo-Levin-Luby, and prove a weaker statement that the existence of *injective* one-way functions implies the existence of cryptographic PRGs.

We call a function $G\colon \{0,1\}^\ell \to \{0,1\}^n$ a *k-pseudo-entropy generator* for $\ell \le k \le n$, if G can be computed in $\mathrm{poly}(n)$ time, and there exists a distribution X over $\{0,1\}^n$ with $H_\infty(X) \ge k$ such that:

- X is efficiently samplable: there exists $N \le \mathrm{poly}(n)$ and a function $H\colon \{0,1\}^N \to \{0,1\}^n$ computable in $\mathrm{poly}(n)$ time, such that $H(y)$ has the same distribution as X for y uniformly drawn from $\{0,1\}^N$.
- $G(U_\ell)$ and X is indistinguishable: that is,

$$\left| \mathop{\mathbb{E}}_{s\sim\{0,1\}^\ell}[A(G(s))] - \mathop{\mathbb{E}}_{x\sim X}[A(x)] \right| \le \mathrm{negl}(n)$$

  for every $\mathrm{poly}(n)$-time distinguisher A.

1. **[2 pt].** Let $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be an explicit (k,ε)-extractor for some $\varepsilon \le \mathrm{negl}(n)$. Show that, if $G\colon \{0,1\}^\ell \to \{0,1\}^n$ a k-pseudo-entropy generator, then $G'\colon \{0,1\}^{\ell+d} \to \{0,1\}^m$ defined as

$$G'(s,r) = \mathrm{Ext}(G(s),r)$$

   is a cryptographic pseudorandom generator.

2. **[3 pt].** Let $a \le b$, and suppose $F\colon \{0,1\}^a \to \{0,1\}^b$ is an one-way function that is injective. Prove that $G\colon \{0,1\}^{2a} \to \{0,1\}^{a+b+1}$ defined as

$$G(s,r) = (F(s), r, \langle s,r\rangle), \quad s,r \in \{0,1\}^a$$

   is a $(2a+1)$-pseudo-entropy generator.

   Hint. Follow the proof of the Blum-Micali generator. You will need to modify the Goldreich-Levin proof from class a little bit.

3. **[3 pt].** Suppose $G\colon \{0,1\}^\ell \to \{0,1\}^n$ is an $(\ell+1)$-pseudo-entropy generator. Prove that for every $t \le \mathrm{poly}(n)$, the direct product $G^{\otimes t} : \{0,1\}^{t\ell} \to \{0,1\}^{tn}$, defined as

$$G^{\otimes t}(s_1,\ldots,s_t) = (G(s_1),\ldots,G(s_t))$$

   is an $(t\ell+t)$-pseudo-entropy generator.

Hint. Use a hybrid argument.

4. **[2 pt].** Use the claims above to conclude that if there exist injective one-way functions, there must exist non-trivial cryptographic PRGs.

   Hint. Here non-trivial means that the output length of the PRG needs to be larger than the seed length. Use one of the explicit extractor constructions from class to get the proper parameters.