Notes for Lecture 13 (Draft)

Summary

Today we complete the proof that it is possible to construct a pseudorandom generator from a one-way permutation

1 Pseudorandom Generators from One-Way Permutations

Last time we proved the Goldreich-Levin theorem.

Theorem 1 (Goldreich and Levin) *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a (t, ϵ)-one way permutation computable in time $r \leq t$. Then the predicate $x, r \to \langle x, r \rangle$ is $(\Omega(t \cdot \epsilon^2 \cdot n^{-O(1)}, 3\epsilon)$ hard core for the permutation $x, r \to f(x), r$.*

A way to look at this result is the following: suppose f is $(2^{\Omega(n)}, 2^{-\Omega(n)})$ one way and computable in $n^{O(1)}$ time. Then $\langle x, r \rangle$ is a $(2^{\Omega(n)}, 2^{-\Omega(n)})$ hard-core predicate for the permutation $x, r \to f(x), r$.

From now on, we shall assume that we have a one-way permutation $f : \{0,1\}^n \to \{0,1\}^n$ and a predicate $P : \{0,1\}^n \to \{0,1\}$ that is (t, ϵ) hard core for f.

This already gives us a pseudorandom generator with one-bit expansion.

Theorem 2 (Yao) *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a permutation, and suppose $P : \{0,1\}^n \to \{0,1\}$ is (t, ϵ)-hard core for f. Then the mapping*

$$x \to f(x), P(x)$$

is $(t - O(1), \epsilon)$-pseudorandom generator mapping n bits into $n + 1$ bits.

We will amplify the expansion of the generator by the following idea: from an n-bit input, we run the generator to obtain $n + 1$ pseudorandom bits. We output one of those $n + 1$ bits and feed the other n back into the generator, and so on. Specialized to above construction, and repeated k times we get the mapping

$$G_k(x) := P(x), P(f(x)), P(f(f(x)), \ldots, P(f^{(k-1)}(x), f^{(k)}(x) \tag{1}$$

Theorem 3 (Blum-Micali) *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a permutation, and suppose $P : \{0,1\}^n \to \{0,1\}$ is (t,ϵ)-hard core for f and that f, P are computable with complexity r.*

Then $G_k : \{0,1\}^n \to \{0,1\}^{n+k}$ as defined in (1) is $(t - O(rk), \epsilon k)$-pseudorandom.

Thinking about the following problem is a good preparation for the proof the main result of the next lecture.

Exercise 1 (Tree Composition of Generators) *Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a (t,ϵ) pseudorandom generator computable in time r, let $G_0(x)$ be the first n bits of the output of $G(x)$, and let $G_1(x)$ be the last n bits of the output of $G(x)$.*

Define $G' : \{0,1\}^n \to \{0,1\}^{4n}$ as

$$G'(x) = G(G_0(x)), G(G_1(x))$$

Prove that G' is a $(t - O(r), 3\epsilon)$ pseudorandom generator.