Exercise 2 : Topics in Pseudorandomness (Fall 2005-2006)

Ronen Shaltiel

December 13, 2005

1. ($(2,\epsilon)$-wise families of hash functions) Given a family H of functions $h : \{0,1\}^n \to \{0,1\}^m$ we consider the probability space of choosing a function $h \in_R H$ and for every $a \in \{0,1\}^n$ define a random variable $R_a = h(a)$. Recall that H is a 2-wise independent family of hash functions if for every $a_1 \neq a_2$ the pair (R_{a_1}, R_{a_2}) is distributed exactly like the uniform distribution on $\{0,1\}^{2m}$. We say that H is a $(2,\epsilon)$-wise family of hash functions if if for every $a_1 \neq a_2$ the pair (R_{a_1}, R_{a_2}) is ϵ-close to the uniform distribution on $\{0,1\}^{2m}$.

   (a) Show that for every n, m and ϵ there is an explicit family H that is of size $2^{O(m+\log n+\log(1/\epsilon))}$ (that is it takes seed $O(m + \log n + \log(1/\epsilon))$ to select a random hash function). Recall that it takes a seed of $2n$ to select a hash function for $\epsilon = 0$.

   Hint: You first need to realize that we've solved the case of $m = 1$ in class.

   (b) Conclude that for every $a_1 \neq a_2$, $\Pr[h(a_1) = h(a_2)] \leq 2^{-m} + \epsilon$.

2. (Existence of Pseudorandom generators) A function $G : \{0,1\}^d \to \{0,1\}^m$ is called a *generator* if $m > d$. We say that a generator G is ϵ-pseudorandom against a function $A : \{0,1\}^m \to \{0,1\}$ if

$$|\Pr_{x \leftarrow U_m}[A(x) = 1] - \Pr_{s \leftarrow U_d}[A(G(s)) = 1]| \leq \epsilon$$

   A generator is ϵ-pseudorandom against a class $\mathcal{A}$ of functions $A : \{0,1\}^m \to \{0,1\}$ if it is ϵ-pseudorandom against every $A \in \mathcal{A}$.

   (a) Show that for every class $\mathcal{A}$ which contains at most t functions, and every $\epsilon > 0$ there exists a pseudorandom generator with seed length $d = O(\log\log t + \log(1/\epsilon))$. (Hint: first consider the case $t = 1$. It is helpful to use use sampling and amplification).

   (b) (Existence of small ϵ-bias spaces) The class of linear tests is the class of all functions $A : \{0,1\}^m \to \{0,1\}$ such that there exists an $S \subseteq \{1, \cdots, m\}$ such that $A(x) = \oplus_{i \in S} x_i$. Show that for every $\epsilon > 0$ there is an ϵ-pseudorandom generator against linear tests with seed length $d = O(\log m + \log(1/\epsilon))$.

   (c) (Existence of small (k,ϵ)-wise spaces) The class of k-wise tests is the class of all functions $A : \{0,1\}^m \to \{0,1\}$ which depend on at most k input bits. Show that for every $\epsilon > 0$ there is an ϵ-pseudorandom generator against k-wise tests with seed length $d = O(k + \log\log m + \log(1/\epsilon))$.

   (d) (Existence of pseudorandom generators against circuits) The class of tests of size s is the class of all functions $A : \{0,1\}^m \to \{0,1\}$ which are computable by a boolean circuit of size s.[1]

[1] We haven't yet defined what this means. The only thing you need to know for this question is that the number of size s circuits is at most s^{2s}.

Show that for every $\epsilon > 0$ there is an ϵ-pseudorandom generator against tests of size s with seed length $d = O(\log m + \log s + \log(1/\epsilon))$.