Homework 4
Due 2006/7/1

Amnon Ta-Shma
Dept. of Computer Science
Tel Aviv University

Topic today: Extractors, generators and two questions about space bounded computations.

We say a generator $G : \{0,1\}^d \to \{0,1\}^m$ ε fools a predicate A, if

$$|\Pr_{x\in\{0,1\}^m}[A(x)=1] - \Pr_{y\in\{0,1\}^d}[A(G(y))=1]| \le \varepsilon.$$

We say G fools a class of predicates if it fools all memebers in the class.

1. Prove that for every $1 \le k \le n$ and every $1 \le m \le k+d-\log\log(\frac{1}{\varepsilon})-O(1)$ and $\varepsilon > 0$, there exists a (k,ε) disperser $F : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d \le \log(n-k)+\log(\frac{1}{\varepsilon})+O(1)$.

2. (ISW99, ISW00)

   For a predicate A on m bits, and $y \in \{0,1\}^m$, define a predicate $A^{\oplus y}$ on m bits by having $A^{\oplus y}(x) = A(x \oplus y)$. Define $A^{\oplus}$ to be the class of all predicates $A^{\oplus y}$.

   Suppose $P_1, \ldots, P_r$ are distributions on $\{0,1\}^m$ and A a predicate on $\{0,1\}^m$. Suppose one of the distributions P_i ε fools $A^{\oplus}$. Prove that $P = P_1 \oplus \ldots \oplus P_r$ ε–fools A, where P is the distribution obtained by sampling independently the distributions P_i and taking the xor of the samples.

3. (ISW99, ISW00) A (k,ε) extractor *scheme* is a function $G : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ such that:
   for every $f \in \{0,1\}^n$ and every predicate A on m bits,
   if G^f does not ε–fool A,
   then $K_A(f) \le k$.

   where $G^f : \{0,1\}^d \to \{0,1\}^m$ is defined by $G^f(y) = G(f,y)$, and $K_A(f)$ is the Kolmogorov complexity of the string f given free access to oracle calls to A.

   Prove that

   - A (k,ε) extractor scheme is a $(k+\log(1/\varepsilon), 2\varepsilon)$ extractor.
   - Any explicit (k,ε) extractor is a $(k+O(1),\varepsilon)$ extractor scheme.

4. Savitch sows that $NL \subseteq DSPACE(O(\log^2 n))$. Extend the argument to show that $BPL \subseteq DSPACE(O(\log^2 n))$.

5. Use Nisan's generator to show that $BPL \subseteq DTimeSPACE(poly(n), O(\log^2 n))$.