

Due on December 1, 2006
In class, at the beginning of the lecture

The work you submit must be your own. You may discuss problems with each other; however, you should prepare written solutions alone. In particular, you should not leave with any written notes from such discussions. The style and clarity of your answers will be an important factor in the grade.

This final assignment has just one question.

1. We say that a function $G : \{0, 1\}^t \rightarrow \{0, 1\}^m$ is a (s, ε) -pseudorandom generator if for every circuit D of size $\leq s$ we have

$$\left| \Pr_{r \in \{0,1\}^m} [D(r) = 1] - \Pr_{z \in \{0,1\}^t} [D(G(z)) = 1] \right| \leq \varepsilon$$

- (a) In a probabilistic algorithm $A(x, r)$, r is the output of a *random source*. A random source is an idealized device that outputs a sequence of bits that are uniformly and independently distributed.

Show that a language L is in **BPP** if there exists a polytime (in $|x|$) algorithm $A(x, r)$ such that

$$\Pr_r [A(x, r) = L(x)] \geq \frac{3}{4}.$$

- (b) Show that if there is a family of generators $G_m : \{0, 1\}^{O(\log(m))} \rightarrow \{0, 1\}^m$ that are computable in polytime in m (i.e., $1^m \mapsto G_m$ is polytime) and are $(2m, 1/8)$ -pseudorandom, then **P** = **BPP**.
- (c) Given a language $L \subseteq \{0, 1\}^*$, let L_n be its characteristic function on inputs of size n . Let $H(L_n)$ be the minimum s such that there is a circuit C of size s such that $\Pr_{x \in \{0,1\}^n} [C(x) = L_n(x)] \geq \frac{1}{2} + \frac{1}{s}$.

In this question you are asked to argue very informally; a few sentences explaining the plausibility of the following statement will do. *Suppose there is a language L in **E** and a $\delta > 0$ such that for all sufficiently large n , $H(L_n) \geq 2^{\delta n}$. Then, there is a family of generators G_m as in part (b).*