Recent advances in Complexity CIS 6930/CIS 4930	November 7, 2002
Lecture 22	
Lecturer: Dr. Meera Sitharam	Scribe: Hongyu Guo

Two corollaries follow from forward direction of the main theorem from Lecture 21 and the standard use of pseudo random generator for derandomization of a randomized algorithms A.

Corollary 1 *If EXPTIME cannot be approximated by polynomial size circuits, then* $BPP \subseteq \bigcap_{\epsilon>0} DTIME(2^{n^{\epsilon}})$.

Exercise 1 *Strenghen the antecedent of the above corollary enough so that consequence is "*$BPP \subseteq P$*".*

Corollary 2 $RAC^0 \subseteq \bigcup_c DSPACE((logn)^c) \subseteq \bigcup_c DTIME(2^{log^c n})$.

Proof. ($\Longleftarrow$ is left out.) (1) $\Longrightarrow$ (2) is easy using Yao's XOR lemma.

Exercise 2 *Yao's XOR lemma implies*
(1) $\Longrightarrow$ *(2):*
Let $s(t)$ *be any function such that* $l \leq s(l) \leq 2^l$. *If* $\exists$ *a function in EXPTIME that cannot be approximated by circuits of size* $s(l)$ *(in the weak sense), then for some* $c > 0$, $\exists$ *another function in EXPTIME whose hardness* $H_{f'}(l) \geq s(l^c)$. *(This is strong non-approximation ability.)*

(2) $\Longrightarrow$ (3):
There are two subparts of the proof here (two lemmas). The first subpart is the onstruction of pseudo random generator $G : l \longrightarrow s(l^c)$, where $l^c = n$, using a hard function f, by first constructing a $(logn, l^{1/2})$ design on $\{1, ..., l\}$, (Here $m = l^{1/2}$ and $k = logn$) and show the pseudo random generator safisfies condition c1. The second subpart is to show such a design exists.
For $x \in \{0,1\}^l$,
$G(x) = f(z_1), ..., f(x_n)$,
where z_i is te restriction of x to the indices in S_i.

Example 1 $x = 01110101$
$l = 8, S_i = \{1, 3, 5\}$
$z_i = 010$.

Subpart 1 If G is based on a $(logn, l^{1/2})$ design, then it is a pseudo random generator satisfying the bias requirement in the statement of the theorem. This is Lemma 3 stated in Lecture 21.

Subpart 2 $(logn, l^{1/2})$ design exists and can be constructed in $DTIME(2^l)$, where $n = s(l^c)$. This will be Lemma 4 stated in the next lecture.

Aside Sitharam'93 has a 2 line proof of subpart 1 using Fourier transforms of Abelian groups showing relations between pseudorandom generators and learning algorithms of sampling.

Proof of Subpart 1 Proof by contradiction. Assume such a pseudorandom generator G based on the $(logn, l^{1/2})$ design does not satisfy condition c1.

......

■