18.405J/6.841J Advanced Complexity Theory April 20, 2000

Lecture 20 Mulit-Prover Interactive Proofs

Lecturer: Dan Spielman *Scribe: Dominic D'Aleo*

1 Review

We intend to prove the following:
$MIP = NEXP$
$MIP = PCP$ (probabilistically checkable proofs)

Idea of $PCP(poly, poly)$
- have a randomized ptime verifier V
- gets a proof Π could have size $2^{p(n)}$
- V gets random access
  - has some tape on which it writes on index into Π
  - in next step gets a bit back

Definition 1 *$L \in PCP$ if $\exists$ a random ptime verifier V with some device for random access s.t.*
$x \in L \Rightarrow \exists\ \Pi\ s.t. Pr[V(x, \Pi)\ accepts] = 1$
$x \notin L \Rightarrow \forall\ \Pi\ Pr[V(x, \Pi)\ accepts] < 1/3$

2 Example

Claim 1 $PSPACE \subseteq PCP$

Claim 2 $IP \subseteq PCP$

Proof: consider an IP
- encode behavior of P, as a long string Π
- to ask a question q_i of P, after asked $q_1, ..., q_{i-1}$
  take a look at the $(q_1, q_2, ..., q_i)^{th}$ (treat this as a binary)
  bit of Π
- Any prover's strategy can be written into Π

Definition
Defined a prover P to be a function:
input: history of conversation so far
output: some string
Π becomes the table of values of this function

Dont Claim : $\forall\ \Pi\ \exists\ P$

Claim : $\forall\ \Pi$, if V accesses it using protocol $(inputs, k)$, then can turn Π into P

3 Theorem $PCP = MIP$

(if MIP redefined to have 1-sided error)

Proof $MIP \subseteq PCP$

MIP: have provers $P_1, ..., P_{poly(n)}$

- each is a func from a history of q's it has been asked, to a string

For $L \in MIP \; \exists \; V$ s.t.

$x \in L \Rightarrow \exists \; P_1, ..., P_{poly(n)} s.t. Pr[V \leftrightarrow P_1, ..., P_{poly(n)} \; accepts] = 1$

$x \notin L \Rightarrow \forall \; P_1, ..., P_{poly(n)} s.t. Pr[V \leftrightarrow P_1, ..., P_{poly(n)} \; accepts] < 1/3$

To prove $MIP \subseteq PCP$

- Create V' that simulates V, but when V would ask q_j of P_i, V' looks at positions $< i, q_i, ..., q_j, k >$ (prover,previous conversation with that prover,k) for $1 \leq k \leq p(n)$

Note: If $x \notin L \Rightarrow \nexists$ provers s.t. accept $> 1/3$

- Consider V' and Π
  If $\exists \; \Pi$ s.t. $Pr[V' accepts] > 1/3$,
  then Π is the behavior of the provers; create them.

Proof $PCP \subseteq MIP$

- guideline: never ask a prover more than one question
- $x \in L \Rightarrow \exists \; \Pi$ - just set up provers s.t. if you ask for a bit of Π, P tells you what it is.
- if $P's$ get V to accept$> \alpha \Rightarrow \exists \; \Pi$ on which V accepts$> \alpha$
- Consider V for PCP system, say it gets $p(n)$ bits
  - Construct a MIP with $n * p(n)$ provers

In the MIP, V' simulates V

- when V would look at the q^{th} bit of Π, V' chooses n provers at random (of those remaining)
  - it asks them all question q
  - if they all give the same answer, it uses it. Otherwise it rejects.

Analysis

Given $P_1, ..., P_{n*p(n)}$ let $\Pi_p(q)$ = answer given by the provers most often on question q

If $Pr[V' \; accepts \; when \; talking \; to \; P_1, ..., P_{n*p(n)}] = \alpha$
then $Pr[V \; accepts \; with \; \Pi] > \alpha - 2^{-n}$

If V' gets all uniform answers to every question, then its getting the answer from Π

$$Pr[gets \; uniform \; wrong \; answer] = \frac{\binom{\frac{1}{2} n * p(n)}{n}}{\binom{n * p(n)}{n}} < 2^{-n}$$