IITM-CS6840: Advanced Complexity Theory February 09 2012

Lecture 19 : Interactive Proofs - introduction and examples

Lecturer: Jayalal Sharma *Scribe: Vamsi Krishna D*

THEME: Interactive Proof Systems
LECTURE PLAN:In this lecture we will be introducing the idea of Interactive proofs (IP).We will start with the weak version of IP (called PS) and then allow for some errors to get IP and finally we will show the Interactive proof system for GNI.

Interactive Proofs
Interactive Proofs can be thought of as a technique that models computation using communication between two parties ,one called Prover P which has the unlimited computational power and tries to convince the verfier V which is a polynomial time Machine ,which is modeled as PS complexity class .Later we will insert randomness and allow the V to commit some small error to define the complexity class IP.The communication between the Prover and verfier is only allowed to be of polynomial length.

NP Vs PS

Let's consider SAT which is a NP-Complete Problem.A Prover verfier Strategy works for this as shown below

Let ϕ is the formula availiable to both prover and verfier
PROVER $\xrightarrow{sendanassignment(\sigma)}$ verfier

Now the verfier checks whether σ satisfies ϕ. If there exists such an assingnment the best strategy of the Prover is to send the satisfying assingnment.Otherwise no matter what Prover sends verfier rejects.Formally

$x \in SAT \Rightarrow \exists P(P, V)$accepts.

$x \notin SAT \Rightarrow \forall P(P, V)$ rejects.

Hence SAT $\in$ PS.Thereby we can say $\mathsf{NP} \subseteq PS$.

Now let's think about the reverse case $PS \subseteq \mathsf{NP}$.For any Language L accepted by PS strategy , we can get a NP machine accepting the same L , as an NP machine gets the accepting certificate if exists .So we can say $\mathsf{NP} = PS$.

Now let us see whether $\Pi_2 \subseteq PS$ .Let $\mathsf{L} \in \Pi_2$.
$x \in \mathsf{L} \Leftrightarrow \forall y \exists z(x, y, z) \in B$ where B is a polynomial time Turing machine .
Prover strategy : Let verfier choose any 'y' ,the Prover gives 'z' such that (x,y,z) $\in B$.
With this strategy the Prover can cheat the verfier when $x \notin \mathsf{L}$ since can Query only a

Polynomial times to the Prover.So the prover get's away without having to give a 'z' for all 'y'. But if we randomize the verfier then there is a chance that the Prover is going to be caught and such a strategy is called Interactive Proofs (IP).

Definition of IP:
$x \in \mathsf{L} \Rightarrow \exists P$ such that Pr(Prover convinces verfier) $\geq \frac{1}{2} + \epsilon$ for $\epsilon > 0$.

$x \notin \mathsf{L} \Rightarrow \forall P$ Pr(Prover convinces verfier) $\leq \frac{1}{2} - \epsilon$ for $\epsilon > 0$.

The argument of Amplication Lemma can be used to show for any arbitary $0 < \epsilon < \frac{1}{2}$ defintions are equivalent.

Graph Non-Isomorphism(GNI):
GNI= $\{(G_1, G_2) : \forall permutations \pi, G_1 \neq \pi(G_2)\}$

Theorem 19.0: GNI $\in$ IP.
Proof: The following are the stratagies of

Verfier: Pick G_i randomly from $\{G_1, G_2\}$ and produce $\mathsf{G}' = \pi(\mathsf{G}_i)$ and send it across the Prover where π is a random permuatation.
Prover: Compare G' to G_1, G_2.If it is isomorphic to one of them then return that one.If it is isomorphic with both of them then randomly return G_1 or G_2.
Verfier: If the prover is correct then accept other wise reject .

For $G_1 \ncong G_2$,the prover makes the Verfier accept.For $G_1 \cong G_2$, the Prover can make the Verfier to accept with a maximum Probability of $\frac{1}{2}$,because $G_1 \cong G_2$ then the Prover outputs randomly any one graph.