CS 221: Computational Complexity **Prof. Salil Vadhan**

Lecture Notes 19

January 25, 2010 **Scribe: Richard Liu**

1 Recap

Recall from last time that we have the following:

- $\mathbf{IP}[k(n)]$ = interactive proofs with $\leq k(n)$ msgs. $\mathbf{IP} := \mathbf{IP}[\text{poly}]$.
- $\mathbf{AM}[k(n)]$ = public coin interactive proofs with $\leq k(n)$ msgs starting with A (verifier). $\mathbf{AM} := \mathbf{AM}[2]$.
- $\mathbf{MA}[k(n)]$ = public coin interactive proofs with $\leq k(n)$ msgs starting with M (prover). $\mathbf{MA} := \mathbf{MA}[2]$.

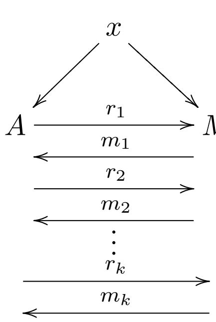
Facts: for $k(n) \geq 2$

- $\mathbf{MA}[k(n)] \subseteq \mathbf{AM}[k(n)] \subseteq \mathbf{IP}[k(n)]$
- $\mathbf{AM}[2k(n)] \subseteq \mathbf{AM}[k(n)]$
- Assume perfect completeness wlog.

You'll prove these inclusions for constant k in PS5 and in section.

2 AM vs. Alternation

Public coin interactive proof:



Perfect Completeness: $\exists$ verifier strategy s.t. A always accepts.

$x \in L \Longrightarrow$ $\forall r_1 \; \exists m_1$
$\forall r_2 \; \exists m_2$
$\vdots$
$\forall r_k \; \exists m_k$
$A(x, r_1, m_1, ..., r_k, m_k) = 1$

Soundness (assume error 2^{-kn}, wlog by parallel repetitions):

$x \notin L \Longrightarrow$ for most r_1 $\exists m_1$
for most r_2 $\exists m_2$
$\vdots$
for most r_k $\exists m_k$
$A(x, r_1, m_1, ..., r_k, m_k) = 0$
"Strong negation of TQBF"

AM games	**Alternation**
One unbounded player M	Two unbounded players
One randomized player A	Which one has winning strategy?
Does M have winning strategy or is M far from having one?	

3 AM vs. IP

$$\mathbf{IP} = \underset{\text{poly \# of alternations}}{\mathbf{PSPACE}} = \underset{\text{poly \# rounds of } \mathbf{AM} \text{ games}}{\mathbf{AM}[\text{poly}]}$$

Recall: Let $f \in \#\mathbf{P}$ so

$$\forall x \; f(x) = |S(x)| \text{ where } \underbrace{S(x) = \{y \in \{0,1\}^{p(|x|)} : M(x,y) = 1\}}_{\mathbf{NP} \text{ search problem}}$$

Theorem 1 *$\forall$poly p, $\textsc{Gap}_{1+1/p(n)}$-f is in* **prAM**

Proof: Last time, we showed this for $\textsc{Gap}_\alpha\ f$ with $\alpha = 8$

$$\begin{aligned} \textsc{Gap}_\alpha\ f_Y &= \{(x,t) : |S(x)| > t\} \\ \textsc{Gap}_\alpha\ f_N &= \{(x,t) : |S(x)| < t/\alpha\} \end{aligned}$$

Trick: to improve approximation factor, apply "8-approx set-size lower bound protocol" to

$$S'(x) = S(x)^k = \{(y_1, ..., y_k) : \forall i \; M(x, y_i) = 1\}$$

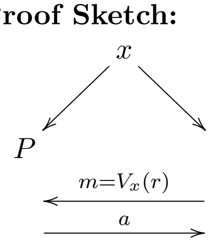
Approximating $|S'(x)|$ to within a factor of 8 $\Longrightarrow$ approximating $|S(x)|$ to under $8^{1/k} = 1 + O(1/k)$. Take $k = \text{poly}(n)$. ■

Now we will prove the following.

Theorem 2 **IP**$[2] \subseteq$ **AM**$[4] \overset{\text{PS5}}{=}$ **AM**.

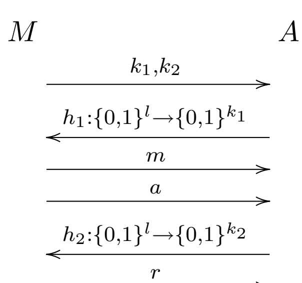
Corollary 3 Graph Nonisomorphism *is in* **AM**.

Proof Sketch:



$r \in \{0,1\}^l$
accept if $V(x,a,r) = 1$

Idea: Prove that there are "many" m s.t. $\exists a$, for "many" $r \in V_x^{-1}(m)$, $V(x,a,r) = 1$



where A accepts if:
$h_1(m) = 0^{k_1}$
$h_2(r) = 0^{k_2}$
$V_x(r) = m$
$V(x,a,r) = 1$
$k_1 + k_2 \geq l - \log l - 3$

Assume WLOG P, V has completeness $\geq 3/4$ and soundness $\leq 2^{-n}$.

When $x \in L$, the completeness of (P, V) tells us that:
w.p. $\geq 1/2$ over $m \leftarrow V_x(U_l)$,
$\exists a$ s.t. w.p. $\geq 1/2$ over $r \stackrel{R}{\leftarrow} V_x^{-1}(m)$,
$V(x, a, r) = 1$.

The above is almost like the condition we want to establish, but saying that something happens with probability at least 1/2 over m does not quite tell us for how many m this occurs (since the distribution $V_x(U_l)$ may be complicated), and saying that something happens with probability at least 1/2 over $r \stackrel{R}{\leftarrow} V_x^{-1}(m)$, since we do not know the size of $V_x^{-1}(m)$ (note that this equals $2^l \cdot \Pr[V_x(U_l) = m]$).

To solve the above problems, we group the m's into buckets each of which have roughly the same size. Specifically, define $B_i = \{m : V_x^{-1}(m) \in [2^i, 2^{i+1})\}$ for $i = 0, ..., l$. Call m *i-good*, if $m \in B_i$ and there exists an a such that with probability at least 1/2 over $r \stackrel{R}{\leftarrow} V_x^{-1}(m)$, we have $V(x, a, r) = 1$.

Since m is i-good for some i with probability at least 1/2 (as above) and there are only $1/(l+1)$ buckets, there must be a fixed i_x such that m is i_x-good with probability at least $1/2(l+1)$. Then we have:

$$\# \; i_x\text{-good } m \geq \frac{2^l}{2(l+1)} \cdot \underbrace{\frac{1}{2^{i_x+1}}}_{\#\text{ of coins corr. to good } m\text{'s}} = 2^{l - i_x - \log l - 3}$$

Moreover, if m is i_x-good, then there exists an a such that there are at least $(1/2) \cdot 2^{i_x}$ values of $r \in V_x^{-1}(m)$ for which $V(x, a, r) = 1$. Thus, if M sets $k_1 = l - i_x - \log l - 3$ and $k_2 = i_x - 1$, A will accept with at least constant probability (by the analysis of the set-size lower bound protocol from last time).

Now we analyze soundness. Let $x \notin L$. Suppose that some M^* can make A accept with constant probability by sending k_1, k_2 in the first message. Then there exists $\geq 2^{k_1 - \log l - O(1)}$ m's s.t. $\exists a$ s.t. there are $\geq 2^{k_2 - O(1)}$ s.t. $V(x, a, r) = 1$. (Here the $O(1)$'s are arbitrarily large constants.) Then we have a strategy P^* making V accept with probability at least

$$\frac{2^{k_1 - \log l - O(1)} \cdot 2^{k_2 - O(1)}}{2^l}$$

By soundness, V accepts with probability at most 2^{-n}. So we have $k_1 + k_2 - \log l \leq l - n + O(1) \ll l - \log l - 3$, which means that A will reject. $\square$

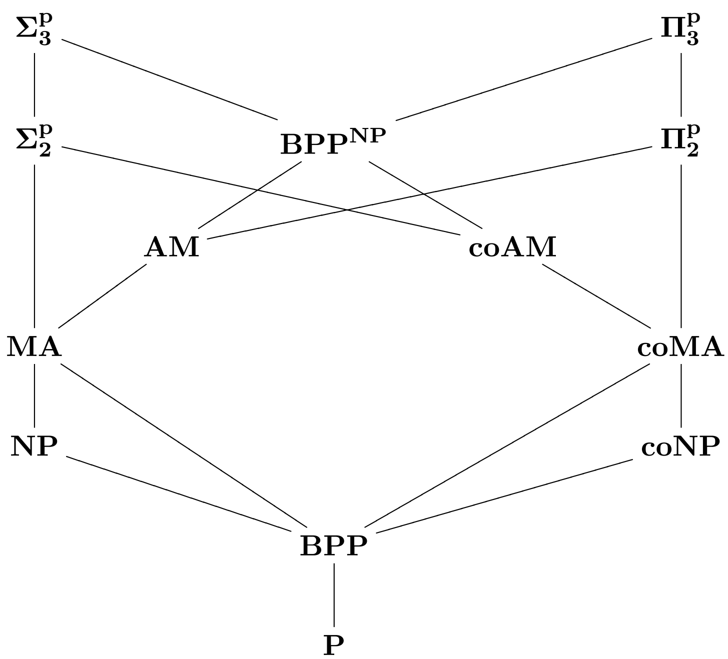
The ideas above can be extended to prove the following, more general theorem:

Theorem 4 *For every* $k(n) \geq 2$, $\mathbf{IP}[k(n)] = \mathbf{AM}[k(n)]$.

Combined with the Collapse Theorem for **AM** (PS5), we have:

Corollary 5 **AM** *equals the class of languages having constant-round interactive proofs.*

4 AM vs. PH



Can Graph Isomorphism be **NP**-complete (under Karp reduction)?
If Y, then GNI is **coNP**-complete, and hence $\mathbf{coNP} \subseteq \mathbf{IP}[2] = \mathbf{AM}$.

Theorem 6 *If* $\mathbf{coNP} \subseteq \mathbf{AM}$, *then* $\mathbf{PH} = \mathbf{AM} \subseteq \mathbf{\Pi_2^p}$.

Proof: Since $\mathbf{AM} \subseteq \mathbf{\Pi_2^p}$, it suffices to show that $\mathbf{\Sigma_2^p} \subseteq \mathbf{AM}$. To get an **AM** protocol to prove $\exists x\, \forall y\, \varphi(x, y)$, we have the prover send x, and then prove the **coNP** statement $\forall y \varphi(x, y)$ using the assumption that $\mathbf{coNP} \subseteq \mathbf{AM}$. ∎

Corollary 7 GNI *is not* **NP**-*complete unless* $\mathbf{PH} = \mathbf{AM} \subseteq \mathbf{\Pi_2^p}$.