18.405J/6.841J Advanced Complexity Theory	April 17, 1997
Lecture 18	
Lecturer: Daniel A. Spielman	*Scribe: John Dunagan*

Public Coins = Private Coins

The general theorem is

Theorem 1 $IP(k(n)) = AM(k(n) + 3)$

We will restrict ourselves to proving the special case

Theorem 2 $IP(2) = AM(5)$

because all the essential ideas are present in this case, and the analysis is several pages shorter. You are welcome to read the original paper by Goldwasser-Sipser if you would like to know the details of the full proof. For notational convenience,
M = Merlin = Σ, and A = Arthur = BP

The essential proposition to prove our theorem is this:
Proposition
Let S $\subset$ $\{0,1\}^m$ be a language in which one can efficiently verify membership, (say S $\in$ C where C is a class analogous to P - later in this lecture, C will appear as AM, something one can efficiently verify membership in with a little help). Then $\forall$ integer N and polynomial p, $\exists$ an MAMC protocol s.t.
if $|S| > N, Pr[accept] > 1 - 2^{p(m)}$
if $|S| < \frac{N}{2}, Pr[accept] < 2^{p(m)}$

Sketch of Proof of Proposition:
M: produces a hash function h s.t. h:$\{0,1\}^m$ is mapped to a set of size N = $\{0,1\}^{\lfloor logN \rfloor}$
A: randomly chooses elements in $\{0,1\}^{\lfloor logN \rfloor}$
M: produces pre-images in S for these elements (as many as possible)
A: accepts if M provided pre-images for most
The rigorous proof is very similar to that which we did in a previous class for graph non-isomorphism, and it will not be given here again. There are minor differences though: in working out an AM protocol of graph non-isomorphism we showed that this method distinguished between N and N/3, not N and N/2 - however we could prove this for any constant by considering the set SxS..xS some large constant number of times instead of the set S alone. We also now allow A to verify membership in C, C not necessarily equal to P. None of these differences present problems in the proof.

Our IP(2) Model

Here is our 2-round interactive proof. Let l be our poly, and let w be the word we are reasoning about. We denote the verifier by V and the prover by P throughout the proof.
V: gets a random string $r \in \{0,1\}^{l(|w|)}$
V: uses r to produce a message q ("q" for "query") to send to P
P: answers with a response a; P should answer with a that causes acceptance on most random strings that produce q (which it can if w is in the set and this a "good" protocol, analogous to the graph

non-isomorphism protocol).

A bit of commentary here is in order. V may be pictured as a map from random strings r to questions q. Any interesting IP protocol has V not injective, because otherwise P knows what r V started with from q. (And thus this is already an AM protocol.)
We can divide the r into two types: those which, with a, cause acceptance, and those which don't.
Let R(q) = $\{r \in \{0,1\}^{l(|w|)}$ s.t. $V(w,r) = q\}$
Let a_q be chosen to maximize $Pr[V(w,r,q,a_q)$ accepts] over r s.t. $V(w,r) = q$
Let $A(q) = \{r : V(w,r) = q$ and $V(w,r,q,a_q)$ accepts $\}$
A(q) are the random strings where P is in good shape.
A = $\cup A(q)$ over q
$Pr[V$ accepts$] = \frac{|A|}{2^{l(|w|)}}$

Our MA(5) Simulation

We now give the MA(5) protocol which solves whatever language the previous IP(2) protocol did.
M will attempt to show that $|A|$ is big. To do this, M will demonstrate that for some c and d, there are at least 2^c q's s.t., $|A(q)| \geq 2^d$, which will imply $|A| \geq 2^{c+d}$. If $|A| > 2^{l-1}$, then $\exists c, d$ s.t. this holds, where $2^{c+d} \geq \frac{2^{l-1}}{2l}$ (this can easily be verified - simply show the converse is not true by considering the l possibilities for c.) This will work great if our original IP protocol had error $< 2^{-n}$ because

- If IP protocol accepted, $|A_w| > (1 - 2^{-n})2^l$
- If it rejected, $|A_w| < (2^{-n})2^l$

(this explains why losing a linear factor is not a problem.)

This requires 2 lower bound protocols

Sub Protocol: we show that $|A(q)| \geq 2^d$ can be shown by a lower bound protocol
Given q, M produces a_q
A can decide membership in A(q) in poly time, so we know from our proposition that $\exists$ an MAM protocol for this lower bound
If $|A(q)| < 2^{d-1}$, A rejects with high probability (this is the second part of the proposition)

Main Protocol: we show $\exists \geq 2^{c-1}$ "good" q's (where good dentoes that for this q, $|A(q)| >= 2^d$), using an MAM protocol and verifying using the sub protocol
M: sends c, d, and a hash function h used to show the number of "good" (or "large") q's $> 2^{c-1}$
A: choose poly number of random elements in image of h
M: provides the q's that were pre-images of those elements, and for each q, provides a hash function h_q to show $A(q)$ is large
A: chooses, for each h_q, a poly number of random elements (call a given one e) in image of each h_q (checking that $|A(q)| > 2^d$)
M: provides r s.t. $h_q(r) = e$ (the image) (thus showing that $|A(q)|$ is big)
A: accepts if M mostly succeeds

Since we have demonstrated an MA(5) protocol which simulates an IP(2) protocol, this concludes our proof of Theorem 2.