CS 221 LECTURE 15

Today: **Power Of Interaction**

- Interactive Proofs
- Complexity Classes: AM, IP
- Basic Closure

**Philosophical Question**: Is reading as informative as a discussion?

**Interaction**: $A \xleftarrow{q_1} \xrightarrow{a_1} q_2 \xrightarrow{a_2} q_3 \xleftarrow{a_3}, \ldots \xrightarrow{a_R} f(x, q_1, \ldots q_R, a_1, a_R)$
Key difference with "Debates": A is outputting verdict. \[ \leq A \text{ is poly time bounded.} \]

**Question**: for what languages \( L \) does there exist poly polytime verifier \( V \) s.t. if \( x \in L \) some prover \( P \) can convince \( V \) of this fact, but if \( x \not\in L \) no one can?

**Answer 1**: if \( L \in \text{NP} \)

\[
\begin{align*}
V & \leq \times \quad \left( x, a_1, a_2, a_3, \ldots, a_k, a_r \right) \\
& \leq \text{"Levin's model"}
\end{align*}
\]

\[ \text{if } V \text{ deterministic } P \text{ can emulate } V, \text{ predict } a_1, a_2, \ldots, a_k \]
\[ \text{or answer them!} \]

What if \( V \) probabilistic?

"Can execute Pepsi Challenge"

Call resulting class \( \text{IP} \).
Graph Non. Isomorphism

\[ L = \{ (G,H) \mid \forall \pi \exists \; G = \pi(H) \} \]

formulates vertex names

Thm: [GMW]: \( L \in \text{NP} \)

Proof: Verifier picks \( F \in \{\hat{\sigma}_6, H\} \) at random
\( \pi \in S_n \) at random
sends \( \pi(F) \) to prover.

- Verifier: tries to guess \( \hat{\pi} \in \{\hat{\sigma}_6, H\} \)
- Verifier: accepts if \( \hat{F} = F \).

To date: \( L \in \text{NP} ? \) (open)

Known: \( L \in \text{TIME}(n \log^e n) \)
Two complexity classes

1. IP: @ unbounded # rounds [6MR]
   * hidden random coins ["poker faces"]

2. AM: @ bounded # rounds
   * open randomness ["no poker face"]

Q: Was L ∈ IP proof also a proof that L ∈ AM?
A: No. F, it needs to be hidden from P.

Many subtle issues:

1. Is many rounds = few rounds?
   R vs. k+1?
   k = 2 vs. k = poly(n)?

2. Is AM[private] = AM[public]
   Is IP[private] = IP[public]

3. AM includes BPP. Is AM[one-sided] = AM[two-sided]

4. If AM = co-AK ?
   IP = co-IP ?

5. How do they relate to traditional comp. classes?
Answers

1. \( \forall k(n) \quad \text{Am}[k(n)] = \text{Am}[O(kn)] \)
   In particular, \( \text{Am}[O(1)] = \text{Am}[2] \equiv \text{Am} \).

2. \( \text{Am} [\text{private}] = \text{Am} [\text{public}] \)
   \( \text{IP} [\text{private}] = \text{IP} [\text{public}] \)

3. \( \text{Am} [\text{one-sided}] = \text{Am} [\text{two-sided}] \)

4. \( \text{Am} = \text{co-Am} \Rightarrow \text{PH collapses} \)
   \( \text{IP} = \text{co-IP} ! \)

5. \( \text{NP} \leq \text{AM} \leq \text{T} \)
   \( \text{IP} = \text{PSPACE} \)
   \( \text{Dramatic, surprising result from 90.} \)

Today: \# Hints for all except \( \text{IP} = \text{PSPACE} \).
Proof

Lesson 0: Amplification Works for IP/AM

$q^{(1)} \ldots q^{(t)} \rightarrow a^{(1)} \ldots a^{(t)}$

- Accept if majority $f(q^{(i)} : a^{(i)})$ accept.
- Works: Optimal prover strategy to try & win every coordinate.
- Analysis: Exercise.

$AM[2k] = AM[2k]:$

$\leftarrow BP. E \cdot BP. E \cdot C = BP. E \cdot C$

$\Theta 2^n \text{ error } 2^{-n^2}$

$2^n \text{ error } 2^{-n^2}$

$2^n \text{ error } 2^{-n^2}$
2. Private coins = Public coins
   One-sided = Two-sided

Note: "Prove #coins that lead to acceptance is large."

a. Protocol tree:

   Claim: # accepting leaves ≥ N₀

   At level i: Prover wishes to prove

   "#q_i at subtree ≥ N_i"

Partition q_i - split into S_1, S_2, ..., S_n

S_j = \{ q_i \} | # accepting leaves in q_i - subtree ∈ S_j \}

N_{i,j} = |S_j|.
Need to verify $\mathbb{E}[k] \leq 2^\ell \cdot |S| \leq N_{i/2}$

Pick random $i \in \{1, \ldots, N_i\}$ w.p. $2^\ell |S_i|$

① Prove $\forall i \in \{1, \ldots, N_i\}$ Protocol has $2^\ell$ accepting paths after question $q_i \notin N_i$

i.e. tasks of this form

$\# \{ x \mid \# \{ y \mid (x, y) \in R \} \geq A \} \geq B$

Key Protocol: Goldwasser–Sipser

- Can prove $\# \{ x \mid x \in L \geq A \}$ (approximately)

(if "$x \in L$" in AM) in AM.

Protocol: Pick $h_1, \ldots, h_n : \Sigma^* \rightarrow [A]$ randomly with uniform probability.

Ask verifier to prove

Verifier: $i \in [n], h_i \in \Sigma^*$

Prover: $i \in [n], x \in L \Rightarrow h_i(x) = i$

...
Next lecture: $\text{PSPACE} \leq \text{IP}$

Why is $\text{IP} \leq \text{PSPACE}$?

- Optimal prover in $\text{PSPACE}$
  (explores protocol tree, picks optimal answer to each question)