CS 221 LECTURE 15

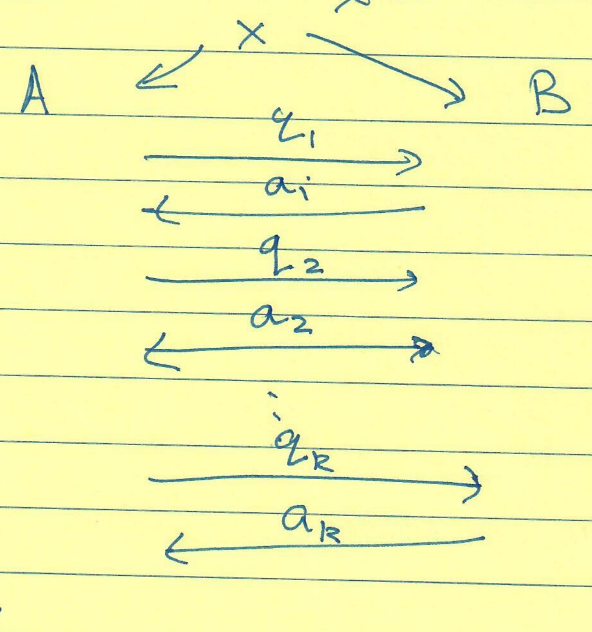
3/20/18

TODAY: POWER OF INTERACTION

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

Philosophical Question: Is reading as informative as a discussion?

Interaction:



$f(x, q_1 \ldots q_k, a_1 \ldots a_k)$

Key difference with "Debates": A is outputting verdict. [$\Leftarrow$ A is poly time bounded.].

<u>Question</u>: for what languages L does there exist prob. poly time verifier V s.t. if $x \in L$ some prover P can convince V of this fact, & if $x \notin L$ no one can?

Answer 1: iff $L \in NP$

x

V $\longleftarrow$ $\longrightarrow$ P

$(q_1, a_1, q_2, a_2 \dots q_k, a_k)$

"Lecture model"

[if V <u>deterministic</u> P can simulate V, predict $q_1 \dots q_k$ & answer them!]

What if V <u>probabilistic</u>?

"Can execute Pepsi Challenge"

Call resulting class <u>IP</u>.

Graph Non-Isomorphism

$L = \{ (G,H) \mid \forall \pi \quad G \neq \pi(H) \}$

↑

permutes vertex names

Thm: [GMW]: $L \in IP$

Proof: • Verifier picks $F \in \{G, H\}$ at random

$\pi \in S_n$ at random

sends $\pi(F)$ to prover.

• Prover: tries to guess $\hat{F} \in \{G, H\}$

• Verifier: accepts if $\hat{F} = F$.

To date: $L \in NP$? (open)

known: $L \in TIME(n^{\log^c n})$

Two complexity Classes

1. IP : (a) unbounded # rounds [GMR]
   (b) hidden random coins] "poker faces"

2. AM : (a) bounded # rounds
   (b) open randomness] "no poker face"

Q: Was $L \in IP$ proof also a proof that $L \in AM$?

A: No. F, π needs to be hidden from P.

Many subtle issues:

1. Is many rounds = few rounds ?

   k 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-AM ?
   IP = co-IP ?

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

Answers

1. $\forall\ k(n) \qquad AM[k(n)] = AM[O(k(n))]$

   in particular $\qquad AM[O(1)] = AM[2] \stackrel{\Delta}{=} AM.$

2. $AM[\text{private}] = AM[\text{public}]$

   $IP[\text{private}] = IP[\text{public}]$

3. $AM[\text{one-sided}] = AM[\text{two-sided}]$

4. $AM = \text{co-}AM \Rightarrow$ PH collapses

   $IP = \text{co-}IP$!

5. $NP \subseteq AM \subseteq \Pi_2$;

   $\boxed{IP = PSPACE}$ $\Leftarrow$ Dramatic, surprising result from '90.

Today: Hints for all except IP = PSPACE.

Proofs

Lesson 0: Amplification works for IP / AM

$$\xrightarrow{\quad q_1^{(1)} \dots q_1^{(t)} \quad}$$

$$\xleftarrow{\quad a_1^{(1)} \dots a_1^{(t)} \quad}$$

$$\vdots$$

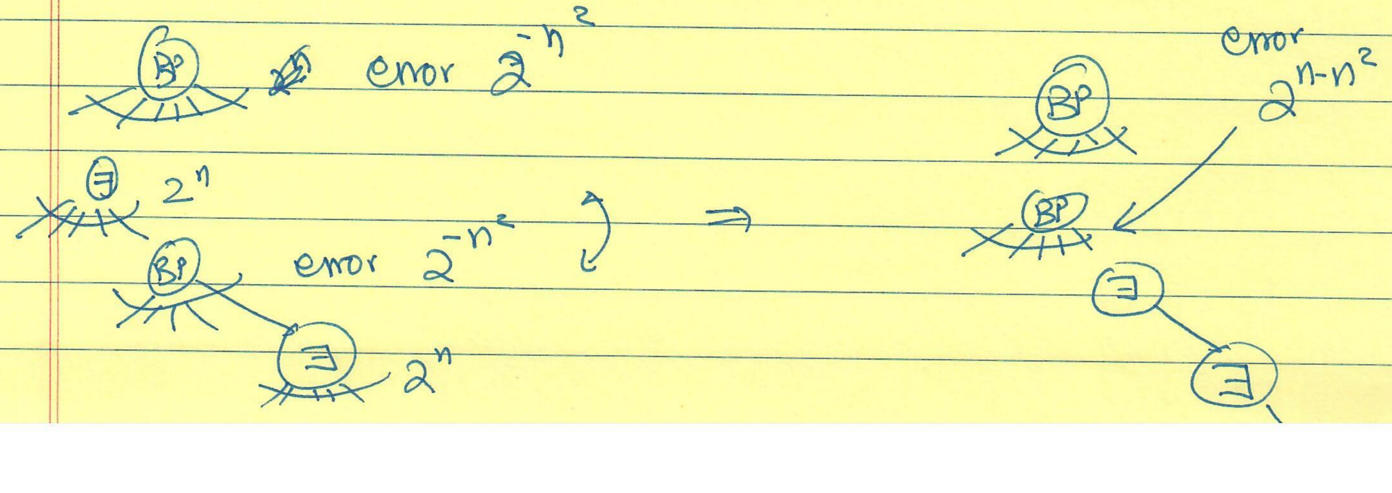
$$\xleftarrow{\quad a_k^{(1)} \dots a_k^{(t)} \quad}$$

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

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

morally

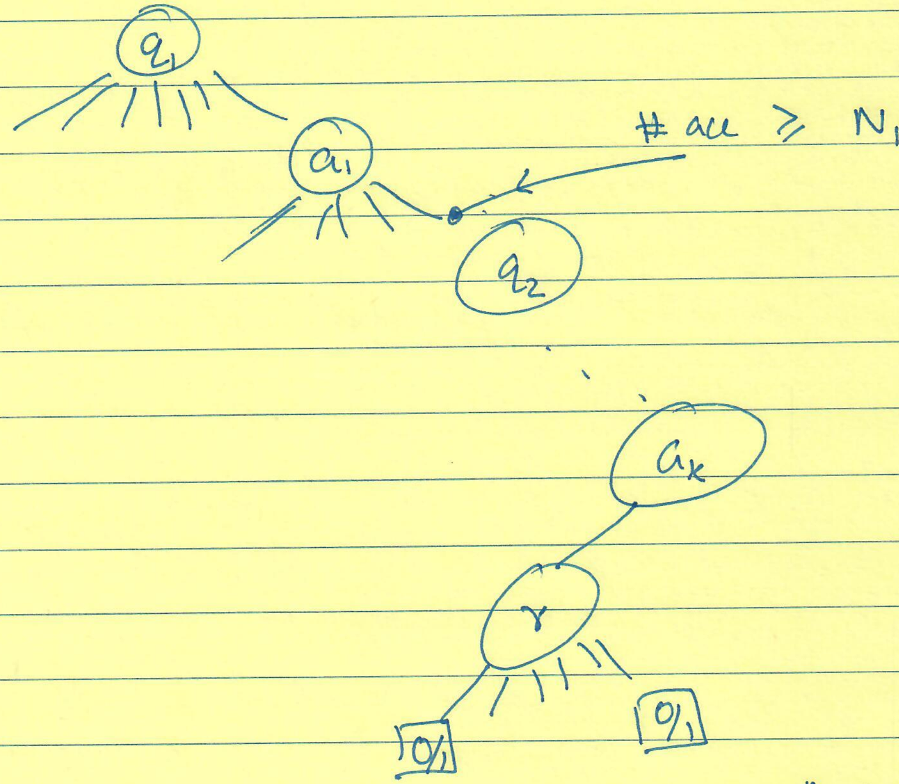
$\Longleftarrow \quad BP \cdot \exists \cdot BP \cdot \exists \cdot C \;=\; BP \cdot \exists \cdot C$



(2) Private-coins = Public coins
One-sided = Two-sided

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

(a) Protocol tree: · Claim: # accepting leaves $\geq N_0$



At level i: Prover wishes to prove # acc leaves at subtree $\geq N_i$
" ~~# q_i s.t. ∃ q_i ...~~

Partion q_i-space into $S_1, S_2, \ldots S_n$

$$S_j = \{ q_i \mid \# \text{ accepting leaves in } q_i\text{-subtree} \in [2^j, 2^{j+1}) \}$$

$N_{ij} = |S_j|$.

Need to verify $\sum 2^j \cdot |S_j| \geq N_i/2$

Pick random j w.p. $\propto 2^j |S_j|$

(1) Prove $\#\{q_i$ s.t. Protocol has 2^j accepting paths ~~with~~ after question $q_i\} \geq N_{ij}$

i.e. tasks of ~~these~~ form

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

Key Protocol : Goldwasser-Sipser

- Can prove $\#\{x \text{ s.t. } x \in L\} \geq A$ (approximately) (if "$x \in L$" in AM) in AM.

- Protocol: . Pick $h_1 \ldots h_n : \{0,1\}^n \to [A]$ ~~rando~~ p.w.i.

  - ~~Ask verifier to prove~~ ~~Prover~~
  - Verifier: $j \in_U [A]$
  - Prover: $i \in [n]$, $x \in L$ s.t.

    $h_i(x) = j$

. . . .

$\boxtimes$

- Next Lecture: PSPACE $\subseteq$ IP
- Why is IP $\subseteq$ PSPACE?
  - Optimal prover in PSPACE
    (explores protocol tree, picks optimal answer to each question)

—— x ——