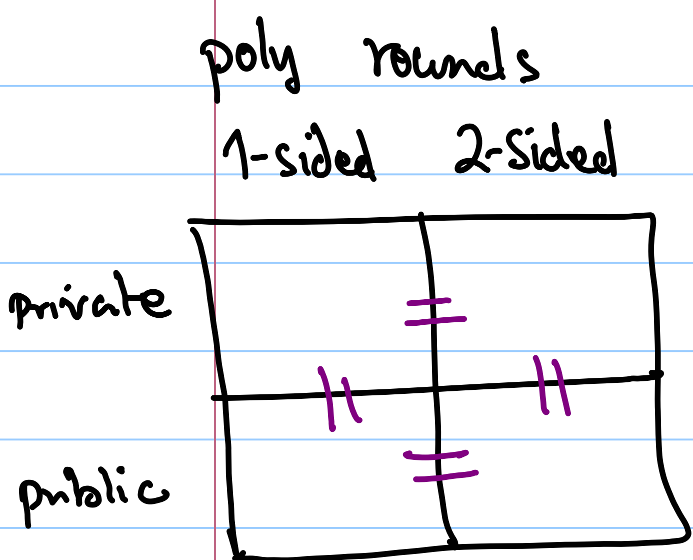
LECTURE 15

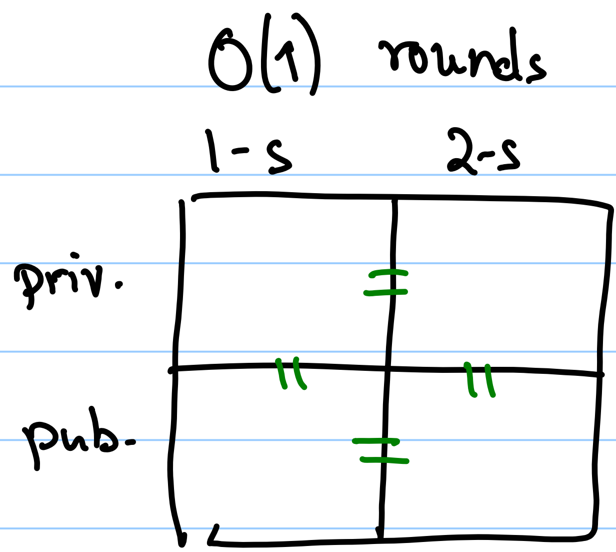
Note Title 4/4/2007

TODAY:
- REVIEW IP, AM
- The [Goldwasser-Sipser] Approx. Counting Protocol
- Private Coins = Public Coins
- Start IP = PSPACE

IP: Interactive Proofs ; AM: Arthur-Merlin

Eight possible classes





Last time: ↑ all four above equal

Today: all four above equal = AM[2]

KEY INGREDIENT: APPROX. COUNTING PROTOCOL

Input: Set $S \subseteq \{0,1\}^n$ given by membership prover

YES: $|S| \geq f(n)$

NO: $|S| \leq \frac{f(n)}{10 \cdot n^2}$

Goal: AM protocol for YES instances

—— x ——

Simple Case: $f(n) = 2^n$ ....

Verifier picks random $x \in \{0,1\}^n$ & verifies $x \in S$.

—— x ——

Next Case: $f(n) = \frac{1}{2} \cdot 2^n$ ...

- Simple protocol doesn't give one-sided error!

- Use [Lautemann-Sipser] ($BPP \subseteq \Sigma_2^P \ldots$)

Verifier $\qquad\qquad\qquad\qquad$ Prover

$$\xleftarrow{\quad x_1, x_2, \ldots x_n \quad}$$

$$x \in_R \{0,1\}^n \quad \xrightarrow{\quad x \quad}$$

$$\xleftarrow[\text{for some } i]{\quad x \oplus x_i \in S \quad}$$

YES $\Rightarrow$ Such $x_1, \ldots x_n$ & $i = i_x$ exist

NO $\Rightarrow$ $\Pr[\text{such } i \text{ exists}] \leq n \cdot \frac{f(n)}{10 n^2}$

$$\leq \frac{1}{n}.$$

Works upto $f(n) = \frac{1}{\text{poly}} \cdot 2^n$

What if $f(n) = 2^{\sqrt{n}}$?

General Case

- Hash $h : \{0,1\}^n \to \underbrace{[10 \cdot f(n)]}_{\{0,1\}^m}$

- Prove $h(S)$ large in $\{0,1\}^m$!

Verifier | **Prover**

Pick $m = O(\log f(n))$

& $h : \{0,1\}^n \to \{0,1\}^m$

from p.w.i. family

$$\xrightarrow{\quad h,\ m \quad}$$

$$y_1 \ldots y_k \in \{0,1\}^m$$

$$\xleftarrow{\qquad\qquad}$$

$y \in \{0,1\}^m$

$$\xrightarrow{\quad y \quad}$$

$$x \in S \text{ s.t. } h(x) \oplus y = y_i$$

$$\xleftarrow{\qquad\qquad}$$

Private Coins → Public Coins

Private Coin Verifier V:

Prover

- Picks $R \in \{0,1\}^n$ at random
- Computes $q = q(R)$

$$\xrightarrow{\quad q \in \{0,1\}^k \quad}$$

$$\xleftarrow{\quad a \quad}$$

Verifies (x, R, a) acceptable

- Want prover to convince us that for many R, $\exists\, a$ s.t. a acceptable answer to $q = q(R)$.

- **Issue:** "acceptability" of "a" function of "R" not "q".

Simple Case: $S_{q,a} = \{ R \mid q = q(R) \ \& \ V(x,R,a) \text{ accepts} \}$

YES: $\forall q \ \exists a$ s.t. $|S_{q,a}| \geq N$

NO: $\forall q, a$ $|S_{q,a}| \leq \frac{N}{n^2}$

. N known to verifier

Protocol: Prover sends (q,a);
Proves $S_{q,a} \geq \frac{2}{3} \cdot N$
using [GS] protocol.

(works for simple case)

But in general:

YES: $|S_{q,a}| \geq N_q$

depends on q!

not known to verifier!!

<u>Solution</u>: Prover tells us "typical" value

of $N_q = N$

& proves $\#\{q \mid N_q \geq N\}$

$$\geq \frac{2^n}{N} \cdot \frac{1}{2n}$$

How? Using [GS] twice.

Verifier $\qquad\qquad\qquad\qquad$ Prover

$\xleftarrow{\quad N \quad}$

/* Verify $|\{q \mid N_q \geq N\}| \geq$ --- */

$\xrightarrow{\quad \text{hash}, \ m \quad}$

$\xleftarrow{\quad y_1 \dots y_k \quad}$

$\xrightarrow{\quad y \quad}$

$\xleftarrow{\quad q_0, \ i \quad}$

Check $h(q_0) \oplus y_i = y$

/* Verify $N_{q_0} \geq N$ */

[GS] again

AM:

- Can induct on previous idea to convert any k-round private protocol to 10·k round public protocol
- $IP(O(1)) = AM(O(1))$.
- But $AMAMAM = BP \cdot \exists \cdot BP \cdot \exists \cdot BP \cdot \exists \cdot P$
- A la [Toda] : $\subseteq BP \cdot BP \cdot BP \cdot \exists \cdot \exists \cdot \exists \cdot P$

$$= BP \cdot \exists \cdot P = AM[2].$$

$\Rightarrow$ $IP[O(1)] = AM$.

- $AM \subseteq NP/_{poly}$ [Adleman]
- GI NP-complete $\Rightarrow$ $\text{coSAT} \in NP/_{poly}$

$\Rightarrow$ PH collapses N (Karp Lipton).

Next Agenda Item: IP = PSPACE

History (according to me):

Lipton '90: Permanent is "random self reducible"
(reduces to random instances of itself)

BLR '90: RSR & downward self-reducible
functions are "checkable"
[applied to modular mult. ...]

Nisan: 2+2=4
Permanent is RSR
" DSR
$\Rightarrow$ Permanent is "checkable"!

LFKN : Permanent $\in$ IP.

Rest of lecture : Proof

Ingredient 1 : RSR of permanent.

- Want to compute perm(A) (mod p). $p > 2n$
- Have Alg "mrep" s.t.

$$\Pr_{R \in \mathbb{Z}_p^{n \times n}} \left[\text{mrep}(R) = \text{perm}(R) \right] \geq 1 - \delta$$

- Pick $R \in_U \mathbb{Z}_p^{n \times n}$

$$M_i = A + i \cdot R$$

- Here $M_0 = A$; M_i = random for other i.
- Let $y_i = \text{mrep}(M_i)$ $i = 1 \ldots n+1$

  Let p be univ. deg n polynomial s.t.

  $p(i) = y_i$ $i = 1 \ldots n+1$

- Output $p(0)$;

Claim: For $i \neq 1$

$$\Pr\left[\, y_i \neq \text{perm}(M_i) \,\right] \leq \delta$$

Claim: $\Pr\left[\, \exists i \quad \right] \leq (n+1)\,\delta$

Claim:
if $\forall i$ $y_i = \text{perm}(M_i)$ then $p(x) = \text{perm}(A + xR)$
& so $p(0) = \text{perm}(A)$.

deg n poly; agree at $i = 1 \ldots n+1$

DSR: Let $A_1 \dots A_n$ be minors of A

then $$\text{Perm}(A) = \sum_{i=1}^{n} a_{1i} \, \text{Perm}(A_i).$$

What follows builds on & doesn't follow from the above

$$\text{Verifier} \xleftarrow[\quad\quad\quad\quad]{A \\ \text{perm}(A) = p} \text{Prover}$$

Let $A_1 \dots A_n$ be minors.

Build matrix $B(x)$ s.t.

$b_{ij}(x) =$ deg. $n-1$ poly in x

$b_{ij}(k) = (A_k)_{ij}$

$$\xrightarrow{\text{perm}(B(x)) = ?}$$

$$\xleftarrow[\text{poly of degree } n^2]{h(x)}$$

<u>Cases</u>:

① $h(x) = \text{perm}(B(x))$ (but $p \neq \text{Perm}(A)$)

$$p \neq \text{perm}(A) = \sum a_{i1} \text{Perm}(A_i)$$

$$= \sum a_{i1} \cdot \text{perm}(B(i))$$

$$= \sum a_{i1} h(i)$$

reject if so : $p \neq \sum a_{i1} h(i)$

② $h(x) \neq \text{perm}(B(x)) = \tilde{h}(x)$

also of deg $\leq n^2$

Disagree $\Rightarrow$ $h(r) = \tilde{h}(r)$ for $p - n^2$

choices of r

Pick $r \in_r \mathbb{Z}_p$

$$\xrightarrow{\quad r \quad}$$

Challenge: Prove "$\underline{h(r)} = \text{perm}(\underline{B(r)})$"

known to verifier

smaller.

$\underline{\text{Moral}}$: - Today we a proof based on #SAT;

- No mention of RSR, DSR, Permanent;

- But wouldn't exist without those notions.