

# LECTURE 15

Note Title

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

————— x —————

IP: Interactive Proofs ; AM: Arthur-Merlin

Eight possible classes

poly rounds  
1-sided 2-Sided

private		=	
public		=	

$O(1)$  rounds  
1-s 2-s

priv.		=	
pub.		=	

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

Simple Case:  $f(n) = 2^n \dots$

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

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

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

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

Verifier

Prover

$x_1, x_2, \dots, x_n$

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

←

$x$

→

$x \oplus x_i \in S$

←

for some  $i$

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

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

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

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

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

## General Case

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

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

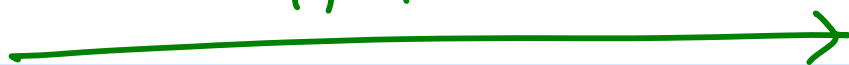
Verifier

Prover

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

2  $h: \{0,1\}^n \rightarrow \{0,1\}^m$

from p.w.i. family  
 $h, m$



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



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

$y$

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



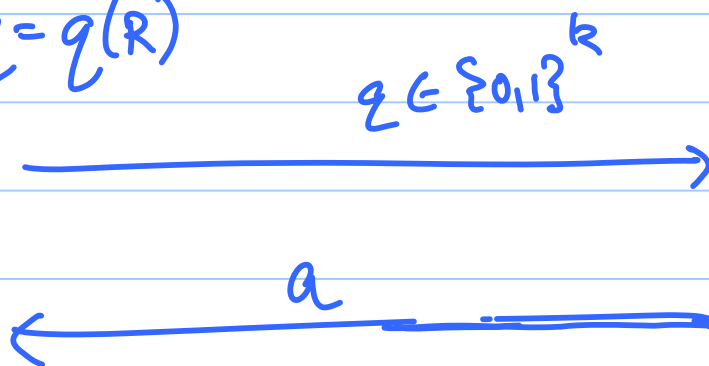
# Private Coins $\rightarrow$ Public Coins

Private Coin Verifier  $V$ :

- Picks  $R \in \{0,1\}^n$  at random

- Computes  $Q = q(R)$

Prover



Verifies  $(Q, R, a)$

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".

————— x —————

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

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

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

N known to verifier

Protocol: Prover sends  $(q, a)$ ;

Proves  $|S_{q,a}| \geq \frac{2}{3} \cdot N$

Using [GIS] protocol.

(works for simple case)

But in general:

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

↑

depends on  $q$ !

not known to verifier!!

Solution: Prover tells us "typical" value

$$\text{of } N_q = N$$

$$\hookrightarrow \text{proves } \# \{q \mid N_q \geq N\}$$

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

How? Using [GS] twice.

Verifier

Prover

N

←

/\* Verify  $|\{q \mid Nq \geq N\}| \geq \dots$  \*/

hash, m

→

←  $y_1 \dots y_k$

y

→

←  $q_0, i$

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

/\* Verify  $Nq_0 \geq N$  \*/

[GIS] Again





## Am:

- An induct on previous idea to  
Convert any  $k$ -round private protocol  
to  $10 \cdot k$  round public protocol
  - $IP(O(n)) = AM(O(n))$ .
  - But  $AMAMAM = BP \cdot \exists \cdot BP \cdot \exists \cdot BP \cdot \exists \cdot P$
  - A la [Toda] :  $\subseteq BP \cdot BP \cdot BP \cdot \exists \cdot \exists \cdot \exists \cdot P$   
 $= BP \cdot \exists \cdot P = AM[2]$ .
- $\Rightarrow IP[O(n)] = AM$ .
- $AM \subseteq NP_{poly}$  [Adleman]
  - $\exists$  NP-complete  $\Rightarrow$  SAT  $\in NP_{poly}$

$\Rightarrow$  P17 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)

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

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

LFKN: Permanent  $\in$  IP.

Rest of lecture = Proof

Ingredient 1: RSR of permanent.

- Want to compute  $\text{perm}(A) \pmod{p}$ .  $p > 2^n$
- Have Alg "mrep" s.t.

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

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

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

• Hence  $M_0 = A$  ;  $M_i = \text{random}$  for other  $i$ .

• Let  $y_i = \text{mrep}(M_i)$   $i = 1 \dots n+1$

Let  $p$  be univ. deg  $n$  polynomial st.

$$p(i) = y_i \quad i = 1 \dots n+1$$

• Output  $p(0)$  ;



Claim: For  $i \neq 1$

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

Claim:  $\Pr [\exists i \downarrow] \leq (n+1)\delta$

Claim:

if  $\forall i \quad y_i = \text{perm}(M_i)$  then  $p(x) = \text{perm}(M+xR)$

& so  $p(0) = \text{perm}(A)$ .

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

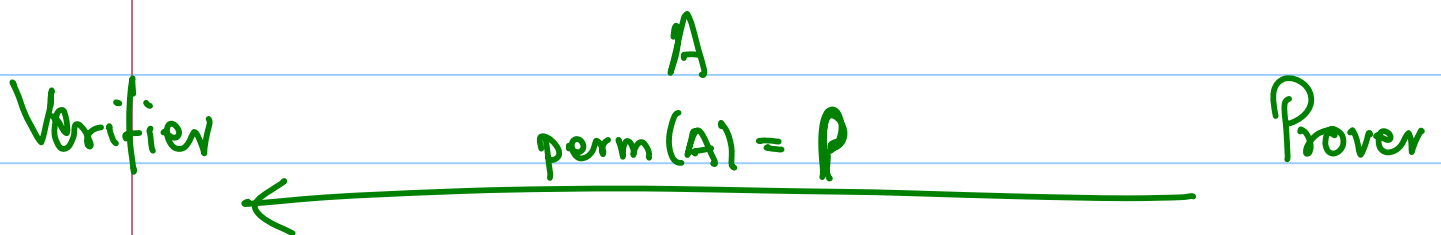
DSR: Let  $A_1 \dots A_n$  be minors of  $A$

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

————— x —————

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

————— x —————

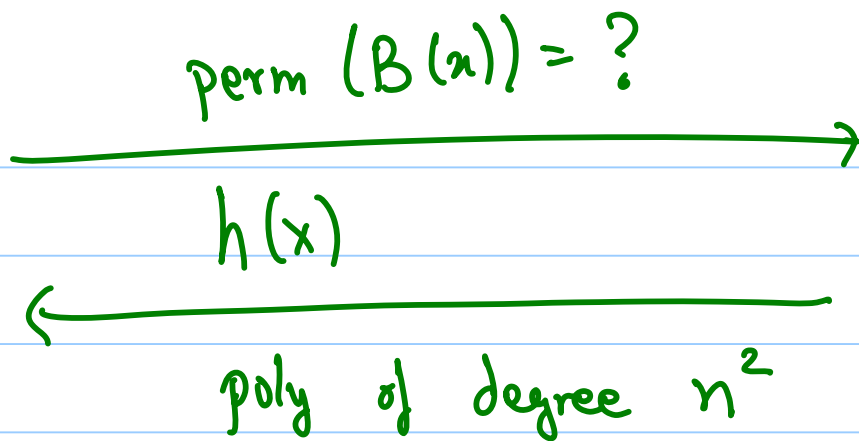


Let  $A_1 \dots A_n$  be minors.

Build matrix  $B(x)$  st.

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

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



Cases:

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

$$\begin{aligned} p \neq \text{perm}(A) &= \sum a_{ii} \text{Perm}(A_i) \\ &= \sum a_{ii} \cdot \text{perm}(B(i)) \\ &= \sum a_{ii} h(i) \end{aligned}$$

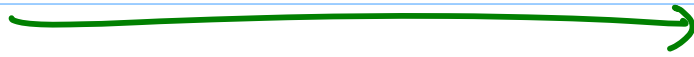
reject if so:  $p \neq \sum a_{ii} h(i)$

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  $r$

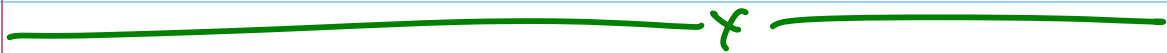
Pick  $r \in \mathbb{Z}_p$

$r$



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

known to verifier  
smaller.



- Moral: - Today we use a proof based on #SAT;
- No mention of RSR, DSR, Permanent;
  - But wouldn't exist without those notions.