Today: REVIEW IP, AM

- Private Coins = Public Coins
- Start $IP = PSPACE$

---

$IP$: Interactive Proofs; $AM$: Arthur-Merlin

Eight possible classes:

<table>
<thead>
<tr>
<th></th>
<th>poly rounds</th>
<th>$O(1)$ rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-sided</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-sided</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Private Public

Last time: all four above equal

Today: all four above equal = $AM[2]$
**Key Ingredient:** Approx. Counting Protocol

**Input:** Set $S$ given by membership prover

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

**Goal:** AM protocol for **YES** instance

---

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

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

---

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

- Simple protocol doesn't give one-sided error!
Use [dautermann-sipser] \( (\text{BPP} \subseteq \Sigma_2^P) \)

**Verifier**

\[ \alpha \in \{0,1\}^n \]

\[ \alpha \in \alpha \odot x_i \in S \]

\[ \text{for some } i \]

**Prover**

\[ x, x_2, \ldots, x_n \]

**YES** ⇒ such \( x_1, \ldots, x_n \) & \( i = i_x \) exist

**NO** ⇒ \( \Pr [ \text{such } i \text{ exists} ] \leq \frac{\text{f}(n)}{10n^2} \leq \frac{1}{n} \).

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

What if \( f(n) = 2^{\sqrt{n}} \)?
**General Case**

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

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

---

**Verifier**

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

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

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

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

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

---

**Prover**

Yes s.t. $h(x) \oplus y = y_i$
Private Coin $\rightarrow$ Public Coin

Private Coin Verifier $V$:

1. Pick $R$ at random

2. Computes $q = q(R)$

\[ q \in \mathbb{Z}_N^k \]

Prover

Acceptable

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

Verifies $(a, R, a)$
Issue: "Acceptability" of "a" function of "R" not "q".

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

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

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

$N$ known to verifier

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

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

Using [GJS] protocol.

(Works for simple case)
But in general:

**YES**: \(|S_q, a| \geq N_q^t\)

↑

depends on \(q\)!

not known to verifier! :(

**Solution**: Prover tells us "typical" value of \(N_q = N\)

\(\ell\) proves \(\#\{q \mid N_q \geq N^t\} \geq 2^n \cdot \frac{1}{N^{2n}}\)

How? Using \([65]\) twice.
Verifier

Prover

\[ N \]

\[ \text{/* Verify } \left| \sum q_i \right| N_q \geq N \text{?} \implies \ldots \text{ */} \]

\[ h(m, h(m, \ldots, h(m, h(m, x) \oplus y))) \]

\[ y_i \ldots y_k \]

\[ y \]

\[ g_0, i \]

\[ \text{/* Verify } N_{g_0} \geq N \text{ */} \]

\[ [G1S] \text{ again} \]
Am:

• An induct on previous idea to convert any k-round private protocol to 10-k round public protocol.

• $IP(0(n)) = Am(0(n))$.

• But $AM Am Am Am = BP \cdot E \cdot BP \cdot E \cdot BP \cdot E$.

• A la [Toda]: $\leq BP \cdot BP \cdot BP \cdot E \cdot E \cdot E \cdot P = BP \cdot E \cdot P = AM[2]$.  

• $\Rightarrow IP(0(n)) = Am$.

• $Am \subseteq NP/poly$ [Adleman].

• If $NP$-complete then $coSAT \subseteq NP/poly$. 
Next Agenda Item: \(1P = \text{PSPACE}\)

History (according to me):

Lipton '90: Permanent is "random self-reducible"

(reduces to random instances of itself)

Burr '90: RSR a downward self-reducible functions are "checkable"

[applied to modular mult. ...]

Nisan: \(2 + 2 = 4\)

Permanent is RSR \(\implies\) Permanent is "checkable"
LFKN: Permanent $\in IP$.

Rest of lecture: Proof

Ingredient 1: RSR of permanent.

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

$$\Pr \left[ \text{mrep}(R) = \text{perm}(R) \right] > 1 - \delta$$

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

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

$$M_i = A + i \cdot R$$
- Define $M_0 = A$; $M_i$ = random for all $i$.

- Let $Y_i = \text{mrep}(M_i)$, $i = 1 \ldots n+1$.

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

\[ p(i) = Y_i, \quad i = 1 \ldots n+1 \]

- Output $p(0)$.

Claim: For $i \neq 1$

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

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

Claim: If $i \neq 1$, $Y_i = \text{perm}(M_i)$, then $p(x) = \text{perm}(M_{x+1})$.

So $p(0) = \text{perm}(A)$, deg $n$ poly; agree at $i=1$. 
\[ \text{DSSR}: \text{ let } A_1, \ldots, A_n \text{ be minors of } A \]

\[ \text{then } \text{Perm}(A) = \sum_{i=1}^{n} A_{i} \text{ perm}(A_{i}) \]

What follows *builds on* and doesn't follow from the above

-----

Verifier \[ A \]

\[ \text{perm}(A) = \beta \]

Prover

let \( A_1, \ldots, A_n \) be minors.

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

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

\[ b_{ij}(k) = (A_{k})_{ij} \]
\[
\text{perm}(B(x)) = ?
\]
\[
\xrightarrow{h(x)}
\]
\[
\xleftarrow{\text{poly of degree } n^2}
\]

\text{Cases:}

1. \( h(x) = \text{perm}(B(x)) \) (but \( \rho \neq \text{Perm}(A_i) \))

\[
\rho \neq \text{perm}(A_i) = \leq a_{i1} \cdot \text{Perm}(A_i)
\]
\[
= \leq a_{i1} \cdot \text{perm}(B(i))
\]
\[
= \leq a_{i1} \cdot h(i)
\]

Reject if so: \( \rho \neq \leq a_{i1} \cdot h(i) \)

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

\( \uparrow \)

Also if \( \text{deg} \leq n^2 \)

Disagree \( \Rightarrow \ h(r) = \tilde{h}(r) \) for \( p-n^2 \) choices of \( r \)
Pick \( r \in \mathbb{Z}_p \)

\[ \gamma \]

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

\[ \uparrow \]

known to verifier smaller.

\[ \uparrow \]

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