Set lower bound IP

Lecture 20

Goldwasser-Sipser

- Some set S
  Known to P, and V

- P knows S explicitly
- V can certify membership in S w/ a certificate.
- Protocol: Prove that $|S| \geq K$ w/ public coins
- Guarantees:
  1. If $|S| \geq K$, V accepts w.p. $\geq 2/3$
  2. If $|S| \leq K/2$, then

V rejects w.p. $\geq 2/3$
for <u>any</u> Prover strategy.

Pairwise-Independent Hash Functions

- $\mathcal{H}_{n,k}$ is a family of functions
  $h : \{0,1\}^n \longrightarrow \{0,1\}^k$.
- $\mathcal{H}_{n,k}$ is pairwise-independent
  if $\forall x \neq x' \in \{0,1\}^n$,
  $\forall y, y' \in \{0,1\}^k$

$$\Pr_{h \xleftarrow{R} \mathcal{H}_{n,k}} [h(x) = y \text{ and } h(x') = y'] = 2^{-2k}$$

Ex: Let $\mathbb{F} = GF(2^n)$ (finite field of order 2^n). Then

$$\mathbb{F}_2[X] / (X^n + X + 1)$$

$$\mathcal{H}_{n,n} := \left\{ h : \{0,1\}^n \to \{0,1\}^n \;\middle|\; h(x) = ax + b \right\}$$

is a pairwise-indep. hash family.

Set LB Protocol

Setup

- $S \subseteq \{0,1\}^m$ w/ efficient membership certification
- $K \in \mathbb{Z}^+$ parameter, $l \in \mathbb{Z}^+$

s.t. $2^{l-2} < K \leq 2^{l-1}$

- $\mathcal{H}_{m,l}$ PIHF

Goal: If $|S| \geq K$, V accepts w.p. $\geq 2/3$; if $|S| \leq K/2$, V rejects w.p. $\geq 2/3$.

Protocol

P	V
	$h \xleftarrow{\$} \mathcal{H}_{m,l}$
	$y \xleftarrow{\$} \{0,1\}^l$
	$\xleftarrow{(h,y)}$
• Find $x \in S$ s.t. $h(x)=y$ (easy)	
• Certificate w for "$x \in S$"	$\xrightarrow{(x,w)}$
	If $h(x)=y$ and w certifies $x \in S$

output accept.

Claim: If $|S| \leq \frac{2^\ell}{2}$, then for $p = |S|/2^\ell$,

$$\frac{3}{4}p \leq \Pr_{h,y}\left[\exists x \in S : h(x) = y\right] \leq p.$$

$$h \in \mathcal{H}_{m,\ell} \; ; \; y \in \{0,1\}^\ell$$

Proof:

① $\Pr_{h,y}\left[\exists x \in S : h(x) = y\right] \leq p$

- $\forall h, \; |h(S)| \leq |S|$

$$\Rightarrow \Pr_{h,y}\left[\exists x \in S : h(x) = y\right] \leq \frac{|S|}{2^\ell} = p$$

(2) Lower Bound

- For $x \in S$, let E_x be the event "$h(x) = y$"
- $\Pr_{h,y}[\exists x \in S : E_x]$

$$= \Pr_{h,y}\left[\bigcup_{x \in S} E_x\right]$$

inclusion-exclusion

$$\geq \sum_{x \in S} \Pr_{h,y}[E_x] - \frac{1}{2} \sum_{x \neq x' \in S} \Pr_{h,y}[E_x \cap E_{x'}]$$

$E_x :=$ $h(x) = y$

$E_x \cap E_{x'} :=$ $h(x)=y$ and $h(x')=y$

$x \neq x'$

$$\Pr[E_x \cap E_{x'}] = 2^{-2k}$$

$\Pr[E_x] = 2^{-\ell}$ /

Therefore

$$\geq \sum_{x \in S} \sum_{h,y} \Pr[E_x]$$

$$- \frac{1}{2} \sum_{x \neq x' \in S} \sum_{h,y} \Pr[E_x \cap E_{x'}]$$

$$\geq \frac{|S|}{2^{\ell}} - \frac{1}{2} \frac{|S|^2}{2^{-2\ell}}$$

$$= \frac{|S|}{2^{\ell}} \left(1 - \frac{|S|}{2^{\ell+1}}\right) \geq \frac{3}{4} \cdot \frac{|S|}{2^{\ell}}$$

$$= \frac{3}{4} \cdot P \quad \square$$

* what does this tell us?

- $2^{\ell-2} < K \leq 2^{\ell-1}$

① If $|S| = K \leq 2^{\ell-1} = \frac{2^\ell}{2}$

honest/completeness

$\rightarrow \Pr_{h,y}[\exists x \in S : h(x) = y] \geq \frac{3}{4} \cdot \frac{|S|}{2^\ell}$

$= \frac{3}{4} \cdot \frac{K}{2^\ell}$

$\geq \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{16}$

can boost to $\geq 2/3$ w/ constant # of invocations in parallel.

② If $|S| \leq \frac{K}{2}$

$\Pr_{h,y}[\exists x \in S : h(x) = y] \leq \frac{|S|}{2^\ell}$

$\leq \frac{K}{2^{\ell+1}}$

$$\leq \frac{2^{k-1}}{2^{k+1}} = \frac{1}{4} < \frac{1}{3}$$

Final GNI Public-coin Protocol

- $S = \{ (H, \pi) : (H \cong G_0 \text{ or } H \cong G_1) \text{ and } \pi \in aut(H) \}$

$\pi \in aut(H) \Rightarrow$

$\pi(H) = H$ and

π is not identity.

$\Rightarrow$ handles when G_0 or G_1 have $< n!$ equivalent graphs

$\Rightarrow$ $|S| = n!$ if $G_0 \cong G_1$

$|S| = 2n!$ if $G_0 \ncong G_1$

* Prove $G_0 \ncong G_1$

- **Setup**
  - $k = 2n!$, l s.t.
    $2^{l-2} < k \leq 2^{l-1}$
  - $\mathcal{H}_{m,l}$ PIHF
    m is max # bits to encode any $(H, \pi) \in S$

P	V
	$h \xleftarrow{\$} \mathcal{H}_{m,l}$
$\xleftarrow{(h, m)}$	$y \xleftarrow{\$} \{0,1\}^m$

- Find
  (H, π) s.t.
  $h(H, \pi) = y$
- σ s.t.
  $\sigma(H) = G_0$
  or
  $\sigma(H) = G_1$.

$\xrightarrow{H, \pi, \sigma}$

Verification

1. $h(H, \pi) = y$
2. $\pi(H) = H$
3. $\pi \neq id$

(2) $\sigma(H) = G_0$ xor $\sigma(H) = G_1$

Theorem

GNI $\in$ AM[2]

Arthur-Merlin Protocols

Def. For any $k \geq 2$,

$AM[k] \subseteq IP[\lceil k/2 \rceil]$, s.t.

(1) V sends the first message

② All of V's messages are uniformly random and indep.

③ V's output only depends on these sent random coins + P's messages. + common input

$AM[2] = AM$ $\quad AM[2k] = AM \cdots AM$

$AM[3] = AMA$ $\quad \therefore AM[2k+1] = AM \cdots AMA$

$AM[4] = AMAM$

$MA[k]$ → identical to $AM[k]$ but M/P speaks first

- $AM = AM[2]$
- $MA = MA[2]$

AM properties

① P doesn't see all randomness from V at once.

② $AM = BP \cdot NP = \{L \leq_r 3SAT\}$

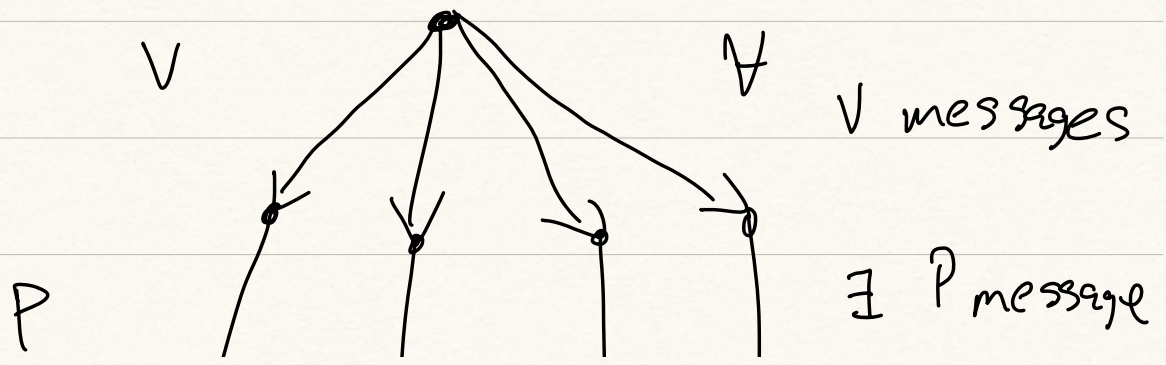
$AM[2]$ (HW)

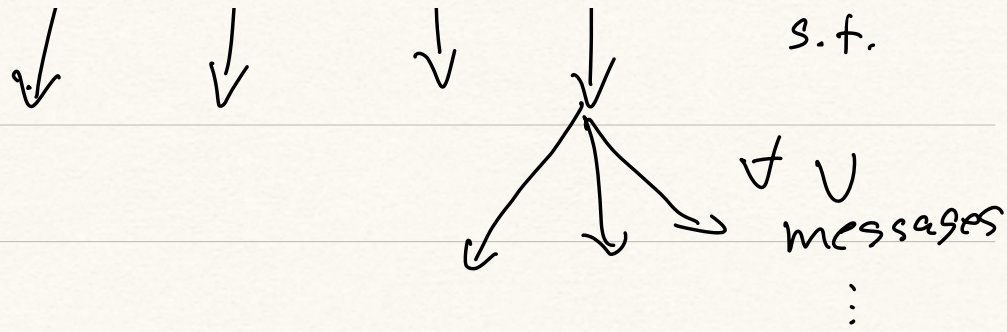
in particular, $AM \subseteq \Sigma_3^P$

③ $\forall k = \Theta(1) \geq 2$

$AM[k] = AM[2]$.

Surprising since $AM[k]$ has a Π_k^P-like structure





(4) For $\sigma(n)$ slow growing ($\sigma(n) = \log\log(n)$), unknown if $AM[\sigma(n)]$ has nice characterization.

- Public and Private coins are equivalent.
- By definition, $AM[k] \subseteq IP[k']$ $k' = \lceil k/2 \rceil$

- **Theorem**: $IP[k'] \subseteq AM[k+2]$ for $k(n)$ computable in poly(n) time and $k' = \lceil k/2 \rceil$.