Today

- TQBF $\subseteq$ IP (Complete Proofs)
- Arthur-Merlin Proof Systems
  - * AM, MA
  - * Properties
- Public Coins = Private Coins [Goldwasser-Sipser]
- Is GI NP-complete?

Lecture 23

Computational Complexity

(28 April, 2020)

Instructor: Prahladh Harsha

TQBF $\subseteq$ IP

Key Step

φ formula (3CNF) — m clauses, n variables $\longrightarrow$ P_φ polynomial, deg $\leq 3m$

$\forall x \in \{0,1\}^n$ $P_\varphi(x) = \varphi(x)$

Extended to quantified Boolean formula

$\psi = \exists x_1 \forall x_2 \ldots \varphi(x_1 \ldots x_n)$

Def of P_φ

1. Constant c: $P_\varphi := c$
2. Var x: $P_\varphi := x$
3. Neg $\neg\psi$: $P_\varphi = 1 - P_\psi$
4. Conj: $\varphi = \psi_1 \wedge \psi_2 \ldots \wedge \psi_m$: $P_\varphi := \prod P_{\psi_i}$
5. Disj: $\varphi = \psi_1 \vee \ldots \vee \psi_m$: $\varphi := \overline{\overline{\psi_1} \wedge \ldots \wedge \overline{\psi_m}}$

$\psi = Q_1 x_1 \, Q_2 x_2 \ldots \quad Q_\ell x_\ell \; \varphi(x_1 \ldots x_n)$

$Q_i \in \{\exists, \forall\}$.

$\psi = \forall x \; \varphi(x, y)$

$P_\psi := P_\varphi(0,y) \cdot P_\varphi(1,y)$

$\mathcal{Q}_{\forall x_1}$

$\psi = \exists x \; \varphi(x, y)$

$P_\psi := 1 - (1 - P_\varphi(0,y)) \cdot (1 - P_\varphi(1,y))$

$\mathcal{Q}_{\exists x_1}$

TQBF: Goal ψ $\quad \psi \equiv 1 ?$ $\quad P_\psi \equiv 1 ?$

Problem: Degree could blowup to as large as $2^\ell \cdot 3^n$

Introduced a Linearization Operation to control degree

$L_{x_1} P(x_1 \ldots x_n) := x_1 P(1, x_2 \ldots x_n) + (1 - x_1) P(0, x_2 \ldots x_n)$

Prop ① $(L_{x_1} P)(b) = P(b) \quad \forall b \in \{0,1\}^n$

② $\deg_{x_1}(L_{x_1} P) \le 1$

$\psi = \exists x_1 \, \forall x_2 . \exists x_3 \; \varphi(x_1, x_2 x_3)$

$\mathcal{Q}_{\exists x_1} \mathcal{Q}_{\forall x_2} \mathcal{Q}_{\exists x_3} P_\varphi(x_1, x_2, x_3)$

$P_\psi \equiv \mathcal{Q}_{\exists x_1} L_{x_1} \mathcal{Q}_{\forall x_2} L_{x_2} L_{x_1} \mathcal{Q}_{\exists x_3} L_{x_3} L_{x_2} L_{x_1} P_\varphi(x_1, x_2, x_3)$

Degree of all intermediate poly $\leq 3m$.

$\overline{Q}$ ... $Q_{\exists x_1} Q_{\forall x_2} Q_{\exists x_1} p_\varphi(x_1 \ldots x_n)$

$g(x_1 .. x_s)$ - be any such intermediate poly on vars $x_1 \ldots x_s$ a t operators

Claim: we have $\forall (a_1 .. a_s) \in \mathbb{F}^s$ & $c \in \mathbb{F}$ there is a protocol s

- $g(a_1 .. a_s) = c$ - Protocol accepts w/p 1
- $g(a_1 .. a_s) \neq c$ - Protocol acc w/p $\leq \varepsilon(m)$

By induction on # operators.

$$\varepsilon(m) = \frac{md}{|\mathbb{F}|}$$

$m = 0$ ✓ No need for prover.

$f(\ ) = Q_x g(x, y_1)$

Case(i) $Q_x = Q_{\forall x_1}$

$f(y) = Q_{\forall x} g(x, y) = g(0, y) \cdot g(1, y)$.

$f(\bar{a}) = C$

(V) (P)

$\xleftarrow{p}$ $\quad p := g(x, \bar{a})$

$p(0) \cdot p(1) = C$

$r \in_R \mathbb{F} \xrightarrow{r}$ $\quad \varepsilon(m+1) = \varepsilon(m) + \frac{d}{|\mathbb{F}|}$

"$g(r, \bar{a}) = p(r)$"

Case (ii) $Q_x = Q_{2x}$

$f(y) = Q_{2x} g(x, y) = (1 - (1 - g(1, y)))(1 - g(0, y))$

Case (iii) $Q_x = Q_{1x}$

$f(x, \bar{y}) = L_x g(x, y) = x \cdot g(1, y) + (1 - x) \cdot g(0, y)$.

$f(\alpha, \bar{a}) = C$

(V) (P)

$\xleftarrow{p}$ $\quad p := g(x, \bar{a})$

$C = \alpha g(1, \bar{a}) + (1 - \alpha) g(0, \bar{a})$

$r \in_R \mathbb{F}_q \xrightarrow{r}$ $\quad \varepsilon(t+1) \leq \varepsilon(t) + \frac{d}{|\mathbb{F}_q|}$.

"$g(r, \bar{a}) = p(r)$"

Total errors. $\varepsilon(t) \leq \frac{td}{|\mathbb{F}|}$ ☒

IP = PSPACE — Public Coins Protocol.

GNI protocol - Private Coins Protocol.

Public Coins Interactive Proofs:

Arthur (Verifier) — Merlin (Prover) — Proof Systems

Averaging — Maximizing

AM[k(n)] = {L | L has a public coins IP protocol w/ atmost k(n) rounds}.

Properties:

(1) PSPACE ⊆ AM[poly] = IP[poly]
(IP - private coins).

(2) IP[k(n)] ⊆ AM[k(n)+2]
private coins protocol — public coins protocol.

Cor: GNI ∈ AM[4]

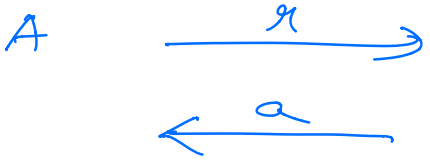
(3) ∀ constants k
AM[k] ⊆ AM[2]

Cor: GNI ∈ AM[2] = AM

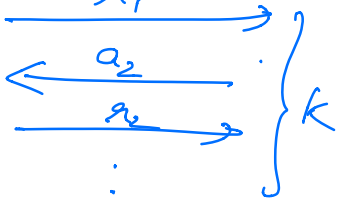
(4) AM[k(n)] - has perfect completeness.

① ✓ ; ② – no class ; ③ = ④ – open.

AM[2]



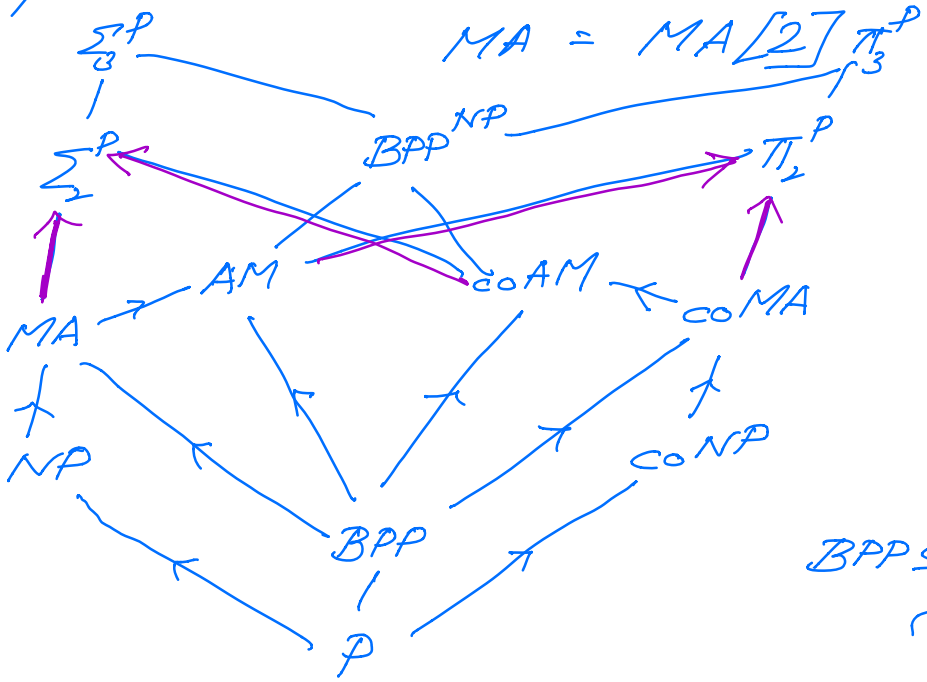
AM[k]



MA

r.

Two specific classes: $AM = AM[2]$, $MA = MA[2]$



$BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

Thm: If $coNP \subseteq AM$, $PH = AM \subseteq \Pi_2^P$

Pf: $\Sigma_2^P = \exists x \forall y \, \varphi(x,y)$ - -

MAM- protocol for Σ_2^P.

$\underbrace{\exists x}_{\text{Merlin}} \quad \underbrace{\forall y \; \phi(x,y)}_{\text{coNP stmt}}$

↳ AM protocol assumption

$coNP \subseteq AM \Rightarrow \Sigma_2^P \subseteq MAM \subseteq AM$

Round redn.

$\Sigma_2^P \subseteq AM \subseteq \Pi_2^P \Rightarrow$ PH collapses to Σ_2^P. ☒

Cor: If GI is NP-complete, then $PH = \Sigma_2^P$

Pf: $\overline{GNI} \subseteq AM$

GNI is coNP-complete (by assumption)

This will imply $coNP \subseteq AM$

Then PH collapses to Σ_2^P. ☒

(3 different proofs, 1- aGore, 2- pset)
3- Arora Barak

Next: Public Coins = Private Coins.

Specific Case: GNI - Public Coins Protocol.

(G_0, G_1) $\quad |V(G_0)| = |V(G_1)| = n$

(V) (P)

$b \in_R \{0,1\}$.
$\sigma \in_R S_n$
$H \leftarrow \sigma(G_b)$

$H \longrightarrow$ Compute c s.t $H \cong G_c$.
$c \longleftarrow$
$c = b$ ✓

Private Coins Protocol

Goldwasser-Sipser:
An alternate 2/3 round protocol. w/ public coins that shows $GNI \in AM[3]$.

Proof Contd in next lecture ☒