Today

Interactive Proofs (Part III)

- $P^{\#P} \subseteq IP$
- $IP = PSPACE$

CSS.203.1 Computational Complexity

- Lecture # 24 (12 May 21)

Instructor: Prahladh Harsha

Recap. $\#SAT_D = \{(\varphi, k) \mid \varphi$ in 3CNF form, $\#SAT(\varphi) = k\}$.

Want to prove: $\#SAT_D \in IP$.

What does it mean to say $L \in IP$

$x \in L$

$V \quad\quad P$

Next message fn

$V \xrightarrow{q_1} P$

$V \xleftarrow{a_1} P$

$\vdots$

$V \xleftarrow{a_{i-1}} P$

$V \xrightarrow{q_i} P$

$q_i = V(x; R_1 .. R_i, a_1 ... a_{i-1})$

(1) Efficiency (Next message fn computable in poly time in $|x|$.

(2) Completeness:

$x \in L \Rightarrow \exists$ Prover P

$$\Pr_R[(V \leftrightarrow P)(x;R) = acc] \geq 2/3$$

(3) Soundness

$x \notin L \Rightarrow \forall$ Prover P^*

$$\Pr_R[(V \leftrightarrow P^*)(x;R) = acc] \leq 1/3.$$

Arithmetization

(Low-degree polynomial representation of a Boolean function)

φ 3CNF formula $\longmapsto$ P_φ polynomial

$\forall b_1 \dots b_n \in \{0,1\}^n$

$$\varphi(b_1 \dots b_n) = P_\varphi(b_1 \dots b_n)$$

Notice for $\alpha_1 \dots \alpha_n \in \mathbb{F}^n \setminus \{0,1\}^n$

$\varphi(\alpha_1 \dots \alpha_n)$ - not defined

however $P_\varphi(\alpha_1 \dots \alpha_n)$ - well defined.

Definition of P_φ

Inductively.

(0) φ - constant 0/1

$P_\varphi \leftarrow$ constant 0/1.

(2) Variables.

φ - x_i

$P_\varphi \leftarrow x_i$

(3) Negations

$\varphi = \neg \psi$ | $P_\varphi \leftarrow 1 - P_\psi$

(4) Conjunctions.

$\varphi = \psi_1 \wedge \psi_2$ / $P_\varphi \leftarrow P_{\psi_1} \cdot P_{\psi_2}$

(5) Disjunctions

$\varphi = \psi_1 \vee \psi_2$

$= \neg[(\neg\psi_1) \wedge (\neg\psi_2)]$ / $P_\varphi \leftarrow 1 - (1-P_{\psi_1})(1-P_{\psi_2})$

φ - 3CNF formula.

m clauses

$\varphi = C_1 \wedge C_2 \ldots \wedge C_m$

where each $C_i = x_4 \vee \overline{x_2} \vee x_3$

P_φ - $\deg(P_\varphi)$?

$C = x_1 \vee x_2 \vee \overline{x_3}$

$\deg(P_C) \leq 3$

$\deg(P_\varphi) \leq 3m$

By construction, P_φ & φ agree on Boolean values.

Want to give an IP-protocol.

"$\displaystyle\sum_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \cdots \sum_{b_n \in \{0,1\}} \varphi(b_1 \ldots b_n) = k$"

Suffices to

$$\sum_{b_1\in\{0,1\}}\sum_{b_2\in\{0,1\}}\cdots\sum_{b_n\in\{0,1\}} P_\varphi(b_1\ldots b_n) = k \quad \ldots (*)$$

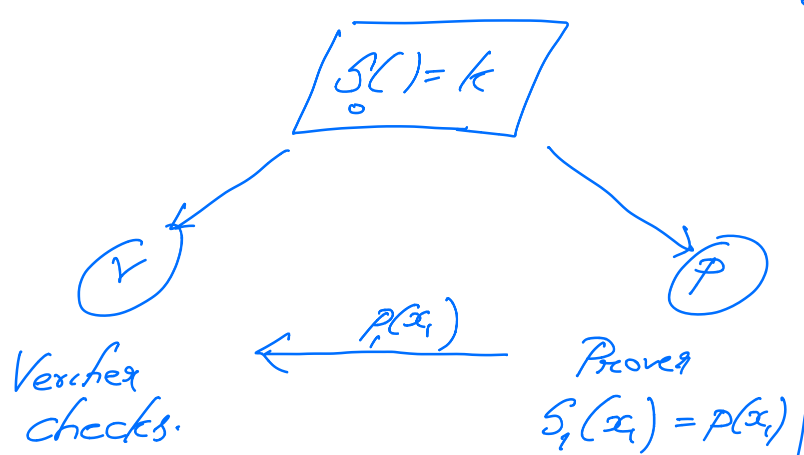
Work w/ some (suitably large) finite field $\mathbb{F}$.

Notation: $S_i(\alpha_1 \ldots \alpha_i)$

$$S_i(\alpha_1\ldots\alpha_i) \triangleq \sum_{b_{i+1}\in\{0,1\}}\sum_{b_{i+2}\in\{0,1\}}\cdots\sum_{b_n\in\{0,1\}} P_\varphi(\alpha_1\ldots\alpha_i, b_{i+1}\ldots b_n)$$

$(*)$ is equivalent to "$S_0() = k$"

We will give an IP-protocol for "$S_i(\alpha_1\ldots\alpha_i) = k_i$" for any $i\in[n]$, $\alpha_1\ldots\alpha_i\in\mathbb{F}$, $k_i\in\mathbb{F}$



$S_0()$

$= S_1(0) + S_1(1)$

$S_i(\alpha_1\ldots\alpha_i)$

$= S_{i+1}(\alpha_1\ldots\alpha_i, 0)$

$+ S_{i+1}(\alpha_1\ldots\alpha_i, 1)$

$k = p_1(0) + p_1(1)$

$r_1 \in_R \mathbb{F} \xrightarrow{r_1}$

"$S_1(r_1) = p_1(r_1)$"

$S_1(r_1) = S_2(r_1, 0) + S_2(r_1, 1)$

$\xleftarrow{p_2(x_2)}$ $p_2(x_2) = S_1(r_1, x_2)$

L

$p_1(r_1) = p_2(0) + p_2(1)$

$r_2 \in_R \mathbb{F}$ - $\xrightarrow{r_2}$

"$S_2(r_1, r_2) = p_2(r_2)$"

At the last round $r_n \in \mathbb{F}$

$S(r_1 \dots r_n)$
$= P_\varphi(r_1 .. r_n)$

Verifier does not employ the prover.

Efficiency

Each of the poly p_i is of degree at most $3m$

Hence, all transcripts are of poly length.

$(\varphi, k) \in \#SAT_D$

Completeness : There is an honest prover P s.t

$$\Pr_{R = r_1 \dots r_n} [(V \leftrightarrow P)((\varphi, k), R) = acc] = 1.$$

Soundness: $(\varphi, k) \notin \#SAT_D$

P^* – any prover.

$$\Pr_{R = r_1 \ldots r_n} \left[(V \leftrightarrow P^*)((\varphi, k), R) = acc \right]$$

$$\geq \underbrace{\left(1 - \frac{d}{q}\right)\left(1 - \frac{d}{q}\right) \cdots \left(1 - \frac{d}{q}\right)}_{n}$$

d = max deg of all poly

q – size of field.

$$\geq \left(1 - \frac{d}{q}\right)^n \geq 1 - \frac{nd}{q} \geq 0.99$$

if $q \geq 100nd$

$= 100 \cdot n \, 3m$

$= 300mn$

So far. $\boxtimes$

$$P^{\#P} \subseteq IP \subseteq PSPACE$$

Theorem [Lund-Fortnow-Karloff-Nisan; Shamir]

$IP = PSPACE$

(ie, $TQBF \in IP$)

Pf: ψ is an instance of TQBF

$$\psi = \exists x_1 \forall x_2 \exists x_3 \exists x_4 \quad \forall x \ \underbrace{\varphi(x_1 \dots x_m)}_{\text{3CNF formula}}$$

TQBF - true quantified Boolean formulae.

$$\exists x_1 \ \forall x_2 \ \dots \quad \exists x_n \ \underbrace{\varphi(x_1 \dots x_n)}$$

$\downarrow$ arithmetize

$$P_\varphi(x_1 \dots x_n)$$

Extend arithmetization to (partially) quantified Boolean formulae.

Induction.

ψ.

(0) ψ - no quantifiers

P_ψ - obtained as before

(1) $\psi = \forall x \ \varphi(x)$

$$P_\psi = P_\varphi(0) \cdot P_\varphi(1)$$

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

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

(2) $\psi = \exists x\, \varphi(x)$

$$P_\psi = 1 - (1 - P_\varphi(0))(1 - P_\varphi(1))$$

Input: $\psi = Q_1 x_1\, Q_2 x_2 \ldots Q_n x_n\, \varphi(x_1 \ldots x_n)$

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

Want to check "$P_\psi = 1$"

. . .

"$P_\psi = 1$"

V $\qquad\qquad\qquad$ P

$P_1(x_1)$

Checks

$1 = P_1(0) \cdot P_1(1)$

$P_1(x_1) = P_\varphi(x_1)$

$r_1 \in_R \mathbb{F}$ $\qquad$ r_1

"$P_\varphi(r_1) = P_1(r_1)$"

$\psi = \forall x_1\, \varphi(x_1)$

$P_\psi = P_\varphi(0) \cdot P_\varphi(1)$

Completeness ✓

Soundness ✓

Efficiency: $\psi = Q \ldots \ldots \quad \varphi(\quad)$

$\deg(P_\varphi) \le 3m$ ✓

Each application of quantifier (from right) doubles degree.

Final polynomial can have degree as large as $\underbrace{2^n \cdot 3m}_{\text{prohibitively large}}$

☹

Idea: Modify the protocol so that the degrees do not blow up.

Arithmetization - polynomial s.t on Boolean values matches w/ original fn

p - Univariate poly (of possibly large degree)

$$q(x) := x \cdot p(1) + (1-x) \cdot p(0)$$

(1) $\deg_x(q) \le 1$

(2) $q(0) = p(0)$; $q(1) = p(1)$

$$p(x) \xmapsto{L_x} x\,p(1) + (1-x)\,p(0)$$

Linearizing Operator:

$$L_x\, p(x) \triangleq q(x)$$

Input: $\psi = Q_1 x_1 Q_2 x_2 \ldots \quad Q_n x_n\, \varphi(x_1 \ldots x_n)$

$$\downarrow$$

$$P_{Q_1 x_1} \ldots \quad \ldots \quad P_{Q_{n-1} x_{n-1}}\, P_{Q_n x_n}\, P_\varphi(x_1 \ldots x_n)$$

$$P_{Q_1 x_1} \ldots P_{Q_{n-1} x_1} L_{x_1} \ldots L_{x_{n-1}} P_{Q_n x_n} \underbrace{L_{x_1} \ldots L_{x_{n-1}} L_{x_n} P_\varphi(x_1 \ldots x_n)}_{\substack{\text{individual degree in} \\ \text{each var } \le 1 \\ \text{(Hence total deg } \le n)}}$$

Polynomial Operations: $n+1$

$$\begin{aligned} &+ (n-1) + 1 \\ &+ (n-2) + 1 \quad = O(n^2) \\ &\\ &+ (n-n) + 1 \end{aligned}$$

Degree of any intermediate poly $\le \max\{3m, 2n\}$.

$$P_\psi = \overbrace{\mathcal{O}_{Q_1 x_1}\, \mathcal{O}_{Q_2 x_1} \ldots \quad \mathcal{O}_{Q_m x_m}}^{m}\, P_\varphi$$

where each $\mathcal{O}_{Q_i x_i} = \begin{cases} L_{x_i} - \text{linearing} \\ \exists x_i - \text{existential} \\ \forall x_i - \text{universal.} \end{cases}$

$g(x_1 .. x_s)$ - be any such intermediate poly on vars $x_1 .. x_s$.

<u>Claim</u>: $\forall (a_1 . a_s) \in \mathbb{F}^s$ & $C \in \mathbb{F}$ there is an IP-protocol s.t. (efficient).

- Case (i) $g_s(a_1 .. a_s) = C$: Protocol accepts w/ prob 1
- Case (ii) $g_s(a_1 .. a_s) \neq C$: Protocol accepts w/ prob. $\leq \varepsilon(m)$

$$\varepsilon(m) = \frac{md}{q}$$

So far.

IP - new model of proof verification

GNI - IP-protocol Private Coins

PSPACE - IP protocol Public Coins
perm
#P

Public-Coins Interactive Proofs.

Arthur (verifier) Merlin (Prover) Proof Systems

$AM[k(n)] = \{L \mid L$ has a public coin IP protocol w/ at most $k(n)$ rounds$\}$

$IP[k(n)]$ -

$GNI \in IP[1]$

$PSPACE \subseteq AM[poly] \subseteq IP[poly]$

Properties:

(1) $PSPACE \subseteq AM[poly] \subseteq IP[poly] \subseteq PSPACE$

(2) Public Coins vs Private Coins

$\underbrace{IP[k(n)]}_{\text{private coins protocol}} \subseteq \underbrace{AM[k(n)+1]}_{\text{public coins}}$

Corollary: $GNI \subseteq IP[1] \subseteq AM[2]$

(3) $\forall$ constants k.

$AM[k] \subseteq AM[1]$

Cor: $GNI \subseteq AM[1] = AM$

(4) $AM[k(n)]$ - perfect completeness

(1) ✓ ; (2) - in class ; (3) & (4) - Pset 5.