Interactive Proof Systems

21 May, 2021 14:44

- Given set $A \subseteq \{0,1\}^n$

Verifier wants to verify that some $x \in \{0,1\}^*$ belongs to A.
Prover comes and tries to convince verifier that $x \in A$.
The system should be s.t. for $x \in A$, verifier gets convinced with high probability, for $x \notin A$, verifier shouldn't get convinced no matter how persuasive the prover is (except for small error.)

Ex: A) $A = SAT$

1) Verifier gets formula φ
2) Prover send a satisfying assignment a
3) Verifier gets convinced (ACCEPTS) if $\varphi(a)$ is true.

$\varphi \in SAT \Rightarrow$ good prover convinces w.p. $=1$
$\varphi \notin SAT \Rightarrow$ no prover can convince the verifier

B) $A = \overline{SAT}$

Verifier? Prover?

Want: Efficient Verifier, all-powerful prover

C) $GI = \{ (G,H) ;\ G \,\&\, H$ are two isomorphic graphs: $G \cong H$ if

$\exists \pi : V(G) \xrightarrow[\text{onto}]{1-1} V(H)$

s.t. $\forall u, v \in V(G)$

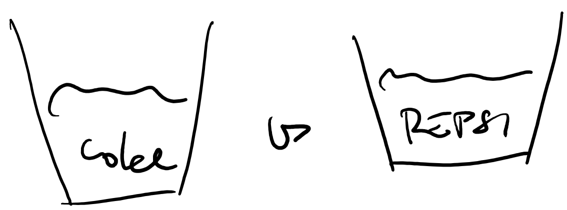
$(u,v) \in E(G) \Leftrightarrow (\pi(u), \pi(v)) \in E(H)$

Verifier gets (G, H)

Prover sends some $\pi : V(G) \to V(H)$

Verifier ACCEPTS if π is an isomorphism of G & H

D)



E) $\text{GnonI} = \{ (G, H) ; \; G \not\cong H \}$

Verifier gets (G, H), picks one of them at random, permutes it @ random and sends it to prover.

Prover determines whether verifier sent a permutation of G or H.

Verifier ACCEPTS if prover determined the graph correctly.

If $G \not\cong H$ then verifier ACCEPTS with prob. 1

If $G \cong H$ the prover has chance at most $1/2$

to convince the Verifier to ACCEPT.

If we repeat the protocol k-times & Verifier ACCEPT if prover determines the graph correctly in each iteration then

For $G \not\cong H$ the Verifier ACCEPTS w.p. 1.

For $G \cong H$ the Verifier ACCEPTS w.p. $\leq \frac{1}{2^k}$ no matter what prover does.

<u>Def:</u> Verifier is a fcn $V : \{0,1\}^* \times \{0,1\}^* \times \{0,1,\#\}^* \to \{0,1\}^* \cup \{ACC, REJ\}$

which is poly-time computable, more precisely, for some polynomial $p : \mathbb{N} \to \mathbb{N}$, on input (x, r, M) it is computable in time $p(|x|)$ where for $|r| > p(|x|)$ or $|M| > p(|x|)$ it returns REJECT.

Prover is an arbitrary fcn $P : \{0,1\}^* \times \{0,1,\#\}^* \to \{0,1\}^*$

x ... the actual input for which we want to verify its property

r ... a string of $\leq p(n)$ random bits

M ... transcript of conversation between prover & verifier

prover gets the input (x, M).

Interaction between P & V proceeds in rounds.

In round i:

case even i) $V(x, r, m_1 \# m_2 \# \cdots \# m_i) \to m_{i+1}$

case odd i) $P(x, m_1 \# m_2 \cdots \# m_i) \to m_{i+1}$

Once V outputs $m_{i+1} = ACC$ or REJ, the interaction stops & V is either convinced (ACC) or not (REJ).
$\Rightarrow$ output $:= m_{i+1}$

- We denote $V \leftrightarrow P\ (x, r)$ the output of the conversation between V & P on input x with random bits r.

- Def: $A \subseteq \{0,1\}^*$ has an interactive proof system if $\exists$ verifier V & prover P s.t.

$$\forall x \in A \qquad Pr_{r \in \{0,1\}^{p(n)}}[V \leftrightarrow P(x,r) \text{ accepts}] \geq \tfrac{2}{3}$$

$$\forall x \notin A \qquad Pr_{r \in \{0,1\}^{p(n)}}[V \leftrightarrow P(x,r) \text{ accepts}] \leq \tfrac{1}{3}$$

$$IP = \{ A \subseteq \{0,1\}^*,\ A \text{ has an interactive proof system} \}$$

- Observation: $SAT \in IP$ $\qquad NP \subseteq IP$
  $GI \in IP$
  $GnonI \in IP$

- Thm: $IP = PSPACE$

Pf: $IP \subseteq PSPACE$ $\qquad$ $A \in IP$, V, P are for A

tree of conversations between V & P on input x

For each partial conversation $M = m_1 \# m_2 \# \dots \# m_{2i+1}$

P wants to maximize its chances V accepts

So he selects as the next message the message m_{2i}, which maximizes the # of random bits r, that will lead to accepting outcome of the interaction.

- def $N_{x,M}$ = the # of random strings $r \in \{0,1\}^{p(n)}$ which are consistent with the verifier V on input x & transcript $M = m_1 \# m_2 \dots \# m_i$

i.e. such r so $\forall j < i$, j even : $V(x, r, m_1 \# m_2 \dots \# m_j) = m_{j+1}$

- given a verifier V & input $x \in \{0,1\}^n$ we want to determine in PSPACE the maximal prob, that any prover can convince V to accept.

We use a recursive procedure

evaluate (x, M):

$M = m_1 \# m_2 \# \dots m_i$ $\qquad n = |x|$

if $|M| > p(n)$ return 0;

If i is even then:

$\quad sum = N_{x, M\#ACC}$

$\quad$ for each m_{i+1} of length $\leq p(n) - |M|$

$\quad\quad sum += evaluate(x, M \# m_{i+1})$

$\quad$ return sum;

if i is odd then:

$\quad max = 0$

$\quad$ For each m_{i+1} of length $\leq p(n) - |M|$

$\quad\quad v = evaluate(x, M \# m_{i+1})$

$\quad\quad$ if $v > max$ then $max := v$;

$\quad$ return max.

end.

$\dfrac{evaluate(x, \varepsilon)}{2^{p(|x|)}}$ = the biggest probability any prover can convince verifier V to accept x.

evaluate(x, ε) runs in space $O(p(n)^2)$

$\Rightarrow A \in PSPACE$ ∎

Thm: #SAT has IP.

Pf: given (φ, k), φ a bool Fla & $k \in \mathbb{N}$
the Verifier wants to verify that φ has
k satisfying assignments, i.e.,

$$k = \sum_{x_1 \dots x_n \in \{0,1\}} \varphi(x_1, x_2, \dots x_n)$$

arithmetization: replace φ by a poly $p_\varphi(x_1 \dots x_n)$

$$x_i \to x_i$$
$$\neg\varphi \to 1 - p_\varphi$$
$$\varphi \wedge \psi \to p_\varphi \cdot p_\psi$$
$$\varphi \vee \psi \to 1 - (1 - p_\varphi)(1 - p_\psi)$$

$\Rightarrow$ verify $$k = \sum_{x_1, \dots x_n \in \{0,1\}} p_\varphi(x_1, \dots x_n) \qquad (*)$$

def: $$f_i(x_1, \dots x_i) = \sum_{x_{i+1} \dots x_n \in \{0,1\}^n} p_\varphi(x_1, x_2, \dots x_n)$$

protocol for $(*)$:

round 0: Prover sends $f_0()$
Verify checks that $f_0() = k$.

round $i > 0$: Prover sends a polynomial

$F_i(r_1, r_2, \ldots r_{i-1}, x_i) = p_i(x_i)$

... polynomial of degree $\leq |\varphi|$
so it suffices to send its coef's.

Verifier checks that

$F_{i-1}(r_1, \ldots r_{i-1}) = p_i(0) + p_i(1)$

& rejects if not
if $i < n$ then Verifier picks
random r_i & sends it to Prover
else $i = n$ then Verifier picks
a random r_n & checks $p_n(r_n)$
$= p_\varphi(r_1, \ldots r_n)$

end.

Here, all arithmetics is done in some field
$GF[p]$ for prime $p > 2^n$, from which
we pick the random elts.

(One could do the arithmetic in small field of size
$O(n \lg n)$ & use the Chinese remainder
theorem.)

If k is the # of sat. assignments to φ, the
Verifier can convince the Prover with prob 1.

If $k \neq \#\varphi$, the Prover must send $\widetilde{p}_1(x_1) \neq f_1(x_1)$

for random r_1, prob $\tilde{p}_1(r_1) = f_1(r_1)$

is $\frac{\deg \tilde{p}_1(x_1)}{|\mathbb{F}|} \leq \frac{1}{n^2}$

if $\tilde{p}_1(r_1) \neq f_1(r_1)$ then in round 2,

prover must send a polynomial $\tilde{p}_2(x_2) \neq f_2(r_1, x_2)$

again, for random r_2, prob. $\tilde{p}_2(r_2) = f_2(r_1, r_2)$

$\leq \frac{1}{n^2}$

if $\tilde{p}_2(r_2) = f_2(r_1, r_2)$ then in round 3

Prover must send $\tilde{p}_3(x_3) \neq f_3(r_1, r_2, x_3)$

$\vdots$

if $\tilde{p}_n(x_n) \neq f_n(r_1, r_2, \ldots r_{n-1}, x_n)$

the Verifier will reject in round n

w.p. $1 - \frac{1}{n^2}$.

$\Rightarrow$ the Verifier will accept only if at some round i, r_i is picked s.t.

$$\tilde{p}_i(r_i) = f_i(r_1, \ldots r_i)$$

so prover can send the true poly's $p_j(x_j)$ in rounds $j > i$.

This happens only with prob. $\leq (n-1) \cdot \frac{1}{n^2}$

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

$\blacksquare$

- PSPACE $\subseteq$ IP

We will design a protocol for QBF.

Let $\psi = Q x_1 Q x_2 \dots Q x_n \phi(x_1, \dots x_n)$

$\hookrightarrow$ CNF-fle

design $\psi' = Q x_1 R x_1 Q x_2 R x_1 R x_2 \dots Q x_n R x_1 R x_2 \dots R x_n \phi(x_1 \dots x_n)$

where R is a new "reduction" quantifier.

Denote: $\psi' = S_1 y_1 S_2 y_2 \dots \quad S_m y_m \phi(x_1 \dots x_n)$

$S_i \in \{\exists, \forall, R\} \quad y_i \in \{x_1 \dots x_n\}$.

$\forall i \leq m$ define f_i inductively: y_i

$S_i = \forall \qquad f_{i-1}(\dots) = f_i(\dots, 0) \cdot f_i(\dots, 1)$

$S_i = \exists \qquad f_{i-1}(\dots) = 1 - (1 - f_i(\dots, 0))(1 - f_i(\dots, 1))$

$S_i = R \qquad f_{i-1}(\dots, y) = (1-y) f_{i+1}(\dots, 0) + y f_{i+1}(\dots, 1)$ y_i

where $\underset{}{f_m} \overset{= P\phi}{}$ is the arithmetization of ϕ as in #SAT $\in$ IP.

Notice, each of the polynomials has degree $\leq 2|\psi|$ thanks to the R quantifiers. (After applying the R-quantifiers to each var, f_i has linear degree in each variable.)

(The protocol proceeds like in #SAT $\in$ IP);

round 0: Prover send $f_0() \overset{= P_0()}{}$ to the verifier.

If $f_0() \neq 1$ verifier rejects

round $i>0$: Prover sends coef's of $f_i(r_1, \dots, y_i) = p_i(y)$ to the Verifier.

Verifier checks:

case $S_i = \forall$: $f_{i-1}(r_1 \dots r_{i-1}) = p_i(0) \cdot p_i(1)$

case $S_i = \exists$: $f_{i-1}(r_1, \dots r_{i-1}) = 1 - (1-p_i(0))(1-p_i(1))$

case $S_i = R$: $f_{i-1}(r_1, \dots, r_{i-1}) = (1-r_{i-1}) p_i(0) + r_{i-1} p_i(1)$.

if either fails $\to$ REJECT

Verifier picks random r_i and proceed to round $i+1$.

round $m+1$: Verifier checks that $p_m(r_1 \dots r_m) = p_\varphi(r_1, \dots, r_m)$.

In this protocol, the arithmetics is done in a field of size $\geq |\varphi|^4$. In each round the probability that a bogus $\tilde{p}_i(y)$ would agree with the real Fcn $f_i(r_1, \dots, y)$ in point r_i is at most $\frac{2|\varphi|}{|\varphi|^4}$.

There are at most $|\varphi|^2$ rounds so the probability that a bogus $\tilde{p}_i(y)$ could replace the real at some point during the protocol $\leq \frac{|\varphi|^3}{|\varphi|^4} \leq \frac{1}{n}$

Cheating Prover is caught w.p. $1 - \frac{1}{n}$.

For true fle, the prover can convince w.prob. 1. $\boxed{}$