§ Интерактивные доказательства.

$x \in L$ $\quad \varphi \in T$

Классические д-ва $\quad$ текст

Prover $\quad$ Verifier

$(x, w) \longrightarrow$

P (prover) $\quad$ V (verifier)

x, r

$\longleftarrow s_1$

$\longrightarrow s_2$

$\longleftarrow$

$$V(x, r, h) \in \Sigma^* \cup \{0, 1\}$$

$s_1 \# s_2 \# s_3$

$$P(x, h) \in \Sigma^*$$

$V(x, r, "") = s_1$

$P(x, "s_1") = s_2$

$V(x, r, "s_1 \# s_2") = \ldots$

$\langle V, P \rangle (x)$ – р-т общения

__Опр.__ $k(n): \mathbb{N} \to \mathbb{N}$. Язык $L \in IP[k(n)]$, если $\exists$ полин. по времени от длины первого своего входа алгоритм $V(x, r, h)$ и функция P.

1) $\forall x \; \forall$ ф-ции P', в общении V и

P' произв. $\le k(|x|)$ посылок сообщ.

2) $\forall x \in L \quad \Pr[\langle V, P\rangle(x) = 1] \ge 2/3$

3) $\forall x \notin L\ \forall P^* \quad \Pr[\langle V, P^*\rangle(x) = 0] \ge 2/3$

$$IP = \bigcup_{c>0} IP[n^c]$$

Пример $GNI = \{(G_0, G_1) \mid G_0$ и G_1 неор. гр. на n вершинах, кот. не изоморфны$\}$

$V(G_0, G_1)$		P

$i \leftarrow \{0,1\}$

$\pi \leftarrow S_n$

$H = \pi(G_i)$

$\xrightarrow{H}$

$\xleftarrow{j \leftarrow \{0,1\}}$

$i = j \Rightarrow 1$

$i \ne j \Rightarrow 0$

$G_0 \cong G_1 \quad 1/2$

$G_0 \not\cong G_1 \quad 0$

$GNI \in IP[4]$

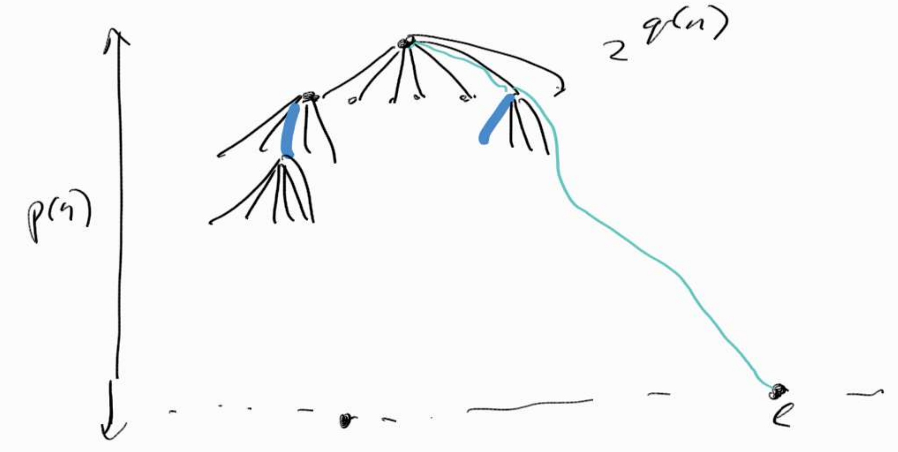
$GNI \in IP[2]$

Теорема (Шамир) $IP = PSPACE$

Д-во $IP \subseteq PSPACE$.

$L \in IP \quad V$ - verifier время раб. ор. $q(|x|)$

Число раундов $= p(n) \quad n = |x|$



Pe вер-ть того что в листе L

P_k = Pr[выдать ответ 1 | приняли в лист ℓ]

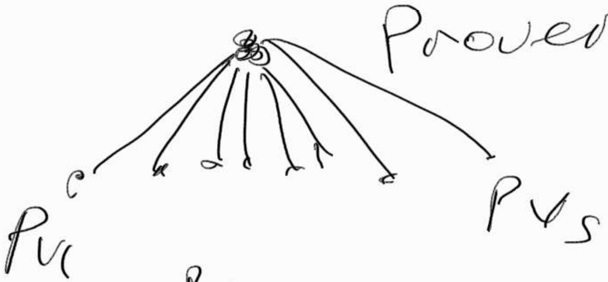
Для каждой верш. дерева v

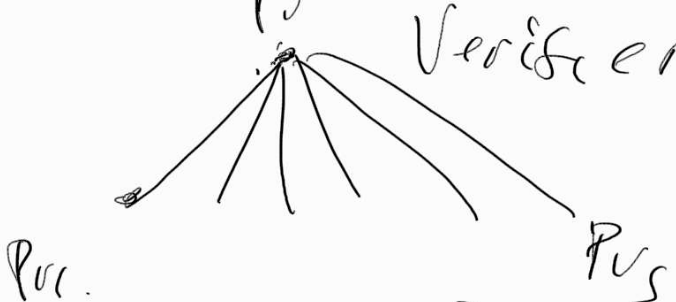
P_v = max Pr[протокол выдаст 1 | приняли в v]

↑ по ходам Prover

Proof ← нужно найти

Prover $P_v = \max\{P_{v_1}, \dots, P_{v_s}\}$





Verifier

$P_v = q_1 \cdot P_{v_1} + q_2 \cdot P_{v_2} + \dots + q_s P_{v_s}$

q_i = Pr[идём в v_i | уже пришли в v]

Pr[придём в верш $\wedge$ потом примем]

$PSPACE \subseteq IP$

$TQBF \in IP$

$Q_1 x_1 Q_2 x_2 \dots Q_n x_n \quad \varphi(x_1, \dots, x_n)$

Арифметизация

φ-ла $\longrightarrow$ многочлен над полем $|F| = \{0, 1, \dots, 3\}$

φ	$\tilde{\varphi}$
x	$\tilde{x}$
$\varphi \wedge \psi$	$\tilde{\varphi} \cdot \tilde{\psi}$
$\neg \varphi$	$1 - \tilde{\varphi}$
$\varphi \vee \psi$	$1 - (1 - \tilde{\varphi})(1 - \tilde{\psi})$
$\forall x_i \varphi$	$A_{x_i} \tilde{\varphi}$
$\exists x_i \varphi$	$E_{x_i} \tilde{\varphi}$

$A_{x_i} P = P(\dots, 0_i, \dots) \cdot P(\dots, 1_i, \dots)$

$E_{x_i} P = 1 - (1 - P(\dots, 0_i, \dots))(1 - P(\dots, 1_i, \dots))$

$Q_1 x_1 \dots Q_n x_n \varphi$ $\qquad$ $\tilde{Q}_1 x_1 \tilde{Q}_2 x_2 \dots \tilde{Q}_n x_n \tilde{\varphi}$

$A_{x_i} P(x_1, \dots, x_n) = (1 - x_i) P(x_1, \dots, 0_i, \dots, x_n) +$

$+ x_i P(x_1, \dots, 1_i, \dots, x_n)$

$Q_1 x_1 \ldots Q_n x_n \varphi$

$Q_1 x_1 \;|\; \tilde{Q} x_{n+1} \angle_{x_1} \ldots \angle_{x_{n-1}} \tilde{Q}_n x_n \tilde{\varphi}$

2   2m   m

cien
no
nonkg. nep ≤ 1

$A_1 A_2 . \;|\; A_{i+1} \ldots A_c \tilde{\varphi}$

$x_1 = r_1 \in \mathbb{F}$

$x_2 = r_2 \in \mathbb{F}$

$\vdots$

$x_i = r_i \in \mathbb{F}$

B

$\tilde{\varphi}$

$x_1 = r_1$

$\vdots$

$x_n = r_n$

B

$$O_{i+1}(x_{a(i)})\,O_{i+2} \quad - \quad O_e \quad \overline{ue}$$

$$\frac{}{h(x_{ai})} \qquad \deg h \le m$$

$$\begin{cases} x_1 = r_1 \\ \vdots \\ x_s = r_s \end{cases}$$

в

$$O_{i+1} = A\, x_{a(i)}$$

$$h(0) \cdot h(1) = b$$

$$O_{i+1} = E\, x_{ai}$$

$$1 - (1 - h(0))(1 - h(1)) = b$$

$$O_{i+1} = \alpha\, x_{ai}$$

$$(1 - r_{ai})\, h(0) + r_{ai}\, h(1) = b$$

$$x_{ai} \leftarrow \mathbb{F}$$

случайное значение

$$\parallel$$

$$r_{ai}$$

$$b = h(r_{ai})$$

O_1 — - - O_s

ложь

правда

ложь → правда

O_{i+1}

$h(X_{a_i})$

Мн-п $h(X_{a_i})$ — неверный

$h'(X_{e_i})$ — истинный

Pr[получить верное утв. на след. шаге] $= \Pr[h(\Gamma_{a_i}) = h'(\Gamma_{e_i})]$

$$\leq \frac{m}{|F|}$$

$$\Pr\left[\begin{array}{c}\text{где-то случился переход}\\ \text{ложь-правда}\end{array}\right] \leq$$

$$\leq n^2 \cdot \frac{m}{|F|} < \frac{1}{10}$$

$n = |\varphi| > m$

$$|F| > 10 m^4$$

Замеч.

1) В опр. класса IP можно считать, что если $x \in L$ $\Pr[\langle V, P\rangle(x) = 1] = 1$

2) В опр класса IP достаточно рассм. Prover ов, вычислимых с полином. памятью.

3) —||— V не скрывает случ. биты от P.