

Continue proof of $co - NP \subseteq IP$

- Define $g_2(x_2) = \sum_{x_3} \sum_{x_4} \cdots \sum_{x_n} \tilde{\phi}(y_1, x_2, \dots, x_n)$.
- $P \rightarrow V$: polynomial $h_2(x)$ of degree less than $3m$. Claim that $h_2 = g_2$.
- V : reject if $h_2(0) + h_2(1) \neq h_1(y_1)$.
- $V \rightarrow P$: $y_2 \in GF(q)$.

If $h_1 \neq g_1$, then

$$Prob(h_2(y_2) = g_2(y_2)) \leq \frac{3m}{q}$$

Repeat until end, we have

$$g_n(y_n) = \tilde{\phi}(y_1, \dots, y_n)$$

and V can verify if $h_n(y_n) = \tilde{\phi}(y_1, \dots, y_n)$ in polynomial time.

- If $\phi \in SAT$, P always sets $h_i = g_i$ and V always accepts.
- If $\phi \notin SAT$, let A_i be the event that $h_i = g_i$, we have

$$\begin{aligned} Prob(A_1) &\leq \frac{3m}{q} \\ Prob(A_2 | \neg A_1) &\leq \frac{3m}{q} \\ &\vdots \\ Prob(A_n) &\leq Prob(A_n | \neg A_{n-1}) + Prob(A_{n-1} | \neg A_{n-2}) + \cdots + Prob(A_1) \\ &\leq n \cdot \frac{3m}{q} \end{aligned}$$

Let $q > 9mn$, we have

$$Prob(A_n) \leq \frac{1}{3}$$

Thus, we have proved that $\overline{SAT} \subseteq IP$. Consequently, $co - NP \subseteq IP$.

TQBF $\in IP$: sketch of proof.

For any QBF:

$$\exists x_1 \forall x_2 \cdots \forall x_n \phi(x_1, \dots, x_n)$$

we can arithmetize it to:

$$V_0 = \prod_{x_1} \prod_{x_2} \cdots \prod_{x_{n-1}} \prod_{x_n} \tilde{\phi}(x_1, \dots, x_n)$$

where the coproduct operator \prod is defined as follows:

$$\prod_n F(n) = 1 - (1 - F(0))(1 - F(1))$$

Comparing to the proof of $\overline{SAT} \in IP$, here the dimension of V_0 is exponential of n . Since V is a polynomial time machine, it is not capable of checking an exponentially dimensioned polynomial. One easy solution to reduce the dimension of polynomial is the following. Define

$$R_i(p(x_1, \dots, x_n)) = p(x_1, \dots, x_n) \pmod{x_i^2 - x_i}$$

for any polynomial p . Notice that R_i reduces the dimension of x_i to 1 for any polynomials w.r.t. x_i , and has the property that

$$R(p(x_1, \dots, x_n)) = p(x_1, \dots, x_n) \quad \forall \{x_1 \cdots x_n\} \in \{0, 1\}^n$$

Now we redefine

$$V_0 = \prod_{x_1} R_1 \prod_{x_2} R_2 \cdots \prod_{x_{n-1}} R_{n-1} \prod_{x_n} \tilde{\phi}(x_1, \dots, x_n)$$

which now has polynomial dimension. Now we can define h_i and g_i in the same way as in the $\overline{SAT} \in IP$ proof and construct an IP machine that decides TQBF.