coNP $\subseteq$ IP. wanted to prove $\sum_{x_1=0}^{1} \cdots \sum_{x_n=0}^{1} p(x_1 \cdots x_n) = 0$. $p \equiv F$.

$a_i(x_1 \cdots x_i) = \sum_{x_{i+1}=0}^{1} \cdots \sum_{x_n=0}^{1} p(x_1 \cdots x_n)$. $a_0 = 0$.

$a_i(\text{—}) = a_{i+1}(\text{—}\,0) + a_{i+1}(\text{—}\,1)$. $\exists \{a_i\}_i$ st $a_0 = 0$, $a_n = p$.

$x_1 \cdots x_i$

$x_1 \cdots x_{i-1} \to r_1 \cdots r_{i-1}$ $\quad g_i = a_i(r_1 \cdots r_{i-1}, \underset{z}{x_i})$.

$v_0 = 0$ for $i = 1 \cdots n$:

- P sends poly g_i'
- V checks $\deg(g_i') \le m$.
- V checks $g_i'(0) + g_i'(1) = v_{i-1}$
- V samples & sends r_i
- $v_i = g_i'(r_i)$.

$\to$ check $v_n = p(r_1 \cdots r_n)$.

correct: $a_0 \ne 0$. $v_n = a_n(r_1 \cdots r_n)$.

$\exists i$ st: $v_{i-1} \ne a_{i-1}(r_1 \cdots r_{i-1})$

but $v_i = a_i(r_1 \cdots r_i)$.

r_i = root of $g_i - g_i'$.

$g(0) + g(1) = a_{i-1}(\cdots) \ne v_{i-1}$

$g'(0) + g'(1) = v_{i-1}$

$g \ne g' \Rightarrow g_i - g_i' \ne 0$ degree $\le m$.

$\Pr[r_i] \text{ root} \le \frac{m}{|\mathbb{F}|}$ //.

1. IP with RP verifier (never accepts $x \notin L$) equiv. NP.

IP/RP $\subseteq$ NP

x, assume $x \in L$. $\to$ $\exists$ transcript polynomial length y

$\exists$ random string r st V accepts with transcript y and randomness r

NTM: guess y, r, simulate V, if ok say $x \in L$.

if $x \notin L$: $\nexists r$ st V accepts $\Rightarrow$ will never say $x \in L$ if not true.

NP $\subseteq$ IP/RP

pick 3SAT. P sends α sat. assignment, V checks deterministically.

2. IP with coRP verifier (never rejects $x \in L$) equiv. IP.

IP $\subseteq$ IP/coRP. IP = PSPACE. take PSPACE-complete problem QBF. build protocol for IP/coRP.

$x = \exists x_1 \forall x_2 \exists x_3 \cdots F(x_1 \cdots x_n)$.

v_0 for $i = 1 \cdots n^2$

- P send g',
- V checks $\deg(g') \le m^2$
- V check $g'(0) + g'(1) = v_i$ /
- $r_i\, g'(1) + (1 - r_i)\, g'(0) = v_i$ /

check $v_n = p(r_1 \cdots r_n)$.

if x true: $g' = g$. always $\exists$.

V always accept.

if x false:

V reject w/pr $\ge 1/2$.

AM protocol st $|S| \ge K_1$ V always accept.
$|S| \le K_2$ V reject w-pr $\ge 1/2$. $\quad \frac{K_1}{K_2}$ may be large.

Hashing. $h : \{0,1\}^n \to \{0,1\}^k$ $\quad 2^k < K_1$.

$2^k > 2 \cdot K_2^2$.

$\underset{\{h\}}{\overset{\shortparallel}{\mathcal{H}}}$ pairwise independent family

Protocol: V samples h, sends to P.
P sends $x, x' \in S$ st $h(x) = h(x')$ + certificate that $x \in S$, $x' \in S$.

If $|S| \ge K_1$: always accept (h cannot be injective).

If $|S| \le K_2$: fix x, x'.

$$\Pr_h[h(x) = h(x')] \le \sum_{y \in \{0,1\}^k} \Pr[h(x) = h(x') = y] = 2^k \cdot 2^{-2k} = 2^{-k}.$$

union bound $\sum_{x \ne x' \in S} \Pr[\;] \le \binom{|S|}{2} \cdot 2^{-k} \le K_2^2 \cdot 2^{-k} \le 1/2$.

4. AM protocol st $|S| \ge K_1$ V always accept.
$|S| \le K_2$ V reject w-pr $\ge 1/2$. $\quad \frac{K_1}{K_2} = 2$.

hint: $|S_1| = K_1$ $\quad \frac{K_1}{K_2} = 2$. $\quad |S_1 \times S_1| = K_1^2$ $\quad \frac{K_1^2}{K_2^2} = 4$.

$|S_2| = K_2$ $\quad |S_2 \times S_2| = K_2^2$

S_1^ℓ, S_2^ℓ. $\quad \ell = \log K_2$. $\quad K_2^{\log K_2} = 2^{\log^2 K_2}$. $\quad \frac{K_1^\ell}{K_2^\ell} = K_2$.

$K_1^{\log K_2} = 2^{\log K_1 \cdot \log K_2}$

$K_1 = 2^{\log K_1}$

3 (alt.). multiple hashes. $\quad 2^k \simeq \frac{K_1}{2}$.

(i). ok if P chooses h, as long as before V chooses y.

say $\Pr_h[y \in h(S)] \ge 1/4$. $\left(\Pr_h[y \notin h(S)] \le \frac{3}{4}\right)$.

pick m hash functions $\Pr_{h_1 \cdots h_m}[y \in \bigcup h_i(S)] \le \left(\frac{3}{4}\right)^m$?.

$m > 10k$ $\quad \Pr < 2^{-k}$.

$\exists\, h_1 \cdots h_m$ st $\bigcup_i h_i(S) \supseteq \{0,1\}^k$.

P sends $h_1 \cdots h_m$.
V chooses $y \in \{0,1\}^k$
P i, x st $h_i(x) = y$, $x \in S$.

$\frac{K_1}{K_2} > 100k$. $\quad |S| < \frac{K_1}{100k} \Rightarrow \left|\bigcup_i h_i(S)\right| \le \frac{1}{2} \cdot \{0,1\}^k$.

5. #3SAT. how many assignments F has, F 3-CNF.

build IP protocol for #3SAT.

#3SAT $\in$ PSPACE $\exists$ protocol.

$$\sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \cdots \sum_{x_n=0}^{1} p(x_1 \cdots x_n)$$

$p(x_1 \cdots x_n) = \begin{cases} 0 & \text{if } x_1 \cdots x_n \text{ unsat} \\ \cancel{>0}\ \ 1 & \text{if } x_1 \cdots x_n \text{ sat. to } F. \end{cases}$

~~$\vee \to +$~~ $\quad 0 \cdot 0 = 0$ $\quad 0 + 0 = 0$

$\wedge \to \cdot$ $\quad 0 \cdot 1 = 0$ $\quad 0 + 1 = 1$

$\neg \to 1 -$. $\quad 1 \cdot 1 = 1$. $\quad 1 + 1 = 2$.