Man kann zeigen:

$$IP(k) = BP(NP)$$

für jedes konstante $k \geq 2$.

Da gilt: $coNP \subseteq BP(NP) \Rightarrow PH = \Sigma_2^p$

ist es unwahrscheinlich, dass coNP-vollständige Probleme interaktive Beweise mit konstant vielen Runden besitzen.

<u>Aber</u>:

<u>Theorem</u> (Shamir, 1990)

$IP = PSPACE$; insbesondere $coNP \subseteq IP$.

$IP \subseteq PSPACE$ ($\rightarrow$ Blatt 11); andere Inklusion $IP \supseteq PSPACE$ ist recht überraschend.

Wir zeigen „mehr"

<u>Satz</u> (Lund, Fortnow, Karloff, Nisan, 1990)

$coNP \subseteq IP$

Bew.:

Wissen: 3-COLORABILITY $\in$ NPC (→ S. 93).

Also: $\overline{\text{3-COLORABILITY}}$ ist coNP-vollständig, und es genügt z.z., dass $\overline{\text{3-COLORABILITY}} \in$ IP.

Sei $G=(V,E)$ ein Graph mit $V=\{1,\dots,n\}$.

Betrachte die Polynome

$$g(t) = \left(t-\tfrac{1}{4}\right)(t+1)(t-1)(t+2)(t-2)+1$$

und

$$f(x_1,\dots,x_n) = \prod_{\{i,j\}\in E} g(x_i - x_j).$$ f hat Grad $d = 5|E|$.

Sei $\gamma_1,\dots,\gamma_n \in \{0,1,2\}$ eine 3-Färbung der Knoten von V.

Falls $\gamma_1,\dots,\gamma_n$ eine gültige Färbung von G ist, dann ist

$$f(\gamma_1,\dots,\gamma_n) = 1$$

Falls $\gamma_1,\dots,\gamma_n$ keine gültige Färbung von G ist, dann ist

$$f(\gamma_1,\dots,\gamma_n) = 0.$$

Somit ist die Anzahl der gültigen 3-Färbungen von G gleich

$$h_0 = \sum_{x_1=0}^{2} \sum_{x_2=0}^{2} \cdots \sum_{x_n=0}^{2} f(x_1, \ldots, x_n).$$

Definiere allgemein

$$h_j(x_1, \ldots, x_j) = \sum_{x_{j+1}=0}^{2} \sum_{x_{j+2}=0}^{2} \cdots \sum_{x_n=0}^{2} f(x_1, \ldots, x_n).$$

Interaktives Beweissystem für $\overline{\text{3-COLORABILITY}}$.

Sei $H \subseteq \mathbb{N}$ mit $|H| = N$.

0. P behauptet, dass $h_0 = p_0 = 0$ ist
1. V fragt nach dem Polynom $h_1(x_1)$.
2. P gibt Polynom $p_1(x_1)$ (vom Grad $\leq d$) zurück
3. V überprüft, ob $p_1(0) + p_1(1) + p_2(2) = p_0$.

   Falls nein: V verwirft

   Falls ja: Wähle zufällig $S_1 \in H$.

   V fragt P nach Polynom $h_2(S_1, x_2)$.
4. P gibt Polynom $p_2(x_2)$ (Grad $\leq d$) zurück

5. V überprüft, ob $p_2(0) + p_2(1) + p_2(2) = p_1(\rho_1)$.

Falls nein: V verwirft.

Falls ja: wähle zufällig $\rho_2 \in H$

V fragt P nach Polynom $h_3(\rho_1, \rho_2, x_3)$

$\vdots$

$2n$: P gibt Polynom $p_n(x_n)$ zurück (und behauptet, dass $p_n(x_n) = h_n(\rho_1, \dots, \rho_{n-1}, x_n)$)

$2n+1$: V überprüft, ob

$$p_n(x_n) = h_n(\rho_1, \dots, \rho_n, x_n) = f(\rho_1, \dots, \rho_n, x_n).$$

Falls ja: V akzeptiert.

Falls nein: V verwirft.

<u>1. Fall</u>: $G \in \overline{3\text{-COLORABILITY}}$

Dann ist $p_0 = 0$. Wenn P im Protokoll immer mit $p_i(x_i) = h_i(\rho_1, \dots, \rho_{i-1}, x_i)$ antwortet, dann akzeptiert V mit W.keit 1.

<u>2. Fall</u>: $G \notin \overline{3\text{-COLORABILITY}}$

Dann ist $p_0 \neq 0$. Wenn aber P behauptet, dass $p_0 = 0$ ist, und wenn $p_1(0) + p_1(1) + p_2(2) = p_0$ ist, dann

ist das Polynom p_1 vom Polynom h_1 verschieden.
Also hat $p_1 - h_1$ höchstens d Nullstellen und die W.keit, dass ξ_1 eine NST ist, ist $\leq \frac{d}{N}$.

Dieses Argument kann man in jeder Runde wiederholen:
Falls die Beh. von P: $p_i(x_i) = h_i(\xi_1, \dots, \xi_{i-1}, x_i)$ falsch ist, und falls $p_i(0) + p_i(1) + p_i(2) = p_{i-1}(\xi_{i-1})$ ist, dann ist $p_i(\xi_i) = h_i(\xi_1, \dots, \xi_{i-1}, \xi_i)$ mit W.keit $\leq \frac{d}{N}$. Insgesamt ist also die W.keit, dass V akzeptiert obwohl $p_0 \neq 0$ ist, höchstens $n\frac{d}{N} \leq \frac{1}{3}$, wenn $N \geq 3nd$ gewählt wurde. $\boxtimes$

<u>Bem.</u>: Der Beweis zeigt eine viel stärkere Aussage: Er ermöglicht die Verifikation der <u>genauen Anzahl</u> von gültigen 3-Färbungen von G.
[$\rightsquigarrow$ #P-vollständige Probleme.]