Satz $BP(NP) \subseteq IP(2)$.

Bew.: Sei $L \in BP(NP)$. Interaktives Beweis-system für L: Sei $x \in \Sigma^*$

0. V wählt $r \in \{0,1\}^{p(|x|)}$ zufällig und schreibt r auf das Kommunikationsband.

1. P berechnet $y \in \Sigma^{p(|x|)}$ und schreibt y auf das Kommunikationsband.

2. V akzeptiert gdw. $(x, y, r) \in L'$.

Da $L' \in P$, ist V poly. zeit beschränkt. $\boxtimes$

Satz $\overline{GI} \in BP(NP)$.

Bew.: $x = (G_1, G_2)$, $G_i = (V_i, E_i)$

und $V_i = \{1, \dots, n\}$.

Definiere

$$N(G_1, G_2) = \{(H, \varphi) : (H \cong G_1 \text{ oder } H \cong G_2) \text{ und } \varphi \in Aut(H)\},$$

wobei $Aut(H) = \{\sigma \in S_n : \forall i,j \in [n] : \{i,j\} \in E_H \Leftrightarrow \{\sigma(i), \sigma(j)\} \in E_H\}$.

die <u>Automorphismengruppe</u> von H.

Es ist

$$N(G_1, G_2) = \{ (H, \varphi) : H \cong G_1 \text{ und } \varphi \in \mathrm{Aut}(H) \}$$
$$\cup \{ (H, \varphi) : H \cong G_2 \text{ und } \varphi \in \mathrm{Aut}(H) \}.$$

<u>Lemma 1</u> $|N(G_1, G_2)| = \begin{cases} n!, & \text{falls } G_1 \cong G_2 \\ 2n!, & \text{falls } G_1 \not\cong G_2. \end{cases}$

<u>Bew.</u>: später.

Definiere $Y = N(G_1, G_2) \times N(G_1, G_2) \times N(G_1, G_2) \times N(G_1, G_2)$
$\times N(G_1, G_2) = N(G_1, G_2)^5$.

Dann $|Y| = \begin{cases} (n!)^5, & \text{falls } G_1 \cong G_2 \\ 2^5 (n!)^5, & \text{falls } G_1 \not\cong G_2. \end{cases}$

Die Elemente von Y können als binäre Vektoren $\neq 0$ der Länge $p(n)$, p ein Polynom, aufgeschrieben werden.

<u>Lemma 2</u> Sei $R \in \{0,1\}^{k \times p}$ eine zufällige Matrix. Sei $X \subseteq \{0,1\}^p$, $X \neq \emptyset$, $0 \notin X$, eine Menge. Def. die Zufallsvariable

$$S = |\{x \in X : Rx \underset{(\mathrm{mod}\, 2)}{=} 0\}| = |X \cap \ker R|.$$

Dann gilt

(i) $\mathbb{E}[S] = \frac{|X|}{2^k}$.

(ii) $\mathrm{Var}[S] = \mathbb{E}[S^2] - \mathbb{E}[S]^2$

$$= \frac{\left(1-\frac{1}{2^k}\right)|X|}{2^k} \leq \mathbb{E}[S].$$

<u>Bew.:</u> (i) später, (ii) Blatt 12.

<u>Lemma 3</u>

(i) <u>Markov Ungleichung</u>

Sei $X \in \mathbb{R}_{\geq 0}$ Zufallsvariable, $t \geq 0$. Dann

$$\Pr[X \geq t] \leq \frac{\mathbb{E}[X]}{t}.$$

(ii) <u>Chebyshev Ungleichung</u>

Sei $X \in \mathbb{R}$ Zufallsvariable. Dann

$$\Pr[|X - \mathbb{E}[X]| > t] \leq \frac{\mathrm{Var}[X]}{t^2}.$$

<u>Bew.:</u> $\rightarrow$ VL Stochastik.

Wende nun Lemma 2 auf $X = Y$ an mit $k = \lceil \log 2^2 (n!)^5 \rceil$

Betrachte $S = |Y \cap \ker R|$.

<u>1. Fall $G_1 \cong G_2$:</u>

$$\mathbb{E}[S] = \frac{(n!)^5}{2^{\lceil \log(2^2 (n!)^5 \rceil}} \leq \frac{(n!)^5}{2^{\log(2^2 (n!)^5)}} = \frac{1}{4}.$$

Außerdem gilt nach der Markov Ungleichung

$$\Pr[S \geq 1] \leq \frac{1}{4}.$$

<u>2. Fall</u> $G_1 \not\cong G_2$:

$$\mathbb{E}[S] = \frac{2^5 (n!)^5}{2^{\lceil \log(2^2 (n!)^5) \rceil}} \geq \frac{2^5 (n!)^5}{2^{\log(2^2 (n!)^5) + 1}} = \frac{2^5}{2 \cdot 2^2} = 4.$$

Außerdem nach Chebyshev

$$\Pr[S = 0] \leq \Pr[|S - \mathbb{E}[S]| \geq \mathbb{E}[S]]$$

$$\leq \frac{\mathrm{Var}[S]}{\mathbb{E}[S]^2} \overset{L.2(ii)}{\leq} \frac{\mathbb{E}[S]}{\mathbb{E}[S]^2} \leq \frac{1}{4}.$$

Also $\Pr[S \geq 1] \geq \frac{3}{4}$.

Zusammen: Wir wollten ja eine Sprache $L' \in P$ finden und ein Polynom p finden mit

$$\forall x = (G_1, G_2) \in \Sigma^*$$

(i) $x = (G_1, G_2) \in \overline{GI} \Rightarrow \Pr_r [\exists y \in \Sigma^{p(|x|)} : (x, y, r) \in L'] \geq \frac{2}{3}$

(ii) $x \notin \overline{GI} \Rightarrow \Pr_r [\exists y \in \Sigma^{p(|x|)} : (x, y, r) \in L'] \leq \frac{1}{3}$

Dabei besteht $y = (y', y'')$, wobei $y' \in Y$ und y'' ist ein Zertifikat für die Tatsache $y' \in Y$ [dafür können wir explizite Isomorphismen von G_i nach H angeben.]

$r = R \in \{0,1\}^{p \times k}$ und $(x, y, r) \in L'$ gdw.

$y = (y', y'')$ und y'' zertifiziert, dass $y' \in Y$, und $Ry' \neq 0$. Dies kann alles in polynomieller Zeit berechnet werden. $\boxtimes$