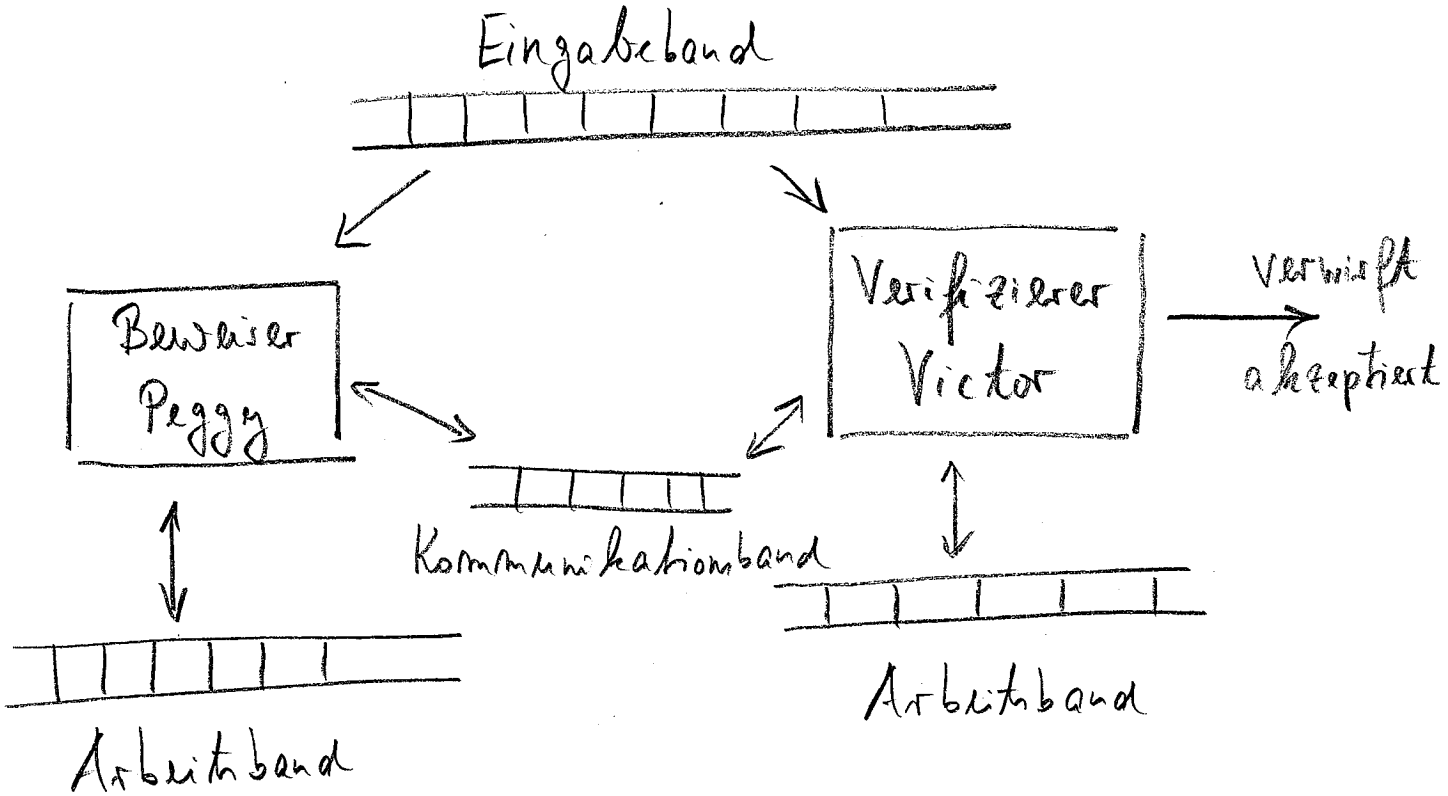
§ 3 Interaktive Beweise

Ziel:

- Modelliere „Beweisen" als interaktiven Prozess zwischen einem „Beweiser" und einem „Verifizierer"
- Interaktive Beweise können deutlich kürzer sein als konventionelle, falls Zufall verwendet wird.
- Interessante komplexitätstheoretische Konsequenzen: Falls $GI \in NPC \Rightarrow PH = \Sigma_2^p$
- Interessante kryptographische Konsequenzen: Beweiser kann Verifizierer überzeugen, einen Beweis zu besitzen, <u>ohne</u> ein Beweisdetail zu geben. („zero knowledge proofs").

Interaktive Beweise gehen auf Goldwasser, Micali, Rackhoff, 1989, zurück.

Interaktives Beweissystem:



- Peggy, Victor sind TM
- P./V. berechnen in Runden: In jeder Runde ist nur ein Spieler aktiv: Dieser liest vom Eingabe- und vom Kommunikationsband, berechnet etwas mit Hilfe des eigenen Arbeitsbandes und schreibt das Ergebnis zurück auf das Kommunikationsband. Danach ist der jeweils andere Spieler an der Reihe. Die gesamte Berechnung endet, sobald i. Victor verwirft bzw. akzeptiert.

Def.: Eine Sprache $L \subseteq \Sigma^*$ gehört zur Klasse IP, falls es ein interaktives Beweissystem mit einer poly.-zeit. beschr. prob. TM V gibt, so dass für alle Eingaben $x \in \Sigma^*$ gilt:

(i) $x \in L \Rightarrow \exists$ TM P:

$$\Pr[\text{V kommuniziert mit P und akzeptiert } x] \geq \frac{2}{3}$$

(ii) $x \notin L \Rightarrow \forall$ TM P:

$$\Pr[\text{V kommuniziert mit P und akzeptiert } x] \leq \frac{1}{3}.$$

[Hierbei kann P jede berechenbare Fkt. berechnen.]

Definiere $L \in IP(k) \Leftrightarrow L \in IP$, wobei die Anzahl der Runden $\leq k$ ist.

Lemma (a) $IP(0) = BPP$

(b) $NP \subseteq IP(1)$

(c) $IP \subseteq PSPACE$.

Bew.: (a) V ist auf sich alleine gestellt.

(b) $L \in NP \iff \exists$ TM M, poly. zeit. berch.,

$\exists\, p$ Polynom $\forall x \in \Sigma^*$:

$x \in L \iff \exists y \in \Sigma^{p(|x|)} : M(x,y) = 1$

<u>Interaktives Beweissystem (mit einer Runde)</u>

Sei $x \in \Sigma^*$ eine Eingabe

0. P schreibt Zertifikat $y \in \Sigma^{p(|x|)}$ auf das Kommunikationsband.

1. V simuliert die Berechnung von M mit Eingabe (x,y) und akzeptiert gdw. $M(x,y) = 1$.

(c) $\rightarrow$ Blatt 11. $\boxtimes$

<u>Zur Komplexität des Graphenisomorphismusproblem</u>

$GI = \{ \langle G_1, G_2 \rangle : G_1 = (V_1, E_1),\ G_2 = (V_2, E_2),$

$\exists\, \sigma : V_1 \to V_2$ Bijektion:

$\forall i,j \in V_1 : \{i,j\} \in E_1 \iff$

$\{\sigma(i), \sigma(j)\} \in E_2 \}$.

Allgemeiner Tenor: GI ist NP-unvollständig

Weil:
- $GI \in NP$
- Kein effizienter (polynomieller) Algo. für GI bekannt
- $\boxed{GI \in NPC \Rightarrow PH = \Sigma_2^P}$

Satz $\overline{GI} \in IP(2)$.

Bew: Interaktives Beweissystem (mit zwei Runden)

Eingabe $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ mit $V_1 = V_2 = \{1, \dots, n\}$.

0. V wählt zufällig Index $i \in \{1,2\}$ und Permutation $\pi \in S_n$.
   V berechnet Graph $H = \pi(G_i)$ und schreibt H auf das Kommunikationband
1. P berechnet $j \in \{1,2\}$ und schreibt j auf das Kommunikationband.
2. V akzeptiert genau dann, wenn $i = j$.

Klar: V ist poly. zeit. berch. prob. TM.

1. Fall: $(G_1, G_2) \in \overline{GI}$

D.h. G_1 und G_2 sind nicht zueinander isomorph.
Dann ist H entweder zu G_1 isomorph oder zu G_2.
Nun kann P alle Permutationen $\sigma \in S_n$ ausprobieren,
um zu entscheiden, ob $H \cong G_1$ oder $H \cong G_2$.
Er gibt den entsprechenden Index j zurück.
Also ist für $(G_1, G_2) \in \overline{GI}$:

$$\Pr[V \text{ akzeptiert } (G_1, G_2) \text{ nach Kommunikation mit } P] = 1 \geq \frac{2}{3}.$$

2. Fall: $(G_1, G_2) \notin \overline{GI}$

D.h. $G_1 \cong G_2$. Dann ist auch $G_1 \cong H \cong G_2$.
P kann also H nicht von G_1 und von G_2 unterscheiden. D.h. die W.keit, dass $i = j$ ist, ist höchstens $1/2$. Also ist für $(G_1, G_2) \notin \overline{GI}$:

$$\forall P: \Pr[V \text{ akzeptiert } (G_1, G_2) \text{ nach Kommunikation mit } P] \leq \frac{1}{2}.$$

Benötigen aber $Pr[\ldots] \leq \frac{1}{3}$.

Wir bekommen $Pr[\ldots] \leq \frac{1}{4}$, wenn wir in 0. $i_1, i_2 \in \{0,1\}$ und $\pi_1, \pi_2 \in S_n$ und $H_1 = \pi_1(G_{i_1})$, $H_2 = \pi_2(G_{i_2})$ zufällig wählen. $\boxtimes$

<u>Def.</u>: Sei $\mathcal{C}$ eine Komplexitätsklasse. Sei $L \subseteq \Sigma^*$ eine Sprache. Sie gehört zur Klasse $BP(\mathcal{C})$, falls es eine Sprache $L' \in \mathcal{C}$ gibt und ein Polynom p gibt, so dass für alle $x \in \Sigma^*$:

(i) $x \in L \Rightarrow Pr_r[(x,r) \in L'] \geq \frac{2}{3}$

(ii) $x \notin L \Rightarrow Pr_r[(x,r) \in L'] \leq \frac{1}{3}$,

wobei $r \in \{0,1\}^{p(|x|)}$ zufällig gewählt.

<u>Bsp.</u>: $L \in BP(NP) \Leftrightarrow \exists L' \in P$, p Polynom, so dass für alle $x \in \Sigma^*$ gilt:

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

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

wobei $r \in \{0,1\}^{p(|x|)}$ zufällig gewählt.