gilt immer $\Sigma_i^P \subsetneq \Pi_{i+1}^P \subsetneq \Sigma_{i+2}^P$, oder kann auch Gleichheit herrschen? Kann $\Sigma_i^P = \Sigma_{i+1}^P$ gelten?

<u>Satz</u> (Meyer, Stockmeyer, 1972)

a) Für jedes $i \geq 1$ gilt: Falls $\Sigma_i^P = \Pi_i^P$, dann ist $PH = \Sigma_i^P$.
("PH kollabiert auf das i-te Level")

b) Falls $P = NP$, dann ist $P = PH$
("PH kollabiert auf P")

<u>Bew</u>: b) per Induktion nach i: $\Sigma_i \subseteq P$, $\Pi_i \subseteq P$.

<u>$i=1$</u>: Klar nach Annahme, da $coP = P$.

<u>$i>1$</u>: Es reicht, $\Sigma_i^P \subseteq P$ zu zeigen.

Sei $L \in \Sigma_i^P$, also ex. ein Polynom p und eine pzb TM M mit

$x \in L \Leftrightarrow \exists u_1 \in \Sigma^{p(|x|)} \forall u_2 \in \Sigma^{p(|x|)} \ldots Q_i u_i \in \Sigma^{p(|x|)} : M(x, u_1, \ldots, u_i) = 1.$

Definiere nun $L' \subseteq \Sigma^*$ durch

$\langle x, u_1 \rangle \in L' \Leftrightarrow \forall u_2 \in \Sigma^{p(|x|)} \ldots Q_i u_i \in \Sigma^{p(|x|)} : M(x, u_1, \ldots, u_i) = 1.$

Dann ist $L' \in \Pi_{i-1}^P$ und nach I.V. $L' \in P$.

Also ex. eine pzb TM M' mit $\langle x, u_1 \rangle \in L' \Leftrightarrow M'(x, u_1) = 1$.

Aber damit gilt auch $x \in L \Leftrightarrow \exists u_1 \in \Sigma^{p(|x|)} : M'(x, u_1) = 1$, also ist $L \in NP$ und nach Annahme $L \in P$.

a) Ähnlich. $\square$

Allgemeine Vermutung: PH kollabiert nicht.

Auch die Idee von NP-vollständigen Sprachen lässt sich auf die polynomielle Hierarchie übertragen:

Definiere $\Sigma_i\text{-SAT} = \{\langle\varphi\rangle : \exists u_1 \forall u_2 \dots Q_i u_i : \varphi(u_1, \dots, u_i) = 1\}$

wobei u_j ein Vektor von Variablen ist.

<u>Satz</u>: a) Falls es eine PH-vollständige Sprache gibt, dann kollabiert PH auf level i, für ein $i \geq 1$.

b) $\Sigma_i\text{-SAT}$ ist Σ_i^P-vollständig für jedes $i \geq 1$.

<u>Beweis</u>: a) Sei $L \in PH$ eine PH-vollst. Sprache. Dann gibt es ein $i \geq 1$, so dass $L \in \Sigma_i^P$ ist. Sei nun $L' \in PH$ gegeben. Nach Annahme können wir L' in polynomieller Zeit auf L reduzieren, also ist $L' \in \Sigma_i^P$.

b) Aufgabe. $\square$

Aus dem Diagramm noch zu zeigen:

<u>Satz</u>: (Sipser-Gács-Lautemann, 1983)

$$BPP \subseteq \Sigma_2^P \cap \Pi_2^P.$$

Vorbereitung: Die W'keit 2/3 in der Definition von BPP kann stark abgeschwächt werden:

Lemma: Sei $c \geq 1$ und $L \subseteq \Sigma^*$. Falls es eine pzb PTM M gibt, so dass für jedes $x \in \Sigma^*$ gilt: $\Pr[M(x) = L(x)] \geq \frac{1}{2} + |x|^{-c}$,

dann ex. für jedes $d \geq 1$ eine pzb PTM M', so dass für jedes $x \in \Sigma^*$ gilt:

$$\Pr[M'(x) = L(x)] \geq 1 - 2^{-|x|^d}.$$

Bew: Wie auf Seite 106: Wiederhole Berechnung von M $k = 8|x|^{2c+d}$ mal und entscheide nach Mehrheit.

Definiere Zufallsvariable $X_i = \begin{cases} 1 & \text{falls } i\text{-te Berechnung } L(x) \text{ entspricht} \\ 0 & \text{sonst.} \end{cases}$

Dann ist $\mathbb{E}[X_i] = \Pr[X_i = 1] \geq \frac{1}{2} + |x|^{-c} =: p$ und für ausreichend kleines δ gilt

$$\Pr\left[\left|\sum_{i=1}^{k} X_i - p \cdot k\right| > \delta p k\right] < e^{-\delta^2/4\, pk}.$$

(Chernoff-Schranke)

Setze $\delta = |x|^{-c}$. Dann ist

$$p - \delta p = \left(\frac{1}{2} + \frac{1}{|x|^c}\right)\left(1 - \frac{1}{|x|^c}\right) = \frac{|x|^c + 2}{2|x|^c} \cdot \frac{|x|^c - 1}{|x|^c}$$

$$= \frac{1}{2}\left(1 + \frac{|x|^c - 2}{|x|^c}\right) \geq \frac{1}{2} \quad \text{für } |x| \geq 2,$$

also $pk - \delta pk \geq \frac{k}{2}$.

Falls also $\sum_{i=1}^{k} X_i \geq pk - \delta pk$ ist, dann ist die Ausgabe von M' korrekt.

Also ist die W'kait für eine falsche Ausgabe beschränkt durch $e^{-\frac{1}{4|x|^{2c}} \cdot \frac{1}{2} \cdot \delta |x|^{2c+d}} \leq 2^{-|x|^d}$. $\square$

<u>Bew:</u> (Sipser-Gács-Lautemann)

Da $BPP = coBPP$, reicht es, $BPP \subseteq \Sigma_2^P$ zu zeigen.

Sei $L \in BPP$, das heißt es ex. ein Polynom q und eine pzb TM M, so daß

$$x \in L \iff Pr[M(x,r) = 1] \geq 1 - 2^{-|x|},$$
$$x \notin L \iff Pr[M(x,r) = 1] \leq 2^{-|x|},$$

wobei $r \in \{0,1\}^{q(|x|)}$. Notation: $q(|x|) =: m$.

Für $x \in \Sigma^*$ setze $S_x = \{r \in \{0,1\}^m : M(x,r) = 1\}$.

$\Rightarrow$ Entweder $|S_x| \geq (1 - 2^{-|x|}) 2^m$ oder $|S_x| \leq 2^{-|x|} 2^m$.

Für $u, v \in \{0,1\}^m$ definiere $u + v = w \in \{0,1\}^m$ durch $w_i = u_i + v_i \bmod 2$; Setze entsprechend $S + u = \{x + u, x \in S\}$.

Sei $k := \lceil \frac{m}{|x|} \rceil + 1$.

<u>Beh 1</u>: Für $S \subseteq \{0,1\}^m$ und $u_1, \dots, u_k \in \{0,1\}^m$ gilt:
Falls $|S| \leq 2^{m-|x|}$, dann ist $\bigcup_{i=1}^{k} (S+u_i) \neq \{0,1\}^m$.

<u>Bew</u>: $\left|\bigcup_{i=1}^{k} (S+u_i)\right| \leq \sum_{i=1}^{k} |S+u_i| = k \cdot |S| < 2^m$ (für $|x|$ ausreichend groß.)

//

<u>Beh 2</u>: Für $S \subseteq \{0,1\}^m$ gilt: Falls $|S| \geq (1-2^{-|x|})2^m$, dann ex. $u_1, \dots, u_k \in \{0,1\}^m$ mit $\bigcup_{i=1}^{k} (S+u_i) = \{0,1\}^m$.

<u>Bew</u>: Zeigen: Wenn $u_1, \dots, u_k$ unabh. gleichverl. gewählt werden, dann ist $\Pr\left[\bigcup_{i=1}^{k} (S+u_i) = \{0,1\}^m\right] > 0$

$\longrightarrow$ Probabilistische Methode.

Für $r \in \{0,1\}^m$ sei B_r das Ereignis, dass $r \notin \bigcup_{i=1}^{k} (S+u_i)$. Dann ist $B_r = \bigcap_{i=1}^{k} B_r^i$, wobei B_r^i das Ereignis ist, dass $r \notin S+u_i \Leftrightarrow r+u_i \notin S$.
$r+u_i$ ist gleichverl. aus $\{0,1\}^m$ gewählt, also ist $\Pr[r+u_i \in S] \geq 1-2^{-|x|}$. Da $B_r^1, \dots, B_r^k$ unabh. sind, ist $\Pr[B_r] = \prod_{i=1}^{k} \Pr[B_r^i] = \Pr[B_r^i]^k \leq 2^{-|x|k} < 2^{-m}$.

$\Rightarrow \Pr[\exists r \in \{0,1\}^m : B_r] \leq \sum_{r \in \{0,1\}^m} \Pr[B_r] < 2^m \cdot 2^{-m} = 1$.

//

Also ist $x \in L$ genau dann, wenn gilt

$$\exists u_1, \dots, u_k \in \{0,1\}^m \ \forall r \in \{0,1\}^m : r \in \bigcup_{i=1}^{k} (S_x + u_i)$$

$$\Leftrightarrow \exists u_1, \dots, u_k \in \{0,1\}^m \ \forall r \in \{0,1\}^m : \bigvee_{i=1}^{k} M(x, r+u_i) = 1. \ \square$$