Prof. Martin Hofmann
Steffen Jost

Ludwig-Maximilians-Universität München
Institut für Informatik

Wintersemester 2002/03
12. Dezember 2002

Lösungsvorschläge zur 5. Übung

Komplexitätstheorie

Lösung zu G17:

a) "$\Longleftarrow$" Da y polynomial in der Länge beschränkt ist, können wir es "raten". Die Überprüfung, ob $\langle x, y\rangle \in A$ ist, können wir wegen $A \in \mathrm{P}$ ebenfalls in polynomial Zeit durchführen.

"$\Longrightarrow$" Sei $L = L(M)$. Falls $x \in M$, so gibt es eine akzeptierende Berechnung von M. Diesen Berechnungspfad codieren wir in y (hat nur polynomial beschränkte Länge). Die polynomial erkennbare Sprache A bedeutet dann:
$\langle x, y\rangle \in A$ genau dann, wenn y ist ein akzeptierender Berechnungspfad von M für Input x.

b) $L \in \mathrm{coNP}$, d.h. es gibt eine nicht deterministische Turing Maschine M mit $\bar{L} = L(M), \bar{L} \in \mathrm{NP}$. Nach a) gilt:

$$
\begin{aligned}
x \in \bar{L} &\Longleftrightarrow \exists y.\, |y| \le p(|x|) \wedge \langle x, y\rangle \in A\\
x \in \bar{L} &\Longleftrightarrow \neg\forall y.\, |y| \not\le p(|x|) \vee \langle x, y\rangle \notin A\\
x \in L &\Longleftrightarrow \forall y.\, |y| \not\le p(|x|) \vee \langle x, y\rangle \in \bar{A}
\end{aligned}
$$

wegen $x \in L \overset{\text{def}}{\Longleftrightarrow} x \notin \bar{L}$. Aus $A \in P \Longrightarrow \bar{A} \in P$ folgt dann die Behauptung.

c) "$\Longleftarrow$" Bauplan für eine nicht deterministische SAT-Orakel Turing Maschine:

- Rate $|y_1| \le p(|x|)$
- Frage SAT, ob $\exists y_2.\, |y| \le p(|x| \wedge \langle x, y_1, y_2\rangle \in A$, was nach a) in NP, somit auch auf SAT reduzierbar ist, da SAT NP vollständig ist.
- Wenn SAT bejaht, so lehne ab; ansonsten akzeptiere.

"$\Longrightarrow$" Es sei $L \in \mathrm{NP}^{\mathrm{SAT}}$ d.h. es gibt eine nicht-deterministische SAT-Orakelmaschine M mit $L = L(M)$.

- Alles was M rät, codieren wir in y_1.
- Alle SAT-Anfragen codieren wir in y_2.

Lösung zu G18: Aus $\Sigma_k^P \subseteq \Pi_k^P$ folgt auch $\mathrm{co}\Sigma_k^P \supseteq \mathrm{co}\Pi_k^P$, auch die Behauptung, denn $\mathrm{co}\Sigma_k^P = \Pi_k^P$ und $\mathrm{co}\Pi_k^P = \Sigma_k^P$ gilt nach Definition.

Bemerkung: Wer will, kann mit Theorem 7.3 und der Eigenschaft von P, unter Komplementen abgeschlossen zu sein, dies auch nochmal langsamer zeigen.

Lösung zu G19: Im Folgenden machen wir regen Gebrauch von Theorem 7.3; alle auftretenden Quantoren sind polynomial eingeschränkt.

a) Aus $\Sigma_k^P = \mathrm{PH}$ folgt mit $\Pi_k^P \subseteq \mathrm{PH}$ auch $\Pi_k^P \subseteq \Sigma_k^P$ und somit nach der vorherigen Aufgabe auch Gleichheit.

b) Es sei $L \in \Sigma_{k+2}^P$. Dann gibt es ein $L' \in \Pi_k^P + 1$ mit $L = \{x \mid \exists y.\langle x, y\rangle \in L\}$ Nach Voraussetzung gibt es dann aber auch $L \in \Sigma_{k+1}^P$ somit $L' = \{x \mid \exists y.\langle x, y\rangle \in L''\}$ für ein $L'' \in \Pi_k^P$. Wegen $L = \{x \mid \exists z.z = \langle y1, y2\rangle \wedge \langle x, y1, y2\rangle \in L''\}$ folgt dann auch $L \in \Sigma_{k+1}^P$.

c) Mit Induktion über i zeigen wir $\Sigma_k^P = \Sigma_k^P + i$, hieraus folgt, auch Definition $\Sigma_k^P = \mathrm{PH}$.
Der Induktionsanfang gilt nach Voraussetzung.
Indunktionsschritt:
Sei $L \in \Sigma_{k+i+1}$, dann gibt es ein $L' \in \Pi_k + i$ mit $L = x \mid \exists y.\langle x, y\rangle \in L'$.

Nach der Induktionalhypothese gibt $L \in \Sigma_k^P$, also $L' \in \Pi_k^P$. Damit aber $L \in \Sigma_k^P + 1$ und somit nach Voraussetzung auch $L \in \Sigma_k^P$.

Bemerkung: Für die Spezialfälle $k = 0, 1$ erhalten wir Aussagen im Sinne von G11.