Prof. Martin Hofmann
Steffen Jost

Ludwig-Maximilians-Universität München
Institut für Informatik

Wintersemester 2002/03
17. Dezember 2002

Lösungsvorschläge zur 7. Übung

Komplexitätstheorie

Lösung zu G26: Siehe Beweis zu Theorem 7.4 im Buch.

Lösung zu G27: Es bezeichne H das Halteproblem. Wir konsturieren eine Sprache L, mit $L \notin P$ aber $L \in P/poly$: Es sei $L := \{1^h \mid h \in H\}$. Falls $h \in H$ gilt, so muß der Schaltkreis lediglich überprüfen, ob die Eingabe ausschließlich aus 1 besteht (ein großes 'UND'). Andernfalls, also $h \notin H$, wird einfach immer verneint. Der Schlüssel liegt darin, dass wir für jedes h einen eigenen Schaltkreis konstruieren dürfen.

Lösung zu G28:

$\Longrightarrow$ $L \in P/poly$. Somit gibt es für jede Eingabegröße n einen passenden Schaltkreis C_n. Es sei $S := \{\langle 1^n, y\rangle \mid y$ ist Anfangsstück einer Binärcodierung von $C_n\}$. Durch polynomial viele Orakelfragen an S kann der Schaltkreis erraten werden (für jede Stelle der Codierung prüfen wir, ob sie 1 ist oder nicht), so dass wir danach den Schaltkreis einfach simulieren können.

$\Longleftarrow$ Dies ist etwas aufwendiger. Siehe z.B. U. Schöning: "Complexity and Structure", Springer 1986.

Lösung zu G29: Siehe Beweis des Satzes von Karp-Lipton im Vorlesungslogbuch (auf der Webseite der Vorlesung).