

Übungen zur Vorlesung Komplexitätstheorie

Blatt 4

Aufgabe P-8: Konstruieren Sie eine Menge $C \subseteq \{0, 1\}^*$ so dass

$$\text{NP}^C \neq \text{co-NP}^C$$

Hinweise:

- Die Menge C ist so zu konstruieren, dass $L_C := \{0^n \mid \exists x \in C \text{ mit } |x| = n\}$ nicht in co-NP^C ist.
- Gehen Sie davon aus, dass es eine Aufzählung

$$T_1, T_2, \dots, T_i, \dots$$

von Orakel-NTM gibt, so dass für jedes Orakel X gilt

- $\text{NP}^X = \{T_1^X, T_2^X, \dots, T_i^X, \dots\}$
- für jedes i und x ist $\text{TIME}_{T_i^X}(x) \leq |x|^i + i$.
- Konstruieren Sie $C = \bigcup_i C_i$ so, dass die Elemente in $C_i \setminus C_{i-1}$ dafür sorgen, dass L_C nicht das *Komplement* von $L(T_i^C)$ ist.

Aufgabe P-9: Eine *Einwegfunktion* ist eine Funktion $f : X \rightarrow Y$, so dass

- f ist in polynomieller Zeit berechenbar und
- es gibt keine pseudoinverse Funktion zu f , die in polynomieller Zeit berechenbar ist.

Eine Funktion $g : Y \rightarrow X$ ist *pseudoinvers* zu $f : X \rightarrow Y$, falls $f(g(y)) = y$ für alle y im Bild $f(X)$ von f .

Eine Einwegfunktion f heißt *ehrllich*, falls es ein Polynom p gibt, so dass es zu jedem $y \in f(X)$ ein x mit $f(x) = y$ und $|x| < p(|y|)$ gibt.

- Geben Sie eine (unehrliche) Einwegfunktion an.
- Für welche Anwendungen könnten ehrliche Einwegfunktionen nützlich sein? Welche zusätzlichen Eigenschaften wären dann nötig?

- (c) Zeigen Sie, dass ehrliche Einwegfunktionen existieren falls $P \neq NP$. (Es ist unbekannt, ob ehrliche Einwegfunktionen existieren.)

Aufgabe H-6: Die Klasse DP ist definiert als die Menge aller Sprachen L , derart dass es $L_1 \in NP$ und $L_2 \in co-NP$ gibt mit $L = L_1 \cap L_2$.

Eine KNF-Formel $C_1 \wedge \dots \wedge C_m$ wird in dieser Aufgabe als Menge $F = \{C_1, \dots, C_m\}$ aufgefasst.

- (a) Zeigen Sie $NP \subseteq DP$ und $co-NP \subseteq DP$.
- (b) Das Problem U-SAT ist es, zu entscheiden ob eine Klauselmenge, *genau eine* erfüllende Belegung besitzt. Zeigen Sie, dass U-SAT in DP ist. (Es ist offen ob U-SAT vollständig für DP ist.)
- (c) Finden Sie ein vollständiges Problem für die Klasse DP und zeigen Sie, dass es vollständig ist. (Hinweis: Vollständige Probleme für DP lassen sich kanonisch aus vollständigen Problemen für NP und co-NP konstruieren.)
- (d) Eine Menge von Klauseln F heißt *minimal unerfüllbar* falls F unerfüllbar ist und jede echte Teilmenge von F erfüllbar ist. Das Problem MIN-SAT ist es, zu entscheiden, ob eine gegebene Klauselmenge F minimal unerfüllbar ist. Zeigen Sie, dass MIN-SAT in der Klasse DP liegt. (Tatsächlich ist MIN-SAT vollständig für DP.)

Abgabe der Hausaufgaben: Legen Sie Ihre Lösungen bitte bis spätestens Mittwoch, 12.11.2008, 14 Uhr in den Übungskasten vor Raum F2 in der Oettingenstr. 67. Besprechung am Mittwoch, 12.11.2008.