

# Theoretische Informatik II

Prof. Dr. Christoph Kreitz / Holger Arnold

Universität Potsdam, Theoretische Informatik, Sommersemester 2006

Übung 10 (Version 3) — Abgabetermin: 3.7.2006, 11.00 Uhr

---

## Aufgabe 10.1

Zeigen Sie, dass die Menge  $P$  unter Vereinigung, Durchschnitt, Verkettung und Komplementbildung abgeschlossen ist. Zeigen Sie, dass  $NP$  unter Vereinigung, Durchschnitt, Verkettung und Hüllenbildung abgeschlossen ist. Begründen Sie, warum aus  $L \in NP$  nicht direkt  $\bar{L} \in NP$  folgt.

## Aufgabe 10.2

Zeigen Sie: Wenn es eine  $NP$ -vollständige Sprache gibt, deren Komplement in  $NP$  enthalten ist, dann ist das Komplement jeder Sprache aus  $NP$  ebenfalls in  $NP$  enthalten.

## Aufgabe 10.3

1. Die Funktion  $b : \mathbb{Z} \rightarrow \{0,1\}^*$  berechne die Binärcodierung einer ganzen Zahl. Für jede Primzahl gibt es einen Beweis der Primzahleigenschaft, dessen Länge polynomiell in der Länge der Binärdarstellung der Zahl ist [1]. Zeigen Sie, dass unter dieser Voraussetzung die Menge

$$\{(b(n), b(i), b(j)) \mid n, i, j \in \mathbb{Z}_{\geq 2}, i \leq j \leq n \text{ und } \{i, \dots, j\} \text{ enthält einen Primfaktor von } n\}$$

in  $NP$  enthalten ist (inzwischen ist bekannt, dass die Menge der Primzahlen in Binärdarstellung sogar in  $P$  liegt [2]).

2. Zeigen Sie: Wenn  $P = NP$  wäre, dann gäbe es einen Algorithmus, der alle Primfaktoren einer ganzen Zahl berechnet und der polynomiell in der Länge der Binärdarstellung der Zahl ist.

---

## Hausaufgabe 10.4

Zeigen Sie, dass die Menge  $P$  unter Hüllenbildung abgeschlossen ist, d.h. wenn  $L$  in  $P$  ist, dann ist auch  $L^* = \{w \mid \exists n \in \mathbb{N}. w = w_1 \dots w_n \wedge w_1, \dots, w_n \in L\}$  in  $P$  enthalten. Überlegen Sie sich dazu, wie das Enthaltensein eines Wortes  $w$  in  $L^*$  auf das Enthaltensein von Teilen von  $w$  in  $L^*$  zurückgeführt werden kann. Orientieren Sie sich an der Vorgehensweise des Cocke-Younger-Kasami-Algorithmus.

## Hausaufgabe 10.5

Zeigen Sie, dass in polynomieller Zeit entschieden werden kann, ob eine aussagenlogische Formel in konjunktiver Normalform allgemeingültig ist, d.h. von jeder Variablenbelegung erfüllt wird.

## Hausaufgabe 10.6

Sei  $SAT2$  die Menge aller aussagenlogischen Formeln in konjunktiver Normalform, die mindestens zwei verschiedene erfüllende Belegungen besitzen. Beweisen Sie, dass  $SAT2$  NP-vollständig ist, indem Sie zeigen, dass  $SAT2$  in NP liegt und dass sich  $SAT$  polynomiell auf  $SAT2$  reduzieren lässt.

---

## Literatur

- [1] V. R. Pratt. Every prime has a succinct certificate. *SIAM Journal on Computing*, 4(3):214–220, 1975.
- [2] Manindra Agrawal, Neeraj Kayal und Nitin Saxena. PRIMES is in P. *Annals of Mathematics*, 160:781–793, 2004.