

Übungsblatt 7

Aufgabe 1 (HORNSAT). Eine *Horn-Klausel* ist eine Klausel, die höchstens ein positives Literal besitzt. Eine *Horn-Formel* ist eine Konjunktion von Horn-Klauseln.

Zeigen Sie, dass das folgende Problem HORNSAT **P**-vollständig ist.

Gegeben: Eine Horn-Formel ϕ .

Gesucht: Ist ϕ erfüllbar?

Aufgabe 2. In [AB09, Kapitel 2] wird die Klasse NP wie folgt definiert:

Eine Sprache $L \subseteq \{0, 1\}^$ ist in NP, falls es ein Polynom $p : \mathbb{N} \rightarrow \mathbb{N}$ und eine deterministische, polynomiell zeitbeschränkte Turingmaschine M (auch Verifizier genannt) gibt, so dass für jedes $x \in \{0, 1\}^*$:*

$$x \in L \Leftrightarrow \exists u \in \{0, 1\}^{p(|x|)}, \quad \text{so dass } M(x, u) = 1$$

Falls $M(x, u) = 1$ für $x \in L$ und $u \in \{0, 1\}^{p(|x|)}$ gilt, dann heißt u ein Zertifikat für x (bezüglich der Sprache L und der Maschine M).

Definieren Sie, in dem Stil, die Klassen NL und coNP.

Aufgabe 3. Lesen Sie das Essay *Structure vs Combinatorics in Computational Complexity* [Bar14] von Boaz Barak.

1. Welche aus der Vorlesung bekannt Ergebnisse werden im Essay zitiert?
2. Geben Sie Barak's Beschreibungen von *Unstructured Problem* und *Structured/Algebraic Problem* wieder, und geben Sie Beispiele an.
3. Wie zeigt sich die genannte Unterteilung in kryptographischen Anwendungen?
4. Welcher Grund wird erwähnt, der verdeutlicht, dass eine Karp-Reduktion-ähnliche Konstruktion für den Average-Case schwierig ist?
5. Was besagt die *Random CSP Hypothesis*?

Literatur

- [AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.
- [Bar14] Boaz Barak. Structure vs combinatorics in computational complexity. *Bulletin of the EATCS*, 112, 2014.