

Blatt 9

Ausgabe: 03.07.2012
Abgabe: 10.07.2012

Hinweis: Dies ist das letzte Blatt und es handelt sich um eine Bonusrunde!

9.1. Aufgabe (6+4+8 Bonuspunkte)

P, NP und PCP

- a) Zeige, dass der Zugriff nur auf logarithmisch viele Bits eines Beweises oder aber nur auf logarithmisch viele Zufallsbits, keinen Zuwachs der Rechenleistung deterministischer Polynomialzeitalgorithmen mit sich bringt. Zeige also

$$P = \text{PCP}(0, 0) = \text{PCP}(0, O(\log n)) = \text{PCP}(O(\log n), 0).$$

- b) Zeige, dass es eine „universelle“ Konstante K gibt, so dass $\text{NP} \subseteq \text{PCP}(O(\log n), K)$ gilt, dass also *jede* Sprache in NP mit einem Verifier mit $O(\log n)$ Zufallsbits und K Beweisbits entschieden werden kann.
- c) Zeige $\text{PCP}(O(\log n), 2) \subseteq P$, d.h. $K > 2$ gilt, wenn $P \neq \text{NP}$.

Hinweis: Eine Sprache $L \in \text{PCP}(O(\log n), 2)$ werde von dem Verifier V erkannt, der mit zwei Beweisbits auskommt. Versuche für eine Eingabe w eine 2-KNF Formel K_w zu konstruieren, so dass K_w genau dann erfüllbar ist, wenn es einen Beweis gibt, der von V stets akzeptiert wird. Wir wissen, dass 2-SAT in polynomieller Zeit lösbar ist.

9.2. Aufgabe (6 Bonuspunkte)

Mächtigere Verifier!?

Für die Klasse PCP* wird der Verifier der Klasse PCP verstärkt: ein *adaptiver Verifier* darf die Anfrage des nächsten Beweisbits auch auf Basis der bisher gesehenen Beweisbits formulieren.

Zeige $\text{PCP}(O(r), O(1)) = \text{PCP}^*(O(r), O(1))$.