1 Beweissysteme

Definition 1.1.

Sei Σ ein endliches Alphabet und $L \subseteq \Sigma^*$ eine Sprache. Ein Relation $R \subseteq \Sigma^* \times \Sigma^*$ ist ein Beweissystem für L, falls:

- für alle $(w,x) \in R$ gilt $w \in L$ (Korrektheit)
- für jedes $w \in L$ existiert ein $x \in \Sigma^*$ mit $(w,x) \in R$ (Vollständigkeit)
- es gibt ein Algorithmus, der in Zeit $(|w|+|x|)^{O(1)}$ entscheidet, ob $(w,x) \in R$.

Definition 1.2

Ein Beweissystem R für L ist polynomiell beschränkt, falls es Konstanten n_0 und c gibt, sodass für alle $w \in L$ mit $|w| \geq n_0$ ein $x \in \Sigma^*$ mit $|x| \leq |w|^c$ und $(w,x) \in R$ existiert.

Theorem 1.3 (CR79)

Eine Sprache L besitzt genau dann ein polynomiell beschränktes Beweissystem, wenn $L \in NP$.

Beweis:

"$\Rightarrow$" Um zu testen, ob $w \in L$, "rate" x und teste $(w, x) \in R$ in polynomieller Zeit.

"$\Leftarrow$" Wenn $L \in NP$, dann ist

$R = \{ (w, \langle A(w) \rangle) \mid w \in L \}$ ein polynomiell beschränktes Beweissystem, wobei $\langle A(w) \rangle$ die Kodierung eines akzeptierenden Laufes einer nichtdeterministischen Turingmaschine A mit Eingabe w bezeichnet. □

Korollar 1.4

UNSAT := $\{ F \mid F$ ist eine unerfüllbare (aussagenlogische) Formel in KNF $\}$ hat ein polynomiell beschränktes Beweissystem genau dann wenn $NP = co\text{-}NP$.

p-Simulation

Definition 1.5 Seien R und S zwei Beweissysteme für eine Sprache L. Das System R *p-simuliert* das System S, falls es Konstanten n_0, c gibt, sodass es für jedes $(w,x) \in S$ mit $|x| \geq n_0$ ein $y \in \Sigma^*$ mit $(w,y) \in R$ gibt.

Lemma 1.6 Seien R und S zwei Beweissysteme für eine Sprache L. Wenn S polynomiell beschränkt ist und R das System S p-simuliert, dann ist auch R polynomiell beschränkt.

Beweis: Folgt direkt aus Definition 1.2 und 1.5.