Optimale aussagenlogische Beweissysteme und vollständige Sprachen

Jochen Meßner und Jacobo Torán

Abteilung Theoretische Informatik
Universität Ulm, 89069 Ulm

{messner,toran}@informatik.uni-ulm.de

Eine in polynomieller Zeit berechenbare Funktion $h : \Sigma^* \to \Sigma^*$, die als Bildbereich die aussagenlogischen Tautologien besitzt ($h(\Sigma^*) = \mathrm{TAUT}$) heißt (abstraktes) aussagenlogisches Beweissystem. Ein konkretes Beweissystem wie z.B. die Resolution läßt sich z.B. folgendermaßen darstellen:

$$h(w) = \begin{cases} \varphi & \text{falls } w = \langle \varphi, v \rangle \text{ und } v \text{ ist Resolutionsbeweis für } \varphi, \\ x \vee \overline{x} & \text{sonst.} \end{cases}$$

Um die Stärke verschiedener Beweissysteme vergleichen zu können, wurde von Cook und Reckhow (79) der Begriff der Simulation eingeführt: Ein Beweissystem h simuliert ein Beweissystem g, falls ein Polynom p so existiert, daß für jeden g-Beweis w ein h-Beweis w' mit $g(w) = h(w')$ und $|w'| \leq p(|w|)$ existiert; h p-simuliert g, falls die Abbildung $w \mapsto w'$ in polynomieller Zeit berechnet werden kann. Optimale (bzw. p-optimale) Beweissysteme sind Beweissysteme, die jedes Beweissystem simulieren (bzw. p-simulieren). Der Begriff der Optimalität von Beweissystemen ist in gewissem Sinne eng mit dem Begriff der vollständigen Sprache verwandt, es ist jedoch nicht bekannt ob optimale Beweissysteme existieren. Wir zeigen, daß die Existenz eines p-optimalen Beweissystems many-one vollständige Sprachen für UP bezüglich logspace-Reduktionen impliziert. Unter der schwächeren Voraussetzung optimaler Beweissysteme zeigen wir die Existenz nichtuniform-many-one-vollständiger Probleme für UP und many-one vollständiger Problem für NP $\cap$ SPARSE.