Theoretische Informatik 2

Sommersemester 2017

Georg Schnitger
Philipp Tertel
Hung The Tran

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 10

Ausgabe: 27.06.16
Abgabe: 04.07.16

Dieses Blatt ist ein Bonusblatt.

Aufgabe 10.1 *Die Länge von Beweisen* (2+4 Punkte)

a) Die Komplexitätsklasse **coNP** besteht aus allen Sprachen, deren Komplement zu **NP** gehört. Eine Sprache $L \in$ **coNP** heißt **coNP**-vollständig, wenn sich jede Sprache in **coNP** in polynomieller Zeit auf L reduzieren lässt.

   Zeigen Sie: Die Sprache $\mathcal{T}$ aller Tautologien ist **coNP**-vollständig.

b) Sei $\Sigma = \{0, 1\}$. Ein **Beweissystem** für eine Sprache L ist eine effizient berechenbare Funktion $B : \Sigma^* \to \Sigma^*$ mit $B(\Sigma^*) = L$. Für $w \in L$ und $B(b) = w$ heißt b ein **Beweis** von w.

   Zeigen Sie: **NP** = **coNP** $\iff$ es gibt ein Beweissystem für $\mathcal{T}$, sodass jede Tautologie $\tau \in \mathcal{T}$ einen Beweis polynomieller Länge besitzt.

   Kommentar: Da die Gleichheit **NP** = **coNP** nicht zu erwarten ist, besitzen Beweissysteme für $\mathcal{T}$ in aller Wahrscheinlichkeit stets Tautologien mit ausschließlich superpolynomiell langen Beweisen. Nicht nur ist die Konstruktion kurzer Beweise ein komplexes Problem, möglicherweise gibt es für eine gegebene Tautologie τ überhaupt keine kurzen Beweise!

Aufgabe 10.2 *Erweiterte Resolution* (1+2+(3+4+6)+2 Punkte)

Das Schubfachprinzip

$$S_n := \bigwedge_{i=1}^{n} D_i \wedge \bigwedge_{1 \leq i \neq j \leq n} \bigwedge_{k=1}^{n-1} D_{i,j,k}$$

für n Objekte und $n-1$ Fächer wird definiert durch

- die n Disjunktionsterme $D_i := \bigvee_{k=1}^{n-1} p_{i,k}^{(n)}$:

  Objekt i muss in irgendeines der $n-1$ Fächer gelegt werden

- und die $\mathcal{O}(n^3)$ Disjunktionsterme $D_{i,j,k} := \neg p_{i,k}^{(n)} \vee \neg p_{j,k}^{(n)}$

  verschiedene Objekte $i \neq j$ mit $1 \leq i, j \leq n$ dürfen nicht in dasselbe Fach k gelegt werden.

Es gibt leider nur Resolutionsbeweise der Länge $2^{\Omega(n)}$ für die Widersprüchlichkeit von S_n. In dem Beweissystem $\mathfrak{R}^*$ der erweiterten Resolution hingegen gelingen Widerspruchsbeweise polynomieller Länge. In $\mathfrak{R}^*$ dürfen zusätzlich aussagenlogische Formeln durch aussagenlogische Variablen abgekürzt werden; die Disjunktionsterme einer solchen Definition dürfen als Axiome benutzt werden.

Ein Beweis $\Phi \vdash_{\mathfrak{R}^*} \varphi$ beginnt mit einem Definitionsteil und wird mit der Angabe von Axiomen bzw. mit Anwendungen der Resolutionsregel weitergeführt. Insbesondere seien $x_1, \ldots, x_n$ die in den Formeln aus $\Phi \cup \{\varphi\}$ vorkommenden Variablen. Im Definitionsteil werden „neue" Variablen $y_1, \ldots, y_m$ als Abkürzungen mit der jeweiligen Setzung

$$y_i \leftrightarrow \psi_i$$

Die Formel $\big(y_i \leftrightarrow \psi_i\big)$ muss dann noch in eine äquivalente KNF

$$\big(D_{i_1} \wedge \cdots \wedge D_{i_{k_i}}\big)$$

umgewandelt werden; die Disjunktionsterme D_{i_j} dürfen dann anschließend als Axiome benutzt werden.

a) Wir zeigen, dass sich S_n außerhalb der Aussagenlogik problemlos auf das kleinere Schubfachprinzip S_{n-1} zurückführen lässt. Eine iterative Wiederholung führt dann auf das triviale Schubfachprinzip S_2. Wie sieht dieses Argument aus? Die injektive Funktion $f : \{1, \ldots, n\} \to \{1, \ldots, n-1\}$ sei gegeben. Definiere die Funktion $f^* : \{1, \ldots, n-1\} \to \{1, \ldots, n-2\}$ für $1 \leq i \leq n-1$ durch

$$f^*(i) := \begin{cases} f(i) & \text{falls } f(i) \neq n-1, \\ f(n) & \text{falls } f(i) = n-1. \end{cases}$$

Zeigen Sie: Wenn f injektiv ist, dann ist f^* injektiv.

b) Geben Sie einen Widerspruchsbeweis für S_2 mithilfe der konventionellen Resolution an. Natürlich sollte Ihr Beweis konstante Länge besitzen.

c) Zeigen Sie: $S_n \vdash_{\mathfrak{R}^*} S_{n-1}$. Das Argument aus a) kann also mit erweiterter Resolution innerhalb der Aussagenlogik ausgeführt werden.

   i) Definieren Sie die neuen Variablen $p_{i,k}^{(n-1)}$ (für $1 \leq i \leq n-1$ und $1 \leq k \leq n-2$) durch

   $$p_{i,k}^{(n-1)} \leftrightarrow \Big(p_{i,k}^{(n)} \vee (p_{i,n-1}^{(n)} \wedge p_{n,k}^{(n)})\Big).$$

   Beschreiben Sie die Disjunktionsterme in der Definition von $p_{i,k}^{(n-1)}$.

   ii) Beschreiben Sie eine Herleitung von $p_{i,1}^{(n-1)} \vee \cdots \vee p_{i,n-2}^{(n-1)}$ (für $1 \leq i \leq n-1$) aus S_n mit höchstens $\mathcal{O}(n)$ Resolutionsschritten. Benutzen Sie u. a. die Disjunktionsterme $D_i = p_{i,1}^{(n)} \vee \cdots \vee p_{i,n-1}^{(n)}$ und $D_n = p_{n,1}^{(n)} \vee \cdots \vee p_{n,n-1}^{(n)}$.

   iii) Beschreiben Sie eine Herleitung von $\neg p_{i,k}^{(n-1)} \vee \neg p_{j,k}^{(n-1)}$ für $i \neq j$ (und $1 \leq i, j \leq n-1$ sowie $1 \leq k \leq n-2$) aus S_n mit $\mathcal{O}(1)$ Resolutionsschritten.
   Hinweis: Leiten Sie $\neg p_{i,k}^{(n-1)} \vee \neg p_{n,k}^{(n)} \vee p_{i,n-1}^{(n)}$ und $\neg p_{j,k}^{(n-1)} \vee \neg p_{n,k}^{(n)} \vee p_{j,n-1}^{(n)}$ her.

d) Wie läuft Ihr Widerspruchsbeweis für S_n ab? Eine kurze Skizze, in der Sie Lösungen für die Teile b) und c) annehmen können, ist völlig ausreichend.