Institut für Informatik
der Universität München
Prof. M. Hofmann
Dr. A. Abel

WS 2007/2008

19. November 2007

Übungen zur Vorlesung
Rechnergestütztes Beweisen

Blatt 5

Aufgabe 15: (Skolemisierung und Resolution) [Papier, 3 Punkte] Führen Sie folgende Formeln unter Einführung geeigneter Skolemkonstanten in Pränex-Form über:

1. $(\exists y{:}\tau.\forall x{:}\tau'.R(x,y)) \Rightarrow (\forall x{:}\tau'.\exists y{:}\tau.R(x,y))$
2. $\neg((\exists y{:}\tau.\forall x{:}\tau'.R(x,y)) \Rightarrow (\forall x{:}\tau'.\exists y{:}\tau.R(x,y)))$

Eine dieser Formeln ist allgemeingültig. Zeigen Sie das durch Resolution.

Aufgabe 16: (Unifikation) [Papier, 2 Punkte] Eine *Substitution* σ ist eine endliche Abbildung von Variablen auf (evtl. offene) Terme, geschrieben als $\{t_1/x_1, \ldots, t_n/x_n\}$. Der *Definitionsbereich* der Substitution ist $\mathrm{dom}(\sigma) = \{x_1, \ldots, x_n\}$.

Die *Anwendung* $t\sigma$ einer Substitution σ auf einen Term t sei die gleichzeitige Ersetzung der Variablen $x_1, \ldots, x_n$ durch ihre Werte $t_1, \ldots, t_n$ in t. Eine Substitution σ' ist *allgemeiner* als σ, geschrieben $\sigma' \leq \sigma$, falls es eine Substitution σ_0 gibt, so dass für alle Terme t gilt $(t\sigma')\sigma_0 = t\sigma$. In diesem Fall heisst σ *spezieller* als σ'. (Zum Beispiel sind $\{f(g(z))/x\}$ und $\{f(z)/x, c/y\}$ echt spezieller als $\{f(z)/x\}$, wohingegen $\{f(y)/x\}$ und $\{f(y)/x, z/v\}$ zwar auch spezieller sind, aber nicht echt.)

Der *allgemeinste Unifikator* zweier Terme s und t ist die allgemeinste Substitution σ, so dass $s\sigma = t\sigma$.

Finden Sie, falls existent, den allgemeinsten Unifikator der Terme s und t. Dabei seien x, y, z, w, und v Variablen, alle anderen Buchstaben Funktionssymbole.

1. $s = h(a, x, f(g(y)))$ und $t = h(z, f(z), f(v))$.
2. $s = p(x, f(x))$ und $t = p(f(y), y)$.

Aufgabe 17: (Unifikations-Algorithmus) [Papier, 9 Punkte]

Ein *Unifikationsproblem* $U = (S \mid \sigma)$ ist eine Menge S von Termpaaren, geschrieben

$$\left\{\frac{s_1}{t_1}, \dots, \frac{s_m}{t_m}\right\},$$

zusammen mit einer Substitution σ. Dabei gelte die *Invariante* dass keine freie Variable (geschrieben $\mathsf{FV}(\dots)$) eines der Terme in S in $\mathsf{dom}(\sigma)$ sei. Eine Substitution σ' *löse* S, falls $s_i\sigma' = t_i\sigma'$ für $i = 1, \dots, m$. Eine *Lösung* von U ist eine Substitution $\sigma' \geq \sigma$ die S löst.

Ein Unifikationsproblem wird vereinfacht durch folgende *Reduktionen.*

$$\text{(triv)} \quad \left(\left\{\frac{x}{x}\right\} \uplus S \mid \sigma\right) \longrightarrow (S \mid \sigma)$$

$$\text{(var)} \quad \left(\left\{\frac{x}{t}\right\} \uplus S \mid \sigma\right) \longrightarrow \big(S(x := t) \mid \sigma(x := t)\big), \quad \text{wenn } x \notin \mathsf{FV}(t)$$

$$\text{(var')} \quad \left(\left\{\frac{t}{x}\right\} \uplus S \mid \sigma\right) \longrightarrow \big(S(x := t) \mid \sigma(x := t)\big), \quad \text{wenn } x \notin \mathsf{FV}(t)$$

$$\text{(fun)} \quad \left(\left\{\frac{f(s_1, \dots, s_n)}{f(t_1, \dots, t_n)}\right\} \uplus S \mid \sigma\right) \longrightarrow \left(\left\{\frac{s_1}{t_1}, \dots, \frac{s_n}{t_n}\right\} \uplus S \mid \sigma\right)$$

Dabei bedeutet $S(x := t)$ die Ersetzung von x durch t in allen Termen von S. Und für eine Substitution σ definieren wir (wobei wir $x \notin \mathsf{dom}(\sigma)$ voraussetzen)

$$\sigma(x := t) = \left\{\frac{t}{x}, \frac{t_1(x := t)}{x_1}, \dots, \frac{t_n(x := t)}{x_n}\right\} \quad \text{falls} \quad \sigma = \left\{\frac{t_1}{x_1}, \dots, \frac{t_n}{x_n}\right\}.$$

Eine zulässige Reduktionsfolge ist z. B. (wir sparen uns die Mengenklammern):

$$\left(\frac{h(x, f(g(z)))}{h(f(y), x)} \mid \emptyset\right) \longrightarrow \left(\frac{x}{f(y)}, \frac{f(g(z))}{x} \mid \emptyset\right) \longrightarrow \left(\frac{f(g(z))}{f(y)} \mid \frac{f(y)}{x}\right)$$
$$\longrightarrow \left(\frac{g(z)}{y} \mid \frac{f(y)}{x}\right) \longrightarrow \left(\emptyset \mid \frac{g(z)}{y}, \frac{f(g(z))}{x}\right)$$

(Achtung! Im Gegensatz zur in der Vorlesung vorgestellten Unifikation können oberer und unterer Term gemeinsame Variablen haben an.)

1. Testen Sie den durch das Reduktionssystem gegebenen Unifikationsalgorithmus and den Problemen der letzten Aufgabe. Im Klartext: Reduzieren sie das entsprechende Unifikationsproblem $(s/t \mid \emptyset)$, bis keine weiteren Reduktionen mehr möglich sind.

2. Beweisen Sie: Jede Reduktion erhält die Invariante, also gilt $S\sigma = S$ in jedem Zustand $U = (S \mid \sigma)$. (Dabei sei $S\sigma$ die punktweise Anwendung von σ auf alle Terme in S.)

3. Beweisen Sie: (Korrektheit) Wenn $U_1 \longrightarrow U_2$, dann ist jede Lösung von U_2 auch Lösung von U_1. (Hinweis: Benutzen Sie die Invariante!)

4. Beweisen Sie: (Vollständigkeit) Wenn $U_1 \longrightarrow U_2$, dann ist jede Lösung von U_1 auch Lösung von U_2.

5. Beweisen Sie: Wenn $(S \mid \emptyset) \longrightarrow^* (\emptyset \mid \sigma)$ so ist σ der allgemeinste Unifikator für das Problem S. (Hierin ist $\longrightarrow^*$ die reflexiv-transitive Hülle von $\longrightarrow$.)

Aufgabe 18: [SPASS, 6 Punkte] SPASS ist ein automatischer Beweiser für Prädikatenlogik mit Gleichheit (`equal`). Die Eingabedatei besteht aus der Sprache (`list_of_symbols`), einer Menge von Axiomen (`list_of_formulae(axioms)`) und einer Menge von Behauptungen (`list_of_formulae(conjectures)`), die von SPASS durch Resolution bewiesen werden sollen. Ein Beispiel finden Sie auf den Webseiten der Vorlesung.

Aufgabe: Formalisieren eine Gruppe durch die Axiome *Assoziativität* $(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$, *Links-Inverses* $(x \cdot x^{-}1 = e)$, und *Links-Eins* $(x \cdot e = x)$. Z.B. ist Letzteres in SPASS-Syntax:

```
formula(forall([x],equal(times(x,e),x))).
```

Lassen Sie SPASS die Aussagen *Rechts-Inverses* und *Rechts-Eins* beweisen.

Abgabe: bis **Dienstag, 15.11., 18.00 Uhr** im Sekretariat (**Z1.05**) oder bei Andreas Abel im Büro (**D1.09**). Abgabe am Montag, 26.11.2007 in der Übung. Elektronische Lösungsteile per Mail an `abel@informatik.uni-muenchen.de`.