Verfahren zur automatischen Verifikation

Prof. Dr. Christoph Walther • Markus Aderhold
FG Programmiermethodik • FB Informatik • TU Darmstadt
Sommersemester 2009

2. Übungsblatt

Übung am Dienstag, 05.05.2009

Hinweis Alle Verweise in den Aufgaben beziehen sich auf das Skriptum.

Aufgabe 2.1 (Noethersche Induktion)
Zur Lösung dieser Aufgabe dürfen Sie folgenden Hilfssatz verwenden:

> "Sei $(M, \rightarrow_M)$ eine fundierte Menge (engl. *well-founded set*), sei N eine Menge, sei $f : N \rightarrow M$ eine totale Abbildung, und sei $\rightarrow_N \subset N \times N$ mit $f(n_1) \rightarrow_M f(n_2)$ falls $n_1 \rightarrow_N n_2$. Dann ist $(N, \rightarrow_N)$ eine fundierte Menge."

Mit diesem Satz gilt insbesondere, daß $(N, \rightarrow_N)$ fundiert ist, falls $f : N \rightarrow \mathbb{N}$ und $f(n_1) > f(n_2)$ für alle $n_1 \rightarrow_N n_2$.

(i) Gegeben seien folgende Formeln, wobei $\varphi(x)$ eine Formel mit einer einzigen *freien* Variablen x über $\mathbb{N}$ ist:

(i) $\varphi(0)$
(ii) $\varphi(1)$
(iii) $\forall n \in \mathbb{N}.\ n \neq 0 \wedge n \neq 1 \wedge \varphi(n-2) \curvearrowright \varphi(n)$
(iv) $\forall n \in \mathbb{N}.\ \varphi(n)$

Zeigen Sie mit Hilfe von Satz 4.2, daß mit diesen Formeln ein Induktionsaxiom gegeben ist, d.h. es gilt: Wenn (i), (ii) und (iii) wahr sind, so ist auch (iv) wahr.

(ii) Gegeben seien folgende Formeln, wobei $\varphi(x, y)$ eine Formel mit den einzigen *freien* Variablen x und y über $\mathbb{N}$ ist:

(i) $\forall n, m \in \mathbb{N}.\ n = 0 \vee m = 0 \curvearrowright \varphi(n, m)$
(ii) $\forall n, m \in \mathbb{N}.\ n \neq 0 \wedge m \neq 0 \wedge \forall m^* \in \mathbb{N}.\ \varphi(n \dot{-} m, m^*) \curvearrowright \varphi(n, m)$
(iii) $\forall n, m \in \mathbb{N}.\ \varphi(n, m)$

Zeigen Sie mit Hilfe von Satz 4.2, daß mit diesen Formeln ein Induktionsaxiom gegeben ist, d.h. es gilt: Wenn (i) und (ii) wahr sind, so ist auch (iii) wahr.

(iii) Gegeben seien folgende Formeln, wobei $\varphi(x)$ eine Formel mit einer einzigen *freien* Variablen x über $\mathcal{T}(\Sigma^c)_{\texttt{list}}$ ist:

(i) $\varphi(\mathit{empty})$
(ii) $\forall l \in \mathcal{T}(\Sigma^c)_{\texttt{list}}.\ l \neq \mathit{empty} \wedge \varphi(\mathit{tl}(l)) \curvearrowright \varphi(l)$
(iii) $\forall l \in \mathcal{T}(\Sigma^c)_{\texttt{list}}.\ \varphi(l)$

Zeigen Sie mit Hilfe von Satz 4.2, daß mit diesen Formeln ein Induktionsaxiom gegeben ist, d.h. es gilt: Wenn (i) und (ii) wahr sind, so ist auch (iii) wahr.

Aufgabe 2.2 (Relationenbeschreibungen)

(i) Geben Sie die fundierte Relation, die implizit mit dem Induktionsaxiom aus Aufgabe 2.1(i) definiert wird, als Relationenbeschreibung R an, und bestimmen Sie sowohl $\mathcal{V}(R)$ als auch $\mathcal{IV}(R)$.

(ii) Geben Sie die fundierte Relation, die implizit mit dem Induktionsaxiom aus Aufgabe 2.1(ii) definiert wird, als Relationenbeschreibung R an, und bestimmen Sie sowohl $\mathcal{V}(R)$ als auch $\mathcal{IV}(R)$.

(iii) Geben Sie die fundierte Relation, die implizit mit dem Induktionsaxiom aus Aufgabe 2.1(iii) definiert wird, als Relationenbeschreibung R an, und bestimmen Sie sowohl $\mathcal{V}(R)$ als auch $\mathcal{IV}(R)$.

Aufgabe 2.3 (Relationenbeschreibungen und Induktionsformeln)

Gegeben sei der boolesche Term $goal[x, y, z] \in \mathcal{T}(\Sigma(P), \{x, y, z\})_{\mathtt{bool}}$ mit $x, y, z \in \mathcal{V}_{\mathtt{nat}}$ sowie die Relationenbeschreibung

$$R = \{\langle\{x \neq 0, y = 0\}, \{\{x/x - 1\}\}\rangle, \langle\{x \neq 0, y \neq 0\}, \{\{x/x - 1\}, \{x/x, y/y - 1\}\}\rangle\} \ .$$

(i) Beweisen oder widerlegen Sie, daß R fundiert ist. (Hinweis: Der Hilfssatz aus Aufgabe 2.1 ist hier nicht verwendbar.)

(ii) Bestimmen Sie $\mathcal{IND}(R, goal[x, y, z])$ gemäß Definition 4.13.

Aufgabe 2.4 (Relationenbeschreibungen und Induktionsformeln)

Gegeben sei der boolesche Term $goal[x] \in \mathcal{T}(\Sigma(P), \{x\})_{\mathtt{bool}}$ mit $x \in \mathcal{V}_{\mathtt{nat}}$ sowie die Relationenbeschreibung

$$R = \{\langle\{x \neq x\}, \{\{x/x\}\}\rangle\} \ .$$

(i) Bestimmen Sie $\mathcal{IND}(R, goal[x])$ gemäß Definition 4.13.

(ii) Untersuchen Sie, ob mit $\vDash_P \mathcal{IND}(R, goal[x])$ auch $\vDash_P \forall x{:}nat.\ goal[x]$ gilt, und begründen Sie ihre Antwort.

Aufgabe 2.5 (Relationenbeschreibungen von Datenstrukturen)

(i) Gegeben sei die Datenstruktur

```
structure IF.Expr <= F, T,
                     prop(number:nat),
                     IF(test:IF.Expr,left:IF.Expr,right:IF.Expr) .
```

Bestimmen Sie die Relationenbeschreibung $B_{\mathtt{IF.Expr}}$ gemäß Definition 4.15.

(ii) Gegeben sei die Datenstruktur

```
structure term <= var(vsym:variable.symbol),
                  const(csym:constant.symbol),
                  apply(fsym:function.symbol,argument:term),
                  pack(left:term,right:term) .
```

Bestimmen Sie die Relationenbeschreibung $B_{\mathtt{term}}$ gemäß Definition 4.15.