Verfahren zur automatischen Verifikation

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

2. Hausaufgabe

Abgabe am Donnerstag, den 19.05.2009, in der Übung

Hinweis: Alle Verweise in den Aufgaben beziehen sich auf das Skriptum.
Für diese Hausaufgabe gibt es **20 Punkte**.

Hausaufgabe 2.1 (Noethersche Induktion) **2+2+2=6 Punkte**

(i) Beweisen Sie den Hilfssatz aus Übungsaufgabe 2.1 (und verwenden Sie diesen in den nachfolgenden Teilaufgaben):

> "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."

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

$$\begin{array}{ll} \text{(i)} & \forall n, m \in \mathbb{N}.\ n \leq m \curvearrowright \varphi(n, m) \\ \text{(ii)} & \forall n, m \in \mathbb{N}.\ n > m \wedge \varphi(n, m+1) \curvearrowright \varphi(n, m) \\ \text{(iii)} & \forall n, m \in \mathbb{N}.\ \varphi(n, m) \end{array}$$

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 $\mathcal{T}(\Sigma^c)_{\texttt{sexpr}}$ ist:

$$\begin{array}{ll} \text{(i)} & \varphi(nil) \\ \text{(ii)} & \forall s \in \mathcal{T}(\Sigma^c)_{\texttt{sexpr}}.\ \varphi(atom(index(s))) \\ \text{(iii)} & \forall s \in \mathcal{T}(\Sigma^c)_{\texttt{sexpr}}.\ s \neq nil \wedge s \neq atom(index(s)) \wedge \varphi(car(s)) \wedge \varphi(cdr(s)) \curvearrowright \varphi(s) \\ \text{(iv)} & \forall s \in \mathcal{T}(\Sigma^c)_{\texttt{sexpr}}.\ \varphi(s) \end{array}$$

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.

Hausaufgabe 2.2 (Relationenbeschreibungen) **2+2=4 Punkte**

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

Hausaufgabe 2.3 (Fundierte Mengen) **4 Punkte**
Beweisen oder widerlegen Sie folgende Behauptung:

> "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 $f(n_{\mathbf{2}}) \rightarrow_M f(n_{\mathbf{1}})$ falls $n_1 \rightarrow_N n_2$. Dann ist $(N, \rightarrow_N)$ *keine* fundierte Menge."

(Hinweis: Die Lösung dieser Aufgabe fällt Ihnen leichter, wenn Sie zuvor die Hausaufgaben 2.1 und 2.2 gelöst haben.)

Hausaufgabe 2.4 (Relationenbeschreibungen und Induktionsformeln) **2+2=4 Punkte**
Gegeben sei die Relationbeschreibung

$$R = \{\langle\{j > i\}, \{\{j/(i + \lfloor (j-i)/2 \rfloor) - 1, i/i\}, \{j/j, i/(i + \lfloor (j-i)/2 \rfloor) + 1\}\}\rangle\} \ .$$

mit $i, j \in \mathcal{V}_{\mathtt{nat}}$.[1]
(i) Beweisen Sie unter Verwendung des Hilfsatzes aus Übungsaufgabe 2.1, dass R fundiert ist.
(ii) Bestimmen Sie $\mathcal{IND}(R, goal[h, i, j])$ so, wie in Definition 4.13 angegeben, für den booleschen Term $goal[h, i, j] \in \mathcal{T}(\Sigma(P), \{h, i, j\})_{\mathtt{bool}}$ mit $h, i, j \in \mathcal{V}_{\mathtt{nat}}$.

Hausaufgabe 2.5 (Relationenbeschreibungen von Datenstrukturen) **2 Punkte**
(i) Gegeben sei die Datenstruktur

```
structure EXPR <=
 EXPR0(e-op0:nullary.operator),
 EXPR1(e-op1:unary.operator,arg:EXPR),
 EXPR2(e-op2:binary.operator,arg1:EXPR,arg2:EXPR),
 VAR@(index:nat) .
```

Bestimmen Sie die Relationenbeschreibung $B_{\mathtt{EXPR}}$ gemäß Definition 4.15.
(ii) Gegeben sei die Datenstruktur

```
structure WHILE.PROGRAM <=
 SKIP,
 COMPOUND(LEFT:WHILE.PROGRAM,RIGHT:WHILE.PROGRAM),
 SET(CELL:VARIABLE,TERM:EXPR),
 WHILE(WCOND:EXPR,BODY:WHILE.PROGRAM),
 IF(ICOND:EXPR,THEN:WHILE.PROGRAM,ELSE:WHILE.PROGRAM) .
```

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

[1] $\lfloor n/2 \rfloor$ ist die nach unten gerundete Division durch 2, also $\lfloor 2/2 \rfloor = 1$, $\lfloor 3/2 \rfloor = 1$, $\lfloor 4/2 \rfloor = 2$ usw.