Formale Grundlagen der Informatik 3

Prof. Dr. Christoph Walther / Visar Januzaj, Nathan Wasser
Technische Universität Darmstadt — Wintersemester 2011/12

Lösungsvorschlag zu Hausübung 4 - Teil 2

Aufgabe 4.3 (Induktion) (20 Punkte)

Betrachten Sie das folgende $\mathcal{L}$-Programm P ($\mathbb{N}$ und `bool` sind wie im ✓eriFun-System definiert):

```
structure list[@I] <=
  ø, [infixr] ::(hd : @I, tl : list[@I])

function append(k, l : list[@I]) : list[@I] <=
if ?ø(k)
  then l
  else hd(k) :: append(tl(k), l)
end_if

function isPrefix(x, y : list[@I]) : bool <=
if ?ø(x)
  then true
  else if ?ø(y)
          then false
          else if hd(x) = hd(y)
                 then isPrefix(tl(x), tl(y))
                 else false
               end_if
       end_if
end_if

lemma h4.3 <= ∀ k, l : list[@I]
  isPrefix(k, append(k, l))
```

(a) Geben Sie die Axiome $AX_{\texttt{append}}, AX_{\texttt{isPrefix}}$ und $AX_{\texttt{h4.3}}$ an.

Lösungsvorschlag

$$AX_{\texttt{append}} = \forall k, l : \texttt{list[@I]}\ \texttt{append}(k, l) \equiv \texttt{if}\{?\texttt{ø}(k), l, \texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)\}$$

$$AX_{\texttt{isPrefix}} = \forall x, y : \texttt{list[@I]}\ \texttt{isPrefix}(x, y) \equiv \texttt{if}\{?\texttt{ø}(x), \texttt{true}, \texttt{if}\{?\texttt{ø}(y), \texttt{false}, \texttt{if}\{\texttt{hd}(x)\texttt{=}\texttt{hd}(y), \texttt{isPrefix}(\texttt{tl}(x), \texttt{tl}(y)), \texttt{false}\}\}\}$$

$$AX_{\texttt{h4.3}} = \forall k, l : \texttt{list[@I]}\ \texttt{isPrefix}(k, \texttt{append}(k, l)) \equiv \texttt{true}$$

(b) Bilden Sie die Induktionsformeln in Form von HPL-Sequenzen für den Rumpf b des Lemmas `h4.3` und die Relation $\{\langle\{?\texttt{ø}(k)\}, \emptyset\rangle, \langle\{?::(k)\}, \{\{k/\texttt{tl}(k)\}\}\rangle\}$.

Lösungsvorschlag

$$seq_{\mathcal{I}_1} = \langle \{?\emptyset(k)\}, \emptyset \Vdash \texttt{isPrefix}(k, \texttt{append}(k, l)) \rangle$$
$$seq_{\mathcal{I}_2} = \langle \{?::(k)\}, \{\forall l : \texttt{list[@I]}\ \texttt{isPrefix}(\texttt{tl}(k), \texttt{append}(\texttt{tl}(k), l))\} \Vdash \texttt{isPrefix}(k, \texttt{append}(k, l)) \rangle$$

(c) Beweisen Sie die Induktionsformeln $\mathcal{I}_i$, zeigen Sie also für jede Sequenz $seq_{\mathcal{I}_i} = \langle H_i, IH_i \Vdash b \rangle$:

$$AX_P \cup \mathcal{E}_P \models$$
$$\forall\, k, l : \texttt{list[@I]} \left(\bigwedge_{h \in H_i} h \equiv \texttt{true} \wedge \bigwedge_{(\forall\, l : \texttt{list[@I]}\ ih) \in IH_i} \forall\, l : \texttt{list[@I]}\ ih \equiv \texttt{true} \right) \rightarrow b \equiv \texttt{true}$$

Geben Sie in jedem Schritt die verwendete Gleichung an. Für Axiome der Datentypen verwenden Sie die Bezeichnungen (1)(a) bis (5)(a) wie auf Folie 3, Kapitel 9, angegeben.

Lösungsvorschlag

Um die Implikationen zu zeigen, nehmen wir die Prämissen an.

- $?\emptyset(k) \equiv \texttt{true} \rightarrow \texttt{isPrefix}(k, \texttt{append}(k, l)) \equiv \texttt{true}$

$$\begin{aligned} \texttt{isPrefix}(k, \texttt{append}(k, l)) &\underset{AX_{\texttt{isPrefix}}}{\equiv} \texttt{if}\{?\emptyset(k), \texttt{true}, \ldots\} \\ &\underset{H_1}{\equiv} \texttt{if}\{\texttt{true}, \texttt{true}, \ldots\} \\ &\underset{(4)(a)}{\equiv} \texttt{true} \end{aligned}$$

- $?::(k) \equiv \texttt{true} \wedge \big(\forall l : \texttt{list[@I]}\ \texttt{isPrefix}(\texttt{tl}(k), \texttt{append}(\texttt{tl}(k), l)) \equiv \texttt{true}\big)$
$$\rightarrow \texttt{isPrefix}(k, \texttt{append}(k, l)) \equiv \texttt{true}$$

  Zuerst formulieren wir die Hypothese um:

$$\begin{aligned} ?::(k) \equiv \texttt{true} &\underset{(5)(a)}{\Leftrightarrow} k = \texttt{hd}(k)::\texttt{tl}(k) \equiv \texttt{true} \\ &\underset{\mathcal{E}_P}{\Leftrightarrow} k \equiv \texttt{hd}(k)::\texttt{tl}(k) \qquad (\dagger) \end{aligned}$$

  Aus $?\emptyset(k) \underset{(5)(a)}{\equiv} k = \emptyset \underset{(\dagger)}{\equiv} \texttt{hd}(k)::\texttt{tl}(k) = \emptyset \underset{(3)(a)}{\equiv} \texttt{false}$ folgt:

$$?\emptyset(k) \equiv \texttt{false} \qquad (\ddagger)$$

  Da $x \equiv x$ gilt, folgt mit $\mathcal{E}_P$:

$$x = x \equiv \texttt{true} \qquad (\textit{refl})$$

$$
\begin{array}{ll}
& \texttt{isPrefix}(k, \texttt{append}(k, l)) \\
\underset{AX_{\texttt{append}}}{\equiv} & \texttt{isPrefix}(k, \texttt{if}\{?\emptyset(k), l, \texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)\}) \\
\underset{(\ddagger)}{\equiv} & \texttt{isPrefix}(k, \texttt{if}\{\texttt{false}, l, \texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)\}) \\
\underset{(4)(b)}{\equiv} & \texttt{isPrefix}(k, \underbrace{\texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)}_{t}) \\
\underset{AX_{\texttt{isPrefix}}}{\equiv} & \texttt{if}\{?\emptyset(k), \ldots, \texttt{if}\{?\emptyset(t), \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\}\} \\
\underset{(\ddagger)}{\equiv} & \texttt{if}\{\texttt{false}, \ldots, \texttt{if}\{?\emptyset(t), \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\}\} \\
\underset{(4)(b)}{\equiv} & \texttt{if}\{?\emptyset(t), \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\} \\
\underset{(5)(a)}{\equiv} & \texttt{if}\{t{=}\emptyset, \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\} \\
\underset{(3)(a)}{\equiv} & \texttt{if}\{\texttt{false}, \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\} \\
\underset{(4)(b)}{\equiv} & \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\} \\
\underset{(2)(a)}{\equiv} & \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(k), \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\} \\
\underset{(\mathit{refl})}{\equiv} & \texttt{if}\{\texttt{true}, \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\} \\
\underset{(4)(a)}{\equiv} & \texttt{isPrefix}(\texttt{tl}(k), \texttt{tl}(t)) \\
\underset{(2)(a)}{\equiv} & \texttt{isPrefix}(\texttt{tl}(k), \texttt{append}(\texttt{tl}(k), l)) \\
\underset{(IH_2)}{\equiv} & \texttt{true}
\end{array}
$$

(d) Warum erscheint eine Induktion über die Variable `l` wenig aussichtsreich?

Lösungsvorschlag

Eine Induktion über `l` würde dazu führen, dass schon im Basisfall die Hypothese sich nicht anwenden ließe, man würde also nach der Anwendung von $AX_{\texttt{isPrefix}}$ bzw. $AX_{\texttt{append}}$ nicht weiterkommen. Der Grund dafür ist, dass `l` als unverändertes Argument in `append` bleibt und somit ist das Zeigen von $\texttt{l} = \emptyset$ und $\texttt{l} \neq \emptyset$ für eine Induktion nicht geeignet.