Formale Grundlagen der Informatik 3

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

Lösungsvorschlag zu Übung 6

Version 1 vom 27.01.2012

Aufgabe 6.1 (Induktion)

Betrachten Sie das folgende $\mathcal{L}$-Programm P:

```
structure bool <=
  true, false

structure ℕ <=
  0, +(− : ℕ)

function dbl(n : nat) : nat <=
if ?0(n)
  then 0
  else +(+(dbl(−(n))))
end_if

function even(n : nat) : bool <=
if ?0(n)
  then true
  else if even(−(n))
    then false
    else true
  end_if
end_if

lemma double_is_even <= ∀ x : ℕ
      even(dbl(x))
```

Beweisen Sie $AX_{\texttt{double\_is\_even}}$ durch Induktion über `x` mittels der Relationenbeschreibung

$$R := \{\langle\{\texttt{?0(x)}\}, \emptyset\rangle, \langle\{\neg\texttt{?0(x)}\}, \{\{\texttt{x}/^{-}\texttt{(x)}\}\}\rangle\}.$$

Gehen Sie dazu wie folgt vor:

(a) Geben Sie die Menge AX_P der Axiome zum Programm P an, verweisen Sie dazu gegebenenfalls auf Beispiele aus den Vorlesungsunterlagen.

Lösungsvorschlag

$$
\begin{aligned}
AX_P &= AX_{\texttt{bool}} \cup AX_{\mathbb{N}} \cup \{AX_{\texttt{dbl}}, AX_{\texttt{even}}\} \\
AX_{\texttt{bool}} &= \big\{\forall x, y : \texttt{bool}\ \texttt{if}_{\texttt{bool}}\{\texttt{true}, x, y\} \equiv x, && (1)\\
&\qquad \forall x, y : \texttt{bool}\ \texttt{if}_{\texttt{bool}}\{\texttt{false}, x, y\} \equiv y\big\} && (2)\\
AX_{\mathbb{N}} &= \big\{\texttt{eq}_{\mathbb{N}}(0,0) \equiv \texttt{true} && (3)\\
&\qquad \forall x : \mathbb{N}\ {}^{-}({}^{+}(x)) \equiv x && (4)\\
&\qquad \forall x, y : \mathbb{N}\ \texttt{eq}_{\mathbb{N}}({}^{+}(x), {}^{+}(y)) \equiv \texttt{eq}_{\mathbb{N}}(x, y) && (5)\\
&\qquad \forall x : \mathbb{N}\ \texttt{eq}_{\mathbb{N}}(0, {}^{+}(x)) \equiv \texttt{false} && (6)\\
&\qquad \forall x : \mathbb{N}\ \texttt{eq}_{\mathbb{N}}({}^{+}(x), 0) \equiv \texttt{false} && (7)\\
&\qquad \forall x, y : \mathbb{N}\ \texttt{if}_{\mathbb{N}}\{\texttt{true}, x, y\} \equiv x && (8)\\
&\qquad \forall x, y : \mathbb{N}\ \texttt{if}_{\mathbb{N}}\{\texttt{false}, x, y\} \equiv y && (9)\\
&\qquad \forall x : \mathbb{N}\ ?0(x) \equiv \texttt{eq}_{\mathbb{N}}(x, 0) && (10)\\
&\qquad \forall x : \mathbb{N}\ ?^{+}(x) \equiv \texttt{eq}_{\mathbb{N}}(x, {}^{+}({}^{-}(x)))\big\} && (11)\\
AX_{\texttt{dbl}} &= \forall n : \mathbb{N}\ \texttt{dbl}(n) \equiv \texttt{if}_{\mathbb{N}}\{?0(n), 0, {}^{+}({}^{+}(\texttt{dbl}({}^{-}(n))))\} && (12)\\
AX_{\texttt{even}} &= \forall n : \mathbb{N}\ \texttt{even}(n) \equiv \texttt{if}_{\texttt{bool}}\{?0(n), \texttt{true}, \texttt{if}_{\texttt{bool}}\{\texttt{even}({}^{-}(n)), \texttt{false}, \texttt{true}\}\} && (13)
\end{aligned}
$$

(b) Bilden Sie die Induktionsformeln (nach Kapitel 6, Folie 19f.) in Form von HPL-Sequenzen $seq_{\mathcal{I}_i}$für den Rumpf b des Lemmas `double_is_even` und eine geeignete Umbenennung R' von R.

Lösungsvorschlag

$$
\begin{aligned}
seq_{\mathcal{I}_1} &= \langle \{?0(x)\}, \emptyset \Vdash \texttt{even}(\texttt{dbl}(x)) \rangle \\
seq_{\mathcal{I}_2} &= \langle \{\neg ?0(x)\}, \{\texttt{even}(\texttt{dbl}({}^{-}(x)))\} \Vdash \texttt{even}(\texttt{dbl}(x)) \rangle
\end{aligned}
$$

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

$$
AX_P \cup \mathcal{E}_P \models \forall x : \mathbb{N}\ \left(\bigwedge_{h \in H_i} h \equiv \texttt{true} \wedge \bigwedge_{ih \in IH_i} ih \equiv \texttt{true} \right) \rightarrow b \equiv \texttt{true}
$$

Geben Sie in jedem Schritt an, welche Gleichung Sie anwenden.

Lösungsvorschlag

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

- $?0(x) \equiv \texttt{true} \rightarrow \texttt{even}(\texttt{dbl}(x)) \equiv \texttt{true}$

$$
\begin{aligned}
\texttt{even}(\texttt{dbl}(x)) &\equiv \texttt{even}(\texttt{if}_{\mathbb{N}}\{?0(x), 0, {}^{+}({}^{+}(\texttt{dbl}({}^{-}(x))))\}) && (12)\\
&\equiv \texttt{even}(\texttt{if}_{\mathbb{N}}\{\texttt{true}, 0, {}^{+}({}^{+}(\texttt{dbl}({}^{-}(x))))\}) && (H_1)\\
&\equiv \texttt{even}(0) && (8)\\
&\equiv \texttt{if}_{\texttt{bool}}\{?0(0), \texttt{true}, \texttt{if}_{\texttt{bool}}\{\texttt{even}({}^{-}(0)), \texttt{false}, \texttt{true}\}\} && (13)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{eq}_{\mathbb{N}}(0,0), \texttt{true}, \texttt{if}_{\texttt{bool}}\{\texttt{even}({}^{-}(0)), \texttt{false}, \texttt{true}\}\} && (10)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{true}, \texttt{true}, \texttt{if}_{\texttt{bool}}\{\texttt{even}({}^{-}(0)), \texttt{false}, \texttt{true}\}\} && (3)\\
&\equiv \texttt{true} && (1)
\end{aligned}
$$

Also gilt $AX_P \cup \mathcal{E}_P \models \forall x : \mathbb{N}\ ?0(x) \equiv \texttt{true} \rightarrow \texttt{even}(\texttt{dbl}(x)) \equiv \texttt{true}$.

- $\neg ?0(x) \equiv \texttt{true} \wedge \texttt{even}(\texttt{dbl}(^-(x))) \equiv \texttt{true} \rightarrow \texttt{even}(\texttt{dbl}(x))$

  Zunächst müssen wir aus der Hypothese eine nützliche Gleichung gewinnen. Dazu lösen wir die Abkürzung auf: $\neg ?0(x) \equiv \texttt{if}_{\texttt{bool}}\{?0(x), \texttt{false}, \texttt{true}\}$. Mit $\mathcal{E}_P$ können wir nun eine Fallunterscheidung über $?0(x)$ vornehmen:

  $?0(x) \equiv \texttt{true}$: Dann gilt $\texttt{true} \equiv \texttt{if}_{\texttt{bool}}\{\texttt{true}, \texttt{false}, \texttt{true}\} \underset{(1)}{\equiv} \texttt{false}$, ein Widerspruch.

  $?0(x) \equiv \texttt{false}$: Dann gilt $\texttt{true} \equiv \texttt{if}_{\texttt{bool}}\{\texttt{false}, \texttt{false}, \texttt{true}\} \underset{(2)}{\equiv} \texttt{true}$.

  Da der erste Fall zu einem Widerspruch führt, muss der zweite Fall gelten, also $?0(x) \equiv \texttt{false}$ (†).

$$
\begin{aligned}
\texttt{even}(\texttt{dbl}(x)) &\equiv \texttt{even}(\texttt{if}_{\mathbb{N}}\{?0(x), 0, {}^+({}^+(\texttt{dbl}(^-(x))))\}) && (12)\\
&\equiv \texttt{even}(\texttt{if}_{\mathbb{N}}\{\texttt{false}, 0, {}^+({}^+(\texttt{dbl}(^-(x))))\}) && (\dagger)\\
&\equiv \texttt{even}({}^+({}^+(\texttt{dbl}(^-(x))))) && (9)\\
&\equiv \texttt{if}_{\texttt{bool}}\{?0({}^+({}^+(\texttt{dbl}(^-(x))))), \texttt{true},\\
&\qquad \texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+({}^+(\texttt{dbl}(^-(x)))))), \texttt{false}, \texttt{true}\}\} && (13)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{eq}_{\mathbb{N}}({}^+({}^+(\texttt{dbl}(^-(x)))), 0), \texttt{true},\\
&\qquad \texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+({}^+(\texttt{dbl}(^-(x)))))), \texttt{false}, \texttt{true}\}\} && (10)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{false}, \texttt{true}, \texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+({}^+(\texttt{dbl}(^-(x)))))), \texttt{false}, \texttt{true}\}\} && (7)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+({}^+(\texttt{dbl}(^-(x)))))), \texttt{false}, \texttt{true}\} && (9)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{even}({}^+(\texttt{dbl}(^-(x)))), \texttt{false}, \texttt{true}\} && (4)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{if}_{\texttt{bool}}\{?0({}^+(\texttt{dbl}(^-(x)))), \texttt{true},\\
&\qquad \texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+(\texttt{dbl}(^-(x))))), \texttt{false}, \texttt{true}\}\}, \texttt{false}, \texttt{true}\} && (13)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{if}_{\texttt{bool}}\{\texttt{eq}_{\mathbb{N}}({}^+(\texttt{dbl}(^-(x))), 0), \texttt{true},\\
&\qquad \texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+(\texttt{dbl}(^-(x))))), \texttt{false}, \texttt{true}\}\}, \texttt{false}, \texttt{true}\} && (10)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{if}_{\texttt{bool}}\{\texttt{false}, \texttt{true},\\
&\qquad \texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+(\texttt{dbl}(^-(x))))), \texttt{false}, \texttt{true}\}\}, \texttt{false}, \texttt{true}\} && (7)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{if}_{\texttt{bool}}\{\texttt{even}(^-({}^+(\texttt{dbl}(^-(x))))), \texttt{false}, \texttt{true}\}, \texttt{false}, \texttt{true}\} && (9)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{if}_{\texttt{bool}}\{\texttt{even}(\texttt{dbl}(^-(x))), \texttt{false}, \texttt{true}\}, \texttt{false}, \texttt{true}\} && (4)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{if}_{\texttt{bool}}\{\texttt{true}, \texttt{false}, \texttt{true}\}, \texttt{false}, \texttt{true}\} && (IH_2)\\
&\equiv \texttt{if}_{\texttt{bool}}\{\texttt{false}, \texttt{false}, \texttt{true}\} && (1)\\
&\equiv \texttt{true} && (2)
\end{aligned}
$$

  Also gilt: $AX_P \cup \mathcal{E}_P \models \forall x : \mathbb{N}\ \big(\neg ?0(x) \equiv \texttt{true} \wedge \texttt{even}(\texttt{dbl}(^-(x))) \equiv \texttt{true}\big) \rightarrow \texttt{even}(\texttt{dbl}(x))$.

Aufgabe 6.2 (Induktion)

Betrachten Sie das folgende $\mathcal{L}$-Programm P:

```
structure bool <=
  true, false

structure ℕ <=
  0, +(- : ℕ)

structure list[@I] <=
  ∅, [infixr,100] ::(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

lemma left neut <= ∀ k : list[@I]
  append(ø, k) = k

lemma right neut <= ∀ k : list[@I]
  append(k, ø) = k
```

(a) Geben Sie die Axiome $AX_{\texttt{list[@I]}}$ und $AX_{\texttt{append}}$ an. Verweisen Sie dazu gegebenenfalls auf Beispiele aus den Vorlesungsunterlagen.

Lösungsvorschlag

Bemerkung: Im Folgenden schreiben wir `if` anstatt $\texttt{if}_{struc}$ und `a=b` anstatt $\texttt{eq}_{struc}\texttt{(a, b)}$ (vergleiche Folie 5, Kapitel 9).

$$
\begin{aligned}
AX_{\texttt{list[@I]}} = \{&\texttt{ø=ø} \equiv \texttt{true} && (1)\\
&\forall n : \texttt{@I}, k : \texttt{list[@I]}\ \texttt{hd}(n :: k) \equiv n && (2)\\
&\forall n : \texttt{@I}, k : \texttt{list[@I]}\ \texttt{tl}(n :: k) \equiv k && (3)\\
&\forall n_1, n_2 : \texttt{@I}, k_1, k_2 : \texttt{list[@I]}\ n_1 :: k_1 \texttt{=} n_2 :: k_2 \equiv \texttt{if}\{n_1\texttt{=}n_2, k_1\texttt{=}k_2, \texttt{false}\} && (4)\\
&\forall n : \texttt{@I}, k : \texttt{list[@I]}\ \texttt{ø=}n :: k \equiv \texttt{false} && (5)\\
&\forall n : \texttt{@I}, k : \texttt{list[@I]}\ n :: k\texttt{=ø} \equiv \texttt{false} && (6)\\
&\forall k, l : \texttt{list[@I]}\ \texttt{if}\{\texttt{true}, k, l\} \equiv k && (7)\\
&\forall k, l : \texttt{list[@I]}\ \texttt{if}\{\texttt{false}, k, l\} \equiv l && (8)\\
&\forall k : \texttt{list[@I]}\ ?\texttt{ø}(k) \equiv k\texttt{=ø} && (9)\\
&\forall k : \texttt{list[@I]}\ ?::(k) \equiv k\texttt{=}\texttt{hd}(k) :: \texttt{tl}(k)\} && (10)\\
AX_{\texttt{append}} = \forall k, l : \texttt{list[@I]}\ &\texttt{append}(k, l) \equiv \texttt{if}\{?\texttt{ø}(k), l, \texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)\} && (11)
\end{aligned}
$$

(b) Beweisen Sie das Lemma `left neut`.

Lösungsvorschlag

$$
\begin{aligned}
\texttt{append}(\texttt{ø}, k) &\underset{(11)}{\equiv} \texttt{if}\{?\texttt{ø}(\texttt{ø}), k, \texttt{hd}(\texttt{ø}) :: \texttt{append}(\texttt{tl}(\texttt{ø}), k)\}\\
&\underset{(9)}{\equiv} \texttt{if}\{\texttt{ø=ø}, k, \texttt{hd}(\texttt{ø}) :: \texttt{append}(\texttt{tl}(\texttt{ø}), k)\}\\
&\underset{(1)}{\equiv} \texttt{if}\{\texttt{true}, k, \texttt{hd}(\texttt{ø}) :: \texttt{append}(\texttt{tl}(\texttt{ø}), k)\}\\
&\underset{(7)}{\equiv} k
\end{aligned}
$$

(c) Bilden Sie die Induktionsformeln in Form von HPL-Sequenzen für den Rumpf b des Lemmas `right neut` und die Relationenbeschreibung

$$R' := \{\langle\{\texttt{?ø(k)}\}, \emptyset\rangle, \langle\{\texttt{?::(k)}\}, \{\{\texttt{k/tl(k)}\}\}\rangle\}.$$

Lösungsvorschlag

$$seq_{\mathcal{I}_1} = \langle \{?\emptyset(k)\}, \emptyset \Vdash \texttt{append}(k, \emptyset)\texttt{=}k \rangle$$
$$seq_{\mathcal{I}_2} = \langle \{?\texttt{::}(k)\}, \{\texttt{append}(\texttt{tl}(k), \emptyset)\texttt{=}\texttt{tl}(k)\} \Vdash \texttt{append}(k, \emptyset)\texttt{=}k \rangle$$

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

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

Geben Sie in jedem Schritt die verwendete Gleichung an.

Lösungsvorschlag

Mit $\mathcal{E}_P$ ist $\texttt{append}(k, \emptyset)\texttt{=}k \equiv \texttt{true} \leftrightarrow \texttt{append}(k, \emptyset) \equiv k$.

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

$$\begin{aligned} \texttt{append}(k, \emptyset) &\underset{(11)}{\equiv} \texttt{if}\{?\emptyset(k), \emptyset, \ldots\} \\ &\underset{(H_1)}{\equiv} \texttt{if}\{\texttt{true}, \emptyset, \ldots\} \\ &\underset{(7)}{\equiv} \emptyset \end{aligned}$$

  Mit (9) erhalten wir aus der Hypothese die Gleichung $k\texttt{=}\emptyset \equiv \texttt{true}$, zusammen mit $\mathcal{E}_P$ also $k \equiv \emptyset$.

- $?\texttt{::}(k) \equiv \texttt{true} \wedge \texttt{append}(\texttt{tl}(k), \emptyset)\texttt{=}\texttt{tl}(k) \equiv \texttt{true} \rightarrow \texttt{append}(k, \emptyset) \equiv k$

  Wir formulieren die Hypothese um:

$$\begin{aligned} ?\texttt{::}(k) \equiv \texttt{true} &\underset{(10)}{\Leftrightarrow} k = \texttt{hd}(k)\texttt{::}\texttt{tl}(k) \equiv \texttt{true} \\ &\underset{\mathcal{E}_P}{\Leftrightarrow} k \equiv \texttt{hd}(k)\texttt{::}\texttt{tl}(k) \qquad (10') \end{aligned}$$

  Aus $?\emptyset(k) \underset{(9)}{\equiv} k = \emptyset \underset{(10')}{\equiv} \texttt{hd}(k)\texttt{::}\texttt{tl}(k) = \emptyset \underset{(6)}{\equiv} \texttt{false}$ folgt:

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

  Aus der Induktionshypothese erhalten wir mit $\mathcal{E}_P$ die Gleichung $\texttt{append}(\texttt{tl}(k), \emptyset) \equiv \texttt{tl}(k)$ $(\ddagger)$.

$$\begin{aligned} \texttt{append}(k, \emptyset) &\underset{(11)}{\equiv} \texttt{if}\{?\emptyset(k), \emptyset, \texttt{hd}(k) \texttt{::} \texttt{append}(\texttt{tl}(k), \emptyset)\} \\ &\underset{(\dagger)}{\equiv} \texttt{if}\{\texttt{false}, \emptyset, \texttt{hd}(k) \texttt{::} \texttt{append}(\texttt{tl}(k), \emptyset)\} \\ &\underset{(8)}{\equiv} \texttt{hd}(k) \texttt{::} \texttt{append}(\texttt{tl}(k), \emptyset) \\ &\underset{(\ddagger)}{\equiv} \texttt{hd}(k) \texttt{::} \texttt{tl}(k) \\ &\underset{(10')}{\equiv} k \end{aligned}$$