Formale Grundlagen der Informatik 3

Prof. Dr. Christoph Walther / Simon Siegler, Nathan Wasser
Technische Universität Darmstadt — Wintersemester 2009/10

Lösungsvorschlag zu Hausübung 4

Aufgabe 4.1 (Terminierung) (18 Punkte)

Beweisen Sie die Terminierung der Prozeduren `m` und `f` aus dem nachfolgenden $\mathcal{L}$-Programm, gehen Sie dazu jeweils wie folgt vor:

(a) Bestimmen Sie geeignete Maßterme für den Terminierungsbeweis. Überlegen Sie sich dazu, was bei den rekursiven Aufrufen kleiner wird.

(b) Geben Sie die zusammengesetzte Relationenbeschreibung der Prozedur an.

(c) Geben Sie die aus Maßtermen und Relationenbeschreibung gebildeten Terminierungshypothesen an.

(d) Normalisierung Sie die Terminierungshypothesen gemäß dem Verfahren aus der Vorlesung und vereinfachen Sie diese.

(e) Belegen Sie die Gültigkeit der Terminierungshypothesen durch Anwendung bekannter arithmetischer Gleichungen.

```
structure bool <=
  true, false

structure ℕ
  0, ⁺(⁻ : ℕ)

structure list[@I] <=
  ∅, [infixr,1] ::(hd : @I, tl : list[@I])

function m(a, b : ℕ) : ℕ <=
if ?0(a)
  then b
  else if ?0(b)
         then a
         else m(⁻(b), ⁻(a))
       end_if
end_if
```

```
function f(k : list[ℕ]) : list[ℕ] <=
if ?∅(k)
  then k
  else if ?∅(tl(k))
         then k
         else if hd(k) > hd(tl(k))
                then f(hd(k) :: ⁺(hd(tl(k)))
                               :: tl(tl(k)))
                else hd(k) :: f(tl(k))
              end_if
       end_if
end_if
```

Lösungsvorschlag

Wir beginnen mit der Prozedur `m`:

(a) Als Maßterm wählen wir das Minimum der beiden Argumente $\min(a, b)$.

(b) $R_{\mathtt{m}} = \big\{\langle\{?0(a)\}, \emptyset\rangle, \langle\{\neg?0(a), ?0(b)\}, \emptyset\rangle, \langle\{\neg?0(a), \neg?0(b)\}, \{a/^{-}(b), b/^{-}(a)\}\rangle\big\}$

(c) $\forall a, b : \mathbb{N}\ \mathtt{if}\{\mathtt{if}\{\neg?0(a), \neg?0(b), \mathtt{false}\}, \min(a, b) > \min(^{-}(b), ^{-}(a)), \mathtt{true}\}$

(d) $\forall a, b : \mathbb{N}\ \mathtt{if}\{?0(a), \mathtt{true}, \mathtt{if}\{?0(b), \mathtt{true}, \min(a, b) > \min(^{-}(b), ^{-}(a))\}\}$

Alternativ: $\forall a, b : \mathbb{N}\ \mathtt{if}\{\neg?0(a), \mathtt{if}\{\neg?0(b), \min(a, b) > \min(^{-}(b), ^{-}(a)), \mathtt{true}\}, \mathtt{true}\}$

(e) Als Bedingungen gelten $a > 0$ und $b > 0$, zu zeigen ist $\min(a, b) > \min(b-1, a-1)$. Falls $a \leq b$, dann ist $\min(a, b) = a$ und wegen $a - 1 \leq b - 1$ gilt $\min(b-1, a-1) = a - 1$, zu zeigen ist also $a > a - 1$, was unter diesen Bedingungen offensichtlich ist. Andernfalls ist $a > b$, damit ist $\min(a, b) = b$ und wegen $a - 1 > b - 1$ gilt $\min(b-1, a-1) = b - 1$. Auch $b > b - 1$ gilt offensichtlich.

Nun behandeln wir Prozedur `f`:

(a) Als Maßterme wählen wir die Länge der Liste $\text{length}(k)$ und die Differenz zwischen den beiden ersten Listenelementen $\texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k))$.

(b)

$$\begin{aligned} R_{\texttt{f},1} = \big\{ & \big\langle \{?\emptyset(k)\}, \emptyset \big\rangle, \big\langle \{\neg ?\emptyset(k), ?\emptyset(\texttt{tl}(k))\}, \emptyset \big\rangle, \\ & \big\langle \{\neg ?\emptyset(k), \neg ?\emptyset(\texttt{tl}(k)), \texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k))\}, \{k/\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))\} \big\rangle, \\ & \big\langle \{\neg ?\emptyset(k), \neg ?\emptyset(\texttt{tl}(k)), \neg \texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k))\}, \{k/\texttt{tl}(k)\} \big\rangle \big\} \end{aligned}$$

(c) Wir erhalten die Terminierungshypothesen

$$\begin{aligned} & \forall k : \texttt{list[@I]}\ \texttt{if}\{\texttt{if}\{\texttt{if}\{\neg ?\emptyset(k), \neg ?\emptyset(\texttt{tl}(k)), \texttt{false}\}, \texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k)), \texttt{false}\}, \\ & \qquad \texttt{if}\{\text{length}(k) > \text{length}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))), \texttt{true}, \\ & \qquad\quad \texttt{if}\{\text{length}(k) = \text{length}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))), \\ & \qquad\qquad \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \\ & \qquad\qquad\quad \texttt{hd}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))) \\ & \qquad\qquad\quad - \texttt{hd}(\texttt{tl}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k)))), \texttt{true}\}\}, \texttt{true}\} \end{aligned}$$

und

$$\begin{aligned} & \forall k : \texttt{list[@I]}\ \texttt{if}\{\texttt{if}\{\texttt{if}\{\neg ?\emptyset(k), \neg ?\emptyset(\texttt{tl}(k)), \texttt{false}\}, \neg \texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k)), \texttt{false}\}, \\ & \qquad \texttt{if}\{\text{length}(k) > \text{length}(\texttt{tl}(k)), \texttt{true}, \\ & \qquad\quad \texttt{if}\{\text{length}(k) = \text{length}(\texttt{tl}(k)), \\ & \qquad\qquad \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \texttt{hd}(\texttt{tl}(k)) - \texttt{hd}(\texttt{tl}(\texttt{tl}(k))), \texttt{true}\}\}, \texttt{true}\} \end{aligned}$$

(d)

$$\begin{aligned} & \forall k : \texttt{list[@I]}\ \texttt{if}\{?\emptyset(k), \texttt{true}, \texttt{if}\{?\emptyset(\texttt{tl}(k)), \texttt{true}, \texttt{if}\{\texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k)), \\ & \qquad \texttt{if}\{\text{length}(k) > \text{length}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))), \texttt{true}, \\ & \qquad\quad \texttt{if}\{\text{length}(k) = \text{length}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))), \\ & \qquad\qquad \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \\ & \qquad\qquad\quad \texttt{hd}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))) \\ & \qquad\qquad\quad - \texttt{hd}(\texttt{tl}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k)))), \texttt{true}\}\}, \texttt{true}\}\} \end{aligned}$$

und

$$\begin{aligned} & \forall k : \texttt{list[@I]}\ \texttt{if}\{?\emptyset(k), \texttt{true}, \texttt{if}\{?\emptyset(\texttt{tl}(k)), \texttt{true}, \texttt{if}\{\texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k)), \texttt{true}, \\ & \qquad \texttt{if}\{\text{length}(k) > \text{length}(\texttt{tl}(k)), \texttt{true}, \\ & \qquad\quad \texttt{if}\{\text{length}(k) = \text{length}(\texttt{tl}(k)), \\ & \qquad\qquad \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \texttt{hd}(\texttt{tl}(k)) - \texttt{hd}(\texttt{tl}(\texttt{tl}(k))), \texttt{true}\}\}\} \end{aligned}$$

Alternativ:

$$\begin{aligned} & \forall k : \texttt{list[@I]}\ \texttt{if}\{\neg ?\emptyset(k), \texttt{if}\{\neg ?\emptyset(\texttt{tl}(k)), \texttt{if}\{\texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k)), \\ & \qquad \texttt{if}\{\text{length}(k) > \text{length}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))), \texttt{true}, \\ & \qquad\quad \texttt{if}\{\text{length}(k) = \text{length}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))), \\ & \qquad\qquad \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \\ & \qquad\qquad\quad \texttt{hd}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))) \\ & \qquad\qquad\quad - \texttt{hd}(\texttt{tl}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k)))), \texttt{true}\}\}, \texttt{true}\}, \texttt{true}\}, \texttt{true}\} \end{aligned}$$

und

$$\begin{aligned}\forall k : \texttt{list[@I]}\ \texttt{if}\{\neg ?\emptyset(k), \texttt{if}\{\neg ?\emptyset(\texttt{tl}(k)), \texttt{if}\{\neg \texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k)),\\ \texttt{if}\{\text{length}(k) > \text{length}(\texttt{tl}(k)), \texttt{true},\\ \texttt{if}\{\text{length}(k) = \text{length}(\texttt{tl}(k)),\\ \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \texttt{hd}(\texttt{tl}(k)) - \texttt{hd}(\texttt{tl}(\texttt{tl}(k))), \texttt{true}\}\}, \texttt{true}\}, \texttt{true}\}, \texttt{true}\}\end{aligned}$$

(e) 1. Offenbar sind die Längen beider Listen gleich, zu zeigen ist also, dass für eine Liste k mit mindestens zwei Elementen und $\texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k))$ gilt:

$$\texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \texttt{hd}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))) - \texttt{hd}(\texttt{tl}(\texttt{hd}(k) :: {}^{+}(\texttt{hd}(\texttt{tl}(k))) :: \texttt{tl}(\texttt{tl}(k))))$$

Dies ist läßt sich vereinfachen zu:

$$\texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \texttt{hd}(k) - {}^{+}(\texttt{hd}(\texttt{tl}(k))), \text{ also } \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) > \texttt{hd}(k) - \texttt{hd}(\texttt{tl}(k)) - 1$$

Dies gilt mit $\texttt{hd}(k) > \texttt{hd}(\texttt{tl}(k))$ offensichtlich.

2. Da die Länge von $\texttt{tl}(k)$ für eine nicht-leere Liste k sicher kleiner als die Länge von k ist, gilt die Aussage offensichtlich.

Aufgabe 4.2 (Induktion) (22 Punkte)

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

```
structure bool <=
  true, false

structure ℕ <=
  0, +(⁻ : ℕ)

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

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

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

lemma inv <= ∀ k, l : list[@I]
  f(k, append(k, l)) = l
```

(a) Geben Sie die Axiome $AX_{\texttt{append}}, AX_{\texttt{f}}$ und $AX_{\texttt{inv}}$ an.

Lösungsvorschlag

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

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

$$AX_{\texttt{inv}} = \forall\, k, l : \texttt{list[@I]}\ \texttt{f}(k, \texttt{append}(k, l))\texttt{=}l \equiv \texttt{true}$$

(b) Bilden Sie die Induktionsformeln in Form von HPL-Sequenzen für den Rumpf b des Lemmas `inv` und eine geeignete Umbenennung $R'_{\texttt{list[@I]}}$ von $R_{\texttt{list[@I]}}$.

Lösungsvorschlag

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

(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.

Lösungsvorschlag

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

Mit $\mathcal{E}_P$ ist $\texttt{f}(k, \texttt{append}(k, l))\texttt{=}l \equiv \texttt{true} \leftrightarrow \texttt{f}(k, \texttt{append}(k, l)) \equiv l$, wir zeigen also jeweils:

$$\texttt{f}(k, \texttt{append}(k, l)) \equiv l$$

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

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

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

  Mit $\mathcal{E}_P$ gewinnen wir durch Fallunterscheidung aus der Hypothese die Gleichung $?\emptyset(k) \equiv \texttt{false}$ (†).

  Die Induktionshypothese ist mit $\mathcal{E}_P$ äquivalent zu $\forall l : \texttt{list[@I]}\ \texttt{f}(\texttt{tl}(k), \texttt{append}(\texttt{tl}(k), l)) \equiv l$ (‡).

Schließlich folgt mit $\mathcal{E}_P$ und der Reflexivität von $\equiv$ auch $\forall\, l : \texttt{list[@I]}\ l{=}l \equiv \texttt{true}$ (*refl*).

$$
\begin{aligned}
\texttt{f}(k, \texttt{append}(k, l)) &\underset{AX_{\texttt{append}}}{\equiv} \texttt{f}(k, \texttt{if}\{?\emptyset(k), l, \texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)\}) \\
&\underset{(\dagger)}{\equiv} \texttt{f}(k, \texttt{if}\{\texttt{false}, l, \texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)\}) \\
&\underset{(4)(b)}{\equiv} \texttt{f}(k, \underbrace{\texttt{hd}(k) :: \texttt{append}(\texttt{tl}(k), l)}_{t}) \\
&\underset{AX_{\texttt{f}}}{\equiv} \texttt{if}\{?\emptyset(k), \ldots, \texttt{if}\{?\emptyset(t), \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\}\} \\
&\underset{(\dagger)}{\equiv} \texttt{if}\{\texttt{false}, \ldots, \texttt{if}\{?\emptyset(t), \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\}\} \\
&\underset{(4)(b)}{\equiv} \texttt{if}\{?\emptyset(t), \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\} \\
&\underset{(5)(a_1)}{\equiv} \texttt{if}\{t{=}\emptyset, \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\} \\
&\underset{(3)(a_2)}{\equiv} \texttt{if}\{\texttt{false}, \ldots, \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\}\} \\
&\underset{(4)(b)}{\equiv} \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(t), \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\} \\
&\underset{(2)(a1)}{\equiv} \texttt{if}\{\texttt{hd}(k){=}\texttt{hd}(k), \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\} \\
&\underset{(refl)}{\equiv} \texttt{if}\{\texttt{true}, \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)), \ldots\} \\
&\underset{(4)(a)}{\equiv} \texttt{f}(\texttt{tl}(k), \texttt{tl}(t)) \\
&\underset{(2)(a_2)}{\equiv} \texttt{f}(\texttt{tl}(k), \texttt{append}(\texttt{tl}(k), l)) \\
&\underset{(\ddagger)}{\equiv} l
\end{aligned}
$$