Formale Grundlagen der Informatik 3

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

Lösungsvorschlag zu Übung 4

Version 1 vom 20.12.2011

Hinweis: Im Folgenden bezeichnet $>$ die übliche (transitive) Ordnung auf den natürlichen Zahlen.

Aufgabe 4.1 (Fundierte Mengen)

Beweisen oder widerlegen Sie die Fundiertheit der folgenden Mengen:

1. $(\mathbb{Z}, >_{\mathsf{abs}})$ mit $n >_{\mathsf{abs}} m$ genau dann, wenn $|n| > |m|$

   ### Lösungsvorschlag

   Die Menge ist fundiert. Zum Beweis nehmen wir an, sie sei nicht fundiert, d. h. es gibt eine unendliche Folge $\langle m_i \rangle_{i \in \mathbb{N}}$ mit $m_i >_{\mathsf{abs}} m_{i+1}$. Also ist $|m_i| > |m_{i+1}|$ und somit ist $\langle |m_i| \rangle_{i \in \mathbb{N}}$ eine unendlich absteigende Folge in $\mathbb{N}$. Da aber $(\mathbb{N}, >)$ fundiert ist, kann es keine solche Folge geben. Die Annahme, $(\mathbb{Z}, >_{\mathsf{abs}})$ sei nicht fundiert, muss also falsch gewesen sein.

2. $(\mathcal{C}_{\mathtt{list}[\mathbb{N}]}, \triangleright)$ mit $k \triangleright l$ genau dann, wenn $k \neq \varnothing \wedge \big(l = \varnothing \vee \mathtt{hd}(k) > \mathtt{hd}(l) \vee \mathtt{tl}(k) \triangleright \mathtt{tl}(l)\big)$

   ### Lösungsvorschlag

   Die Menge ist nicht fundiert: Mit $m_1 := 2 :: 1 :: \varnothing$ und $m_2 := 1 :: 2 :: \varnothing$ erhält man die unendlich absteigende Kette $m_1, m_2, m_1, m_2, \ldots$.

3. $(\mathbb{N} \times \mathbb{N}, \succ)$ mit $(n_1, m_1) \succ (n_2, m_2)$ genau dann, wenn $n_1 > n_2$ oder $n_1 = n_2$ und $m_1 > m_2$.

   ### Lösungsvorschlag

   Die Menge ist fundiert. Zum Beweis nehmen wir an, sie sei nicht fundiert, d. h. es gibt eine unendlich absteigende Folge $\langle (n_i, m_i) \rangle_{i \in \mathbb{N}}$ mit (*) $(n_i, m_i) \succ (n_{i+1}, m_{i+1})$. Wir unterscheiden zwei Fälle:

   a) Es gibt ein $j \in \mathbb{N}$, so dass $n_j = n_k$ für alle $k > j$. Damit gilt für alle $k > j$ wegen (*), dass $m_k > m_{k+1}$ im Widerspruch zur Fundiertheit von $(\mathbb{N}, >)$

   b) Andernfalls gibt es für alle $j \in \mathbb{N}$ ein $k_j > j$ mit $n_j \neq n_{k_j}$. Wegen (*) gilt dann $n_j > n_{k_j} > n_{k_{k_j}} > \ldots$ für alle $j \in \mathbb{N}$ im Widerspruch zur Fundiertheit von $(\mathbb{N}, >)$.

   Da beide Fälle zu einem Widerspruch führen, muss die Annahme, dass $\succ$ nicht fundiert ist, falsch gewesen sein. Also ist die Relation fundiert.

Aufgabe 4.2 (Relationen)

Betrachten Sie die folgende Relationenbeschreibung:

$$\begin{aligned} R := \{ &\langle\{?0(x)\}, \emptyset\rangle, \\ &\langle\{\neg?0(x), ?0(y)\}, \emptyset\rangle, \\ &\langle\{\neg?0(x), \neg?0(y)\}, \{\{x/x, y/y \text{ - } x\}, \{x/x \text{ - } y, y/y\}\}\rangle\} \end{aligned}$$

Dabei ist die Prozedur „-“ wie folgt definiert:

```
function [infixl] -(a, b : ℕ) : ℕ <=
if ?0(a)
  then 0
  else if ?0(b)
         then a
         else ⁻(a) - ⁻(b)
       end_if
end_if
```

(a) Bestimmen Sie die Menge $pre_{>_{R,xy}}\big((42, 23)\big)$.

Lösungsvorschlag

Die einzige atomare rekursive Relationenbeschreibung in R ist

$$\langle\{\neg?0(x), \neg?0(y)\}, \{\{x/x, y/y \text{ - } x\}, \{x/x \text{ - } y, y/y\}\}\rangle.$$

Mit $\theta = \{x/42, y/23\}$ ist offenbar $eval_P(\neg?0(42)) = \texttt{true}$ und $eval_P(\neg?0(23)) = \texttt{true}$.

Für $\delta_1 = \{x/x, y/y \text{ - } x\}$ erhält man $(42, 23) >_{R,xy} (eval_P(42), eval_P(23 \text{ - } 42)) = (42, 0)$.

Für $\delta_2 = \{x/x \text{ - } y, y/y\}$ ergibt sich $(42, 23) >_{R,xy} (eval_P(42 \text{ - } 23), eval_P(23) = (19, 23)$.

Somit ist $pre_{>_{R,xy}}\big((42, 23)\big) = \{(42, 0), (19, 23)\}$.

(b) Geben Sie alle mit $(5, 3)$ startenden $>_{R,xy}$-Ketten an.

Lösungsvorschlag

$$\begin{aligned} &(5,3) >_{R,xy} (5,0) \\ &(5,3) >_{R,xy} (2,3) >_{R,xy} (2,1) >_{R,xy} (2,0) \\ &(5,3) >_{R,xy} (2,3) >_{R,xy} (2,1) >_{R,xy} (1,1) >_{R,xy} (1,0) \\ &(5,3) >_{R,xy} (2,3) >_{R,xy} (2,1) >_{R,xy} (1,1) >_{R,xy} (0,1) \\ &(5,3) >_{R,xy} (2,3) >_{R,xy} (0,3) \end{aligned}$$

Aufgabe 4.3 (Minimale Elemente und Vorgänger)

Bestimmen Sie für jede der folgenden fundierten Mengen $(M, \succ)$ die minimalen Elemente $min_{\succ}(M)$. Geben Sie außerdem für jedes nicht-minimale Element $m \in M \setminus min_{\succ}(M)$ die Anzahl der Vorgänger $|pre_{\succ}(m)|$ an.

1. $(\mathbb{N}, >)$

   Lösungsvorschlag

   $min_{>}(\mathbb{N}) = \{0\}$
   Für alle $m \in \mathbb{N}$ mit $m \notin min_{>}(\mathbb{N})$ gilt $|pre_{>}(m \in \mathbb{N})| = m$

2. $(\mathcal{C}_{\texttt{list}[\mathbb{N}]}, \gtrdot)$ mit $k \gtrdot l$ genau dann, wenn $k = n :: l$ für ein $n \in \mathbb{N}$.

   Lösungsvorschlag

   $min_{\gtrdot}(\mathcal{C}_{\texttt{list}[\mathbb{N}]}) = \{\varnothing\}$
   Für alle $k \in \mathcal{C}_{\texttt{list}[\mathbb{N}]}$ mit $k \notin min_{\gtrdot}(\mathcal{C}_{\texttt{list}[\mathbb{N}]})$ gilt $|pre_{\gtrdot}(k)| = 1$

3. $(\mathcal{C}_{\texttt{list}[\mathbb{N}]}, >_{\mathsf{len}})$ mit $k >_{\mathsf{len}} l$ genau dann, wenn $|k| > |l|$. Dabei ist $|k|$ die Länge der Liste k.

   Lösungsvorschlag

   $min_{>_{\mathsf{len}}}(\mathcal{C}_{\texttt{list}[\mathbb{N}]}) = \{\varnothing\}$
   Für alle $k \in \mathcal{C}_{\texttt{list}[\mathbb{N}]}$ mit $|k| > 1$ gilt $|pre_{>_{\mathsf{len}}}(k)| = \infty$, für alle $k \in \mathcal{C}_{\texttt{list}[\mathbb{N}]}$ mit $|k| = 1$ ist $|pre_{>_{\mathsf{len}}}(k)| = 1$

Aufgabe 4.4 (Strukturelle Ordnung)

Geben Sie für die folgenden Datentypen `struc` jeweils die Relationenbeschreibung $R_{\texttt{struc}}$ an.

1. ```
   structure pair[@A, @B] <=
     pair(fst : @A, snd : @B)
   ```

   Lösungsvorschlag

   $R_{\texttt{pair[@A,@B]}} = \{\langle\{\texttt{?pair(u)}\}, \emptyset\rangle\}$

2. ```
   structure tree[@V] <=
     tip,
     node(value : @V, left : tree[@V], right : tree[@V])
   ```

   Lösungsvorschlag

   $R_{\texttt{tree[@V]}} = \{\langle\{\texttt{?tip(u)}\}, \emptyset\rangle, \langle\{\texttt{?node(u)}\}, \{\{\texttt{u/left(u)}\}, \{\texttt{u/right(u)}\}\}\rangle\}$

3. ```
   structure EXPR <=
     VAR#(index : nat),
     EXPR0(e-op0 : nat),
     EXPR2(e-op2 : nat, arg1 : EXPR, arg2 : EXPR)
   ```

   Lösungsvorschlag

   $R_{\texttt{EXPR}} = \{\langle\{\texttt{?VAR\#(u)}\}, \emptyset\rangle, \langle\{\texttt{?EXPR0(u)}\}, \emptyset\rangle, \langle\{\texttt{?EXPR2(u)}\}, \{\{\texttt{u/arg1(u)}\}, \{\texttt{u/arg2(u)}\}\}\rangle\}$
   ```

Aufgabe 4.5 (Rekursion und Induktion)

Betrachten Sie die folgenden Prozeduren p:

1. ```
   function f(n : ℕ) : ℕ <=
   if ?0(n)
     then 1
     else if ?0(pred(n))
            then 1
            else f(pred(n)) + f(pred(pred(n)))
          end_if
   end_if
   ```

2. ```
   function g(n, m : ℕ) : ℕ <=
   if ?0(n)
     then 0
     else if ?0(m)
            then n
            else g(pred(n), pred(m))
          end_if
   end_if
   ```

3. ```
   function h(k : list[nat]) : ℕ <=
   if ?ø(k)
     then ⋆
     else if ?ø(tl(k))
            then hd(k)
            else if hd(k) > hd(tl(k))
                   then h(tl(k))
                   else h(hd(k) :: tl(tl(k)))
                 end_if
          end_if
   end_if
   ```

- Geben Sie zu jeder Prozedur p die zusammengesetzten Relationenbeschreibungen $R_{\mathtt{p}}$, sowie die Induktionsaxiome $IndAx_{\mathtt{p}(\ldots)>0,R_{\mathtt{p}}}$ an.
- Begründen Sie jeweils die Fundiertheit der Relationenbeschreibungen $R_{\mathtt{p}}$. Ein formaler Beweis ist nicht notwendig.

Lösungsvorschlag

1. •

$$
\begin{aligned}
R_{\mathtt{f}} = \{&\langle\{?\mathtt{0}(\mathtt{n})\}, \emptyset\rangle,\\
&\langle\{\neg?\mathtt{0}(\mathtt{n}), ?\mathtt{0}(\mathtt{pred}(\mathtt{n}))\}, \emptyset\rangle,\\
&\langle\{\neg?\mathtt{0}(\mathtt{n}), \neg?\mathtt{0}(\mathtt{pred}(\mathtt{n}))\}, \{\{\mathtt{n}/\mathtt{pred}(\mathtt{pred}(\mathtt{n}))\}, \{\mathtt{n}/\mathtt{pred}(\mathtt{n})\}\}\rangle\}
\end{aligned}
$$

$$
\begin{aligned}
IndAx_{\mathtt{f}(\mathtt{n})>0,R} = {} & \forall \mathtt{n} : \mathbb{N}\ ?\mathtt{0}(\mathtt{n}) \Rightarrow f(n) > 0\\
& \wedge \forall \mathtt{n} : \mathbb{N}\ \neg?\mathtt{0}(\mathtt{n}) \wedge ?\mathtt{0}(\mathtt{pred}(\mathtt{n})) \Rightarrow f(n) > 0\\
& \wedge \forall \mathtt{n} : \mathbb{N}\ \neg?\mathtt{0}(\mathtt{n}) \wedge \neg?\mathtt{0}(\mathtt{pred}(\mathtt{n})) \wedge \mathtt{f}(\mathtt{pred}(\mathtt{pred}(\mathtt{n}))) > \mathtt{0}\\
& \qquad \wedge \mathtt{f}(\mathtt{pred}(\mathtt{n})) > \mathtt{0} \Rightarrow \mathtt{f}(\mathtt{n}) > \mathtt{0}\\
& \Rightarrow \forall \mathtt{n} : \mathbb{N}\ \mathtt{f}(\mathtt{n}) > \mathtt{0}
\end{aligned}
$$
   ```

- Deuten wir die Terme als natürliche Zahlen, so wird deutlich, dass zu keiner Zahl m eine unendliche Kette ($m >_{R_\mathtt{f}} m_1 >_{R_\mathtt{f}} m_2 >_{R_\mathtt{f}} \ldots$) existieren kann, da spätestens für m_m kein Nachfolger mehr existieren kann, weil einer der Basisfälle 0 oder 1 erreicht ist.

2. •

$$
\begin{aligned}
R_\mathtt{g} = \{&\langle\{?\mathtt{0}(\mathtt{n})\}, \emptyset\rangle,\\
&\langle\{\neg?\mathtt{0}(\mathtt{n}), ?\mathtt{0}(\mathtt{m})\}, \emptyset\rangle,\\
&\langle\{\neg?\mathtt{0}(\mathtt{n}), \neg?\mathtt{0}(\mathtt{m})\}, \{\{\mathtt{n}/\mathtt{pred}(\mathtt{n}), \mathtt{m}/\mathtt{pred}(\mathtt{m})\}\}\rangle\}
\end{aligned}
$$

$$
\begin{aligned}
\mathit{IndAx}_{\mathtt{g(n,m)>0},R} = &\forall \mathtt{n}, \mathtt{m} : \mathbb{N}\ ?\mathtt{0}(\mathtt{n}) \Rightarrow \mathtt{g}(\mathtt{n}, \mathtt{m}) > \mathtt{0}\\
&\wedge \forall \mathtt{n}, \mathtt{m} : \mathbb{N}\ \neg?\mathtt{0}(\mathtt{n}) \wedge ?\mathtt{0}(\mathtt{m}) \Rightarrow \mathtt{g}(\mathtt{n}, \mathtt{m}) > \mathtt{0}\\
&\wedge \forall \mathtt{n}, \mathtt{m} : \mathbb{N}\ \neg?\mathtt{0}(\mathtt{n}) \wedge \neg?\mathtt{0}(\mathtt{m}) \wedge \mathtt{g}(\mathtt{pred}(\mathtt{n}), \mathtt{pred}(\mathtt{m})) > \mathtt{0} \Rightarrow \mathtt{g}(\mathtt{n}, \mathtt{m}) > \mathtt{0}\\
&\Rightarrow \forall \mathtt{n}, \mathtt{m} : \mathbb{N}\ \mathtt{g}(\mathtt{n}, \mathtt{m}) > \mathtt{0}
\end{aligned}
$$

- Da in jedem Schritt sowohl m als auch n kleiner werden, ist nach spätestens $\min(m, n)$ Schritten ein Basisfall erreicht, in dem $n = 0$ oder $m = 0$ gilt.

3. •

$$
\begin{aligned}
R_\mathtt{h} = \{&\langle\{?\phi(\mathtt{k})\}, \emptyset\rangle,\\
&\langle\{\neg?\phi(\mathtt{k}), ?\phi(\mathtt{tl}(\mathtt{k}))\}, \emptyset\rangle,\\
&\langle\{\neg?\phi(\mathtt{k}), \neg?\phi(\mathtt{tl}(\mathtt{k})), \mathtt{hd}(\mathtt{k}) > \mathtt{hd}(\mathtt{tl}(\mathtt{k}))\}, \{\{\mathtt{k}/\mathtt{tl}(\mathtt{k})\}\}\rangle,\\
&\langle\{\neg?\phi(\mathtt{k}), \neg?\phi(\mathtt{tl}(\mathtt{k})), \neg\mathtt{hd}(\mathtt{k}) > \mathtt{hd}(\mathtt{tl}(\mathtt{k}))\}, \{\{\mathtt{k}/\mathtt{hd}(\mathtt{k}) :: \mathtt{tl}(\mathtt{tl}(\mathtt{k}))\}\}\rangle\}
\end{aligned}
$$

$$
\begin{aligned}
\mathit{IndAx}_{\mathtt{h(n)>0},R} = &\forall \mathtt{k} : \mathtt{list[nat]}\ ?\phi(\mathtt{k}) \Rightarrow \mathtt{h}(\mathtt{k}) > \mathtt{0}\\
&\wedge \forall \mathtt{k} : \mathtt{list[nat]}\ \neg?\phi(\mathtt{k}) \wedge ?\phi(\mathtt{tl}(\mathtt{k})) \Rightarrow \mathtt{h}(\mathtt{k}) > \mathtt{0}\\
&\wedge \forall \mathtt{k} : \mathtt{list[nat]}\ \neg?\phi(\mathtt{k}) \wedge \neg?\phi(\mathtt{tl}(\mathtt{k})) \wedge \mathtt{hd}(\mathtt{k}) > \mathtt{hd}(\mathtt{tl}(\mathtt{k}))\\
&\qquad\qquad \wedge \mathtt{h}(\mathtt{tl}(\mathtt{k})) > \mathtt{0} \Rightarrow \mathtt{h}(\mathtt{k}) > \mathtt{0}\\
&\wedge \forall \mathtt{k} : \mathtt{list[nat]}\ \neg?\phi(\mathtt{k}) \wedge \neg?\phi(\mathtt{tl}(\mathtt{k})) \wedge \neg\mathtt{hd}(\mathtt{k}) > \mathtt{hd}(\mathtt{tl}(\mathtt{k}))\\
&\qquad\qquad \wedge \mathtt{h}(\mathtt{hd}(\mathtt{k}) :: \mathtt{tl}(\mathtt{tl}(\mathtt{k}))) > \mathtt{0} \Rightarrow \mathtt{h}(\mathtt{k}) > \mathtt{0}\\
&\Rightarrow \forall \mathtt{k} : \mathtt{list[nat]}\ \mathtt{h}(\mathtt{k}) > \mathtt{0}
\end{aligned}
$$

- In jedem Schritt wird die Länge der Liste kleiner, nach endlich vielen Schritten ist also ein Basisfall in Form einer Liste mit Länge 0 oder 1 erreicht.