Formale Grundlagen der Informatik 3

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

Lösungsvorschlag zu Übung 7

Version 1 vom 10.02.2011

Aufgabe 7.1 (Quer durch Kapitel 11 und 12)

Hinweis: Es ist immer nur eine Antwortmöglichkeit richtig.

(a) Eine $\mathcal{S}$-Signatur ist sensibel gdw. ...

- ☐ ... die Menge der Variablensymbol der Sorte s nicht leer ist für alle $s \in \mathcal{S}$.
- ☐ ... die Menge der Grundterme der Sorte s nicht leer ist für alle $s \in \mathcal{S}$.
- ☐ ... die Menge der Variablensymbol der Sorte s leer ist für alle $s \in \mathcal{S}$.

Lösungsvorschlag

- ☒ ... die Menge der Grundterme der Sorte s nicht leer ist für alle $s \in \mathcal{S}$.

siehe Kapitel 11, Folie 4, Definition 3

(b) Mit Σ-Algebren ...

- ☐ ... können Lemmata bewiesen oder widerlegt werden.
- ☐ ... können Stuck-Terme interpretiert werden.
- ☐ ... bekommen die Worte aus $\mathcal{T}(\Sigma)$ eine Bedeutung.

Lösungsvorschlag

- ☒ ... bekommen die Worte aus $\mathcal{T}(\Sigma)$ eine Bedeutung.

siehe Kapitel 11, Folie 9

(c) Eine Σ-Interpretation besteht aus ...

- ☐ ... einer Σ-Algebra sowie einer A-Variablenbelegung.
- ☐ ... einer $\mathcal{S}$-Signatur sowie einer A-Variablenbelegung.
- ☐ ... einer Σ-Algebra sowie einer $\mathcal{S}$-Signatur

Lösungsvorschlag

- ☒ ... einer Σ-Algebra sowie einer A-Variablenbelegung.

siehe Kapitel 11, Folie 16, Definition 8

(d) Die Trägermenge der Standardalgebra $\mathcal{M}_\mathcal{P}$ eines terminierenden $\mathcal{L}$-Programms $\mathcal{P}$ ist ...

- ☐ ... die Menge der Sortensymbole $\mathcal{S}$.
- ☐ ... die Menge der Konstruktorgrundterme $\mathcal{C}(P)$.
- ☐ ... die Menge der Axiome $AX_\mathcal{P}$.

Lösungsvorschlag

- ☒ ... die Menge der Konstruktorgrundterme $\mathcal{C}(P)$.

siehe Kapitel 12, Folie 5 / 6

(e) Die Sprache $\mathcal{L}^-$ ist definiert wie $\mathcal{L}$ jedoch ...

- ☐ ... ohne Stuck-Terme.
- ☐ ... ohne partiell definierte Prozeduren.
- ☐ ... ohne polymorphe Datentypen.

Lösungsvorschlag

- ☒ ... ohne polymorphe Datentypen.

siehe Kapitel 12, Folie 3

Aufgabe 7.2 (Substitutionslemma)

Seien A eine Σ-Algebra, $\mathfrak{a}$ eine A-Variablenbelegung, $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$ eine Substitution und $t \in \mathcal{T}(\Sigma, \mathcal{V})$. Zeigen Sie, dass dann gilt:

$$\mathfrak{a}(\sigma(t)) = \mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](t)$$

Lösungsvorschlag

Der Beweis erfolgt durch Induktion über die Termstruktur.

- $t \in \mathcal{V}$: Falls $t = x_i \in \{x_1, \ldots, x_n\}$, dann ist

  $$\mathfrak{a}(\sigma(t)) = \mathfrak{a}(t_i) = \mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](x_i) = \mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](t).$$

  Andernfalls ist $\mathfrak{a}(\sigma(t)) = \mathfrak{a}(t) = \mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](t)$.

- $t = f(s_1, \ldots, s_n)$:

$$\begin{aligned}
\mathfrak{a}(\sigma(t)) &= \mathfrak{a}(f(\sigma(s_1), \ldots, \sigma(s_n))) \\
&= \alpha_f(\mathfrak{a}(\sigma(s_1)), \ldots, \mathfrak{a}(\sigma(s_n))) \\
&\underset{IH}{=} \alpha_f\big(\mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](s_1), \ldots, \mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](s_n)\big) \\
&= \mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](f(s_1, \ldots, s_n)) \\
&= \mathfrak{a}\big[x_1/\mathfrak{a}(t_1), \ldots, x_n/\mathfrak{a}(t_n)\big](t)
\end{aligned}$$

Aufgabe 7.3 (Theorie einer Σ-Algebra)

Sei $\mathcal{S} := \{s\}, \Sigma_s := \{c\}, \Sigma_{s,s} := \{f, g\}, \Sigma_{s,s,s} := \{h\}$ und $A = (\mathcal{A}, \alpha)$ definiert durch
$\mathcal{A}_s = \mathbb{Z}$
$\alpha_c := 0, \quad \alpha_f(n) := n + 2, \quad \alpha_g(n) := n - 1, \quad \alpha_h(n, m) := 2n + 2m + 1$

Zeigen Sie, dass ϕ_i in der Theorie der Algebra A ist d. h. $A \models \phi_i$:

(a) $\phi_1 := \forall x : s.\ g(g(f(x))) \equiv x$

Lösungsvorschlag

Sei $\mathfrak{a}$ eine A-Variablenbelegung. Es ist zu zeigen, dass $\alpha_g(\alpha_g(\alpha_f(\mathfrak{a}(x)))) = \mathfrak{a}(x)$. Es gilt offensichtlich $\alpha_g(\alpha_g(\alpha_f(\mathfrak{a}(x)))) = \mathfrak{a}(x) + 2 - 1 - 1 = \mathfrak{a}(x)$. Somit gilt $A \models \phi_1$.

(b) $\phi_2 := \forall x, y : s.\ h(x, y) \equiv h(y, x)$

Lösungsvorschlag

Sei $\mathfrak{a}$ eine A-Variablenbelegung. Es ist zu zeigen, dass $\alpha_h(\mathfrak{a}(x), \mathfrak{a}(y)) = \alpha_h(\mathfrak{a}(y), \mathfrak{a}(x))$. Es gilt offensichtlich $2\mathfrak{a}(x) + 2\mathfrak{a}(y) + 1 = 2\mathfrak{a}(y) + 2\mathfrak{a}(x) + 1$, da die Addition kommutativ ist. Somit gilt $A \models \phi_2$.

(c) $\phi_3 := \forall x, y : s.\ \neg h(x, y) \equiv c$

Lösungsvorschlag

Sei $\mathfrak{a}$ eine A-Variablenbelegung. Es ist zu zeigen, dass $\neg\alpha_h(\mathfrak{a}(x), \mathfrak{a}(y)) = 0$. Es gilt $\alpha_h(\mathfrak{a}(x), \mathfrak{a}(y)) = 2\mathfrak{a}(x) + 2\mathfrak{a}(y) + 1$. Da für alle beliebigen ganzen Zahl a und b offensichtlich gilt, dass $2a + 2b + 1$ eine ungerade Zahl und somit insbesondere ungleich 0 ist, gilt $A \models \phi_3$.

Aufgabe 7.4 (Kalküle)

(a) Geben Sie einen geeigneten Kalkül an, der die Länge eines Wortes $w \in \Sigma^*$ berechnet.

Lösungsvorschlag

Formale Sprache: $\Sigma^* \times \mathbb{N}$
Regeln:

$$\frac{b\beta, n}{\beta, n + 1}, b \in \Sigma$$

Herleitung: Eine Herleitung zu einem Wort $w \in \Sigma^*$ ist eine Sequenz von Paaren aus $\Sigma^* \times \mathbb{N}$ beginnend mit $(w, 0)$, sodass jedes Paar aus dem vorherigen durch Anwendung der Regel hervorgeht und auf das letzte Paar keine Regel mehr anwendbar ist.
Semantik: Endet eine Herleitung zu w in (ϵ, n), so gibt n die Länge des Wortes w an.

(b) Berechnen Sie mit Hilfe Ihres Kalküls die Länge der folgenden Wörter aus $\{a, b, c\}^*$:

- cab
- ϵ

Lösungsvorschlag

- Das Wort *cab* hat die Länge 3, wie die folgende Herleitung zeigt:

$$\dfrac{\dfrac{\dfrac{(cab, 0)}{(ab, 1)}}{(b, 2)}}{(\epsilon, 3)}$$

- Das Wort ϵ hat die Länge 0, wie die folgende Herleitung zeigt:

$$(\epsilon, 0)$$

Aufgabe 7.5 (Matching)

Bestimmen Sie den jeweils minimalen Matcher für die folgenden Matchingprobleme, falls ein Matcher existiert. Geben Sie dazu jeweils eine Herleitung im Matchingkalkül an, aus der dieser Matcher hervorgeht. Existiert kein Matcher, geben Sie **eine** scheiternde Herleitung an.
Geben Sie in jeden Schritt die verwendete Regel an.

(a) Pattern: $t_a = f(g(x, y), h(g(y, x)), x)$, Target: $q_a = f(g(h(a), b), h(g(b, h(a))), h(a))$

Lösungsvorschlag

Für $\sigma_a = \{x/h(a), y/b\}$ ist $\sigma_a(t_a) = q_a$, denn

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\{f(g(x,y),h(g(y,x)),x) \doteq f(g(h(a),b),h(g(b,h(a))),h(a))\},\emptyset)}{(\{g(x,y) \doteq g(h(a),b),\ h(g(y,x)) \doteq h(g(b,h(a))),\ x \doteq h(a)\},\emptyset)}\text{ Decompose}}{(\{y \doteq b,\ h(g(y,x)) \doteq h(g(b,h(a))),\ x \doteq h(a)\},\emptyset)}\text{ Decompose}}{(\{h(g(b,x)) \doteq h(g(b,h(a))),\ x \doteq h(a)\},\{y/b\})}\text{ Solve}}{(\{h(g(b,h(a))) \doteq h(g(b,h(a)))\},\{x/h(a),\ y/b\})}\text{ Solve}}{(\emptyset,\{x/h(a),\ y/b\})}\text{ Eliminate}$$

(b) Pattern: $t_b = f(g(x, y), x)$, Target: $q_b = f(g(a, b), b)$

Lösungsvorschlag

Es gibt keinen Matcher, denn keine Herleitung endet in $(\emptyset, \sigma)$.
Eine scheiternde Herleitung ist z. B.:

$$\dfrac{\dfrac{\dfrac{\dfrac{(\{f(g(x,y),x) \doteq f(g(a,b),b)\},\emptyset)}{(\{g(x,y) \doteq g(a,b),\ x \doteq b\},\emptyset)}\text{ Decompose}}{(\{x \doteq a,\ y \doteq b,\ x \doteq b\},\emptyset)}\text{ Decompose}}{(\{y \doteq b,\ a \doteq b\},\{x/a\})}\text{ Solve}}{(\{a \doteq b\},\{x/a,\ y/b\})}\text{ Solve}$$

Aufgabe 7.6 (Fundierte Mengen)

Beweisen oder widerlegen Sie die Fundiertheit der folgenden Mengen:

(a) $(\mathbb{N} \times \mathbb{N}, \succ_a)$ mit $(m_1, n_1) \succ_a (m_2, n_2)$ genau dann, wenn $m_1 > m_2$ oder $n_1 > n_2$

Lösungsvorschlag

Die Menge ist nicht fundiert: Mit $m_1 := (1, 0)$ und $m_2 := (0, 1)$ erhält man die unendlich absteigende Kette $m_1 \succ_a m_2 \succ_a m_1 \succ_a m_2 \succ_a ....$

(b) $(\mathbb{N} \times \mathbb{N}, \succ_a)$ mit $(m_1, n_1) \succ_a (m_2, n_2)$ genau dann, wenn $m_1 > m_2$ und $n_1 > n_2$

Lösungsvorschlag

Die Menge ist fundiert. In jedem Schritt werden beide Elemente des Tupels kleiner. Somit ist nach spätestens $\min(m, n)$ Schritten ein Element des Tupels Null. Dann kann kein Nachfolger mehr gefunden werden (vgl. Menge der minimalen Elemente aus voriger Aufgabe).

Aufgabe 7.7 (Relationenbeschreibungen und Induktionsaxiome)

(a) Geben Sie für den folgenden Datentyp die Relationenbeschreibung $R_{S[@A]}$ an.

```
structure S[@A] <=
  null(value : ℕ),
  first(this : @A, that : S[@A]),
  second(left : S[@A], middle : S[@A], right : S[@A])
```

Lösungsvorschlag

$R_{S[@A]} = \{$
$\langle \{?\texttt{null}(u)\}, \emptyset \rangle,$
$\langle \{?\texttt{first}(u)\}, \{\{u/\texttt{that}(u)\}\} \rangle,$
$\langle \{?\texttt{second}(u)\}, \{\{u/\texttt{left}(u)\}, \{u/\texttt{middle}(u)\}, \{u/\texttt{right}(u)\}\} \rangle \}$

(b) Betrachten Sie die folgenden Prozeduren p:

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

Hierbei sei + folgendermaßen definiert:

```
function [infixr, 10] +(m : ℕ, n : ℕ) : ℕ <=
  if ?0(m)
    then n
    else ⁺(⁻(m) + n)
  end_if
```

2.
```
function g(m : ℕ, n : ℕ) : list[ℕ] <=
  if ?0(m)
    then 0 :: ∅
    else if ?0(n)
           then ∅
           else m :: g(⁻(m), ⁻(n))
    end_if
  end_if
```

- Geben Sie zu jeder Prozedur p die zusammengesetzte Relationenbeschreibung R_p an.

- Geben Sie zu jeder Prozedur p das Induktionsaxiom $IndAx_{p(x,y)=p(^+(x),y),R_p}$ an.

Lösungsvorschlag

1. • $R_{\mathtt{f}} = \{$
   $\langle\{\mathtt{?0}(n)\},\emptyset\rangle,$
   $\langle\{\neg\mathtt{?0}(n)\},\{\{m/m, n/^-(n)\}\}\rangle\}$

   $IndAx_{\mathtt{f}(x,y)=\mathtt{f}(^+(x),y),R_{\mathtt{f}}} = \forall x,y:\mathbb{N}\ \mathtt{?0}(y) \Rightarrow \mathtt{f}(x,y) = \mathtt{f}(^+(x),y)$
   $\wedge\ \forall x,y:\mathbb{N}\ \neg\mathtt{?0}(y) \wedge \mathtt{f}(x,^-(y)) = \mathtt{f}(^+(x),^-(y)) \Rightarrow \mathtt{f}(x,y) = \mathtt{f}(^+(x),y)$
   $\Rightarrow \forall x,y:\mathbb{N}\ \mathtt{f}(x,y) = \mathtt{f}(^+(x),y)$

2. • $R_{\mathtt{g}} = \{$
   $\langle\{\mathtt{?0}(m)\},\emptyset\rangle,$
   $\langle\{\neg\mathtt{?0}(m),\mathtt{?0}(n)\},\emptyset\rangle,$
   $\langle\{\neg\mathtt{?0}(m),\neg\mathtt{?0}(n)\},\{\{m/^-(m),n/^-(n)\}\}\rangle\}$

   $IndAx_{\mathtt{g}(x,y)=\mathtt{g}(^+(x),y),R_{\mathtt{g}}} = \forall x,y:\mathbb{N}\ \mathtt{?0}(x) \Rightarrow \mathtt{g}(x,y) = \mathtt{g}(^+(x),y)$
   $\wedge\ \forall x,y:\mathbb{N}\ \neg\mathtt{?0}(x) \wedge \mathtt{?0}(y) \Rightarrow \mathtt{g}(x,y) = \mathtt{g}(^+(x),y)$
   $\wedge\ \forall x,y:\mathbb{N}\ \neg\mathtt{?0}(x) \wedge \neg\mathtt{?0}(y) \wedge \mathtt{g}(^-(x),^-(y)) = \mathtt{g}(^+(^-(x)),^-(y)) \Rightarrow \mathtt{g}(x,y) = \mathtt{g}(^+(x),y)$
   $\Rightarrow \forall x,y:\mathbb{N}\ \mathtt{g}(x,y) = \mathtt{g}(^+(x),y)$

Aufgabe 7.8 (Berechnungskalkül)

Betrachten Sie das Programm P mit folgender Prozedurdefinition:

```
function a(x : ℕ, y : ℕ) : ℕ <=
if ?0(x)
  then y
  else if ?0(y)
         then x
         else +(a(-(y), -(x)))
       end_if
end_if
```

Bestimmen den Wert von $eval_P(\mathtt{a}(5,1))$, indem Sie eine Herleitung im Berechnungskalkül angeben. Geben Sie dabei in jedem Schritt die verwendeten Regeln an.

Lösungsvorschlag

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathtt{a}(5,1)}{\mathtt{if}\{\mathtt{?0}(5),1,\mathtt{if}\{\mathtt{?0}(1),5,{}^+(\mathtt{a}(^-(1),^-(5)))\}\}}\,(19)}{\mathtt{if}\{\mathtt{false},1,\mathtt{if}\{\mathtt{?0}(1),5,{}^+(\mathtt{a}(^-(1),^-(5)))\}\}}\,(8),\,(4)}{\mathtt{if}\{\mathtt{?0}(1),5,{}^+(\mathtt{a}(^-(1),^-(5)))\}}\,(10)}{\mathtt{if}\{\mathtt{false},5,{}^+(\mathtt{a}(^-(1),^-(5)))\}}\,(8),\,(4)}{{}^+(\mathtt{a}(^-(1),^-(5)))}\,(10)}{{}^+(\mathtt{a}(0,^-(5)))}\,(18),\,(18),\,(5)}{{}^+(\mathtt{a}(0,4))}\,(18),\,(19)}{{}^+(\mathtt{if}\{\mathtt{?0}(0),4,\mathtt{if}\{\mathtt{?0}(4),0,{}^+(\mathtt{a}(^-(4),^-(0)))\}\})}\,(18),\,(8),\,(3)}{{}^+(\mathtt{if}\{\mathtt{true},4,\mathtt{if}\{\mathtt{?0}(4),0,{}^+(\mathtt{a}(^-(4),^-(0)))\}\})}\,(18),\,(9)}{5}$$

Aufgabe 7.9 (Terminierung)

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

(a) Bestimmen Sie geeignete Maßterme für den Terminierungsbeweis. Überlegen Sie sich dazu, was bei den rekursiven Aufrufen kleiner wird. Für in den Maßtermen verwendete Hilfsprozeduren geben Sie deren Definitionen an oder verweisen Sie auf deren Definitionen im Vorlesungskript oder bisherigen Übungen.

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

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

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

```
structure bool <=
  true,
  false

structure ℕ <=
  0,
  ⁺(⁻ : ℕ)

function f(x : ℕ, y : ℕ, z : ℕ) : ℕ <=
  if x > z
    then f(⁺(z), ⁺(y), x)
    else if z > x
           then z
           else if ?0(y)
                  then x
                  else f(⁺(x), ⁻(y), ⁺(z))
                end_if
         end_if
  end_if
```

Lösungsvorschlag

(a) Wir wählen die Maßterme `diff(x, z)` und `y` mit der folgenden Prozedurdefinition:

```
function diff(x : ℕ, y : ℕ) : ℕ <=
  if ?0(x)
    then y
    else if ?0(y)
           then x
           else diff(⁻(x), ⁻(y))
         end_if
  end_if
```

(b) $R_{\mathtt{f}} = \{$
$\langle\{x > z\}, \{\{x/^{+}(z), y/^{+}(y), z/x\}\}\rangle,$
$\langle\{\neg x > z, z > x\}, \emptyset\rangle,$
$\langle\{\neg x > z, \neg z > x, \mathtt{?0}(y)\}, \emptyset\rangle,$
$\langle\{\neg x > z, \neg z > x, \neg\mathtt{?0}(y)\}, \{\{x/^{+}(x), y/^{-}(y), z/^{+}(z)\}\}\rangle\}$

(c) $th_1 = \forall x, y, z : \mathbb{N}$ $\texttt{if}\{x > z,$
$\texttt{if}\{\texttt{diff}(x, z) > \texttt{diff}(^+(z), x),$
$\texttt{true},$
$\texttt{if}\{\texttt{diff}(x, z) = \texttt{diff}(^+(z), x), y > {}^+(y), \texttt{false}\}\},$
$\texttt{true}\}$

$th_2 = \forall x, y, z : \mathbb{N}$ $\texttt{if}\{\neg x > z,$
$\texttt{if}\{\neg z > x,$
$\texttt{if}\{\neg\texttt{?0}(y),$
$\texttt{if}\{\texttt{diff}(x, z) > \texttt{diff}(^+(x), {}^+(z)),$
$\texttt{true},$
$\texttt{if}\{\texttt{diff}(x, z) = \texttt{diff}(^+(x), {}^+(z)), y > {}^-(y), \texttt{false}\}\},$
$\texttt{true}\},$
$\texttt{true}\},$
$\texttt{true}\}$

(d) Wir deuten die Terme als natürliche Zahlen. `diff` berechnet den Abstand zweier Zahlen zu einander. Da dies von der Reihenfolge der Argumente nicht abhängt, gilt $\forall x, y : \mathbb{N}.\ \texttt{diff}(x, y) = \texttt{diff}(y, x)$.

Da in th_1 die Bedingung $x > z$ gilt, lässt sich $\texttt{diff}(x, z) > \texttt{diff}(^+(z), x)$ als arithmetische Gleichung $x - z > x - (z+1)$ ausdrücken, welche offensichtlich wahr ist. Deshalb gilt auch $\texttt{diff}(x, z) > \texttt{diff}(^+(z), x)$ und th_1 ist wahr.

Da in th_2 die Bedingungen $\neg x > z$ und $\neg z > x$ gelten, gilt $x = z$. Somit ist sowohl $\texttt{diff}(x, z) = 0$ als auch $\texttt{diff}(^+(x), {}^+(z)) = 0$. Es gilt daher $\texttt{diff}(x, z) = \texttt{diff}(^+(x), {}^+(z))$.
Zudem gilt die Bedingung $\neg\texttt{?0}(y)$, also ist $y > 0$. $y > {}^-(y)$ lässt sich als arithmetische Gleichung $y > y - 1$ ausdrücken, welche offensichtlich wahr ist für alle $y > 0$.
Somit ist th_2 wahr.

Aufgabe 7.10 (Minimale Elemente und Vorgänger)

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

(a) $(\mathbb{N} \times \mathbb{N}, \succ_a)$ mit $(m_1, n_1) \succ_a (m_2, n_2)$ genau dann, wenn $m_1 > m_2$ und $n_1 > n_2$
Hinweis: $>$ bezeichnet die übliche (transitive) Ordnung auf den natürlichen Zahlen

Lösungsvorschlag

$min_{\succ_a}(\mathbb{N} \times \mathbb{N}) = \{(m, n) | m = 0 \vee n = 0\}$

$$|pre_{\succ_a}((m, n))| = \begin{cases} 0 \text{ , falls } m \in min_{\succ_a}(\mathbb{N} \times \mathbb{N}) \\ m \cdot n \text{ , sonst} \end{cases}$$

(b) $(C_{\texttt{list[}\mathbb{N}\texttt{]}}, \succ_b)$ mit $k \succ_b l$ genau dann, wenn $\texttt{but\_last}(k) = \texttt{but\_last}(l)$ und $k \neq \emptyset$ und $l \neq \emptyset$ und $\texttt{last}(k) > \texttt{last}(l)$
Hinweise:

- die Funktion $\texttt{but\_last}(k)$ schneidet das letzte Element einer Liste ab (siehe Übung 2 Aufgabe 2.3)
- die Funktion $\texttt{last}(k)$ gibt das letzte Element einer Liste zurück (siehe Kapitel 5, Folie 19)

Lösungsvorschlag

$$min_{\succ_b}(\mathbb{N}) = \{k \in C_{\texttt{list[}\mathbb{N}\texttt{]}} | k = \emptyset \vee last(k) = 0\}$$
$$|pre_{\succ_b}(m)| = \begin{cases} 0 \text{ , falls } m \in min_{\succ_b}(\mathbb{N}) \\ \texttt{last}(k) \text{ , sonst} \end{cases}$$

Aufgabe 7.11 (Induktion)

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

```
structure bool <=
        true,
        false

structure ℕ <=
        0,
        +(⁻ : ℕ)

function [infixr, 10] +(m : ℕ, n : ℕ) : ℕ <=
  if ?0(m)
    then n
    else +(⁻(m) + n)
  end_if

function f(m : ℕ, n : ℕ) : ℕ <=
  if ?0(n)
    then 0
    else m + f(m, ⁻(n))
  end_if

function zero(x : ℕ) : ℕ <=
  if ?0(x)
    then 0
    else zero(pred(x))
  end_if

lemma null <= ∀ x : ℕ
        f(0, x) = zero(x)
```

Beweisen Sie $AX_{\texttt{null}}$ durch Induktion über x mittels der Relationenbeschreibung $R_{\mathbb{N}}$.

Gehen Sie dazu wie folgt vor:

(a) Geben Sie die Menge AX_p der Axiome zum Programm P an.

Lösungsvorschlag

$$AX_p = AX_{\texttt{bool}} \cup AX_{\mathbb{N}} \cup \{AX_{\texttt{+}}\} \cup \{AX_{\texttt{f}}\} \cup \{AX_{\texttt{zero}}\}$$

$$\begin{aligned}
AX_{\texttt{bool}} = \{\ & \forall x, y : \texttt{bool}\ \texttt{if}_{\texttt{bool}}\{\texttt{true}, x, y\} \equiv x && (1)\\
& \forall x, y : \texttt{bool}\ \texttt{if}_{\texttt{bool}}\{\texttt{false}, x, y\} \equiv y\ \} && (2)
\end{aligned}$$

$$\begin{aligned}
AX_{\mathbb{N}} = \{\ & \texttt{eq}_{\mathbb{N}}(0,0) \equiv \texttt{true} && (3)\\
& \forall x : \mathbb{N}\ {}^{-}({}^{+}(x)) \equiv x && (4)\\
& \forall x, y : \mathbb{N}\ \texttt{eq}_{\mathbb{N}}({}^{+}(x), {}^{+}(y)) \equiv eq_{\mathbb{N}}(x, y) && (5)\\
& \forall x : \mathbb{N}\ \texttt{eq}_{\mathbb{N}}(0, {}^{+}(x)) \equiv \texttt{false} && (6)\\
& \forall x : \mathbb{N}\ \texttt{eq}_{\mathbb{N}}({}^{+}(x), 0) \equiv \texttt{false} && (7)\\
& \forall x, y : \mathbb{N}\ \texttt{if}_{\mathbb{N}}\{\texttt{true}, x, y\} \equiv x && (8)\\
& \forall x, y : \mathbb{N}\ \texttt{if}_{\mathbb{N}}\{\texttt{false}, x, y\} \equiv y && (9)\\
& \forall x : \mathbb{N}\ \texttt{?0}(x) \equiv \texttt{eq}_{\mathbb{N}}(0, x) && (10)\\
& \forall x : \mathbb{N}\ \texttt{?}^{+}(x) \equiv \texttt{eq}_{\mathbb{N}}(x, {}^{+}({}^{-}(x)))\ \} && (11)
\end{aligned}$$

$$\begin{aligned}
AX_{\texttt{+}} = &\ \forall m, n : \mathbb{N}\ m\ \texttt{+}\ n \equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(m), n, {}^{+}({}^{-}(m)\ \texttt{+}\ n)\} && (12)\\
AX_{\texttt{f}} = &\ \forall m, n : \mathbb{N}\ \texttt{f}(m, n) \equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(n), 0, m\ \texttt{+}\ \texttt{f}(m, {}^{-}(n))\} && (13)\\
AX_{\texttt{zero}} = &\ \forall x : \mathbb{N}\ \texttt{zero}(x) \equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(x), 0, \texttt{zero}({}^{-}(x))\} && (14)
\end{aligned}$$

(b) Bilden Sie die Induktionsformeln (nach Kapitel 6, Folie 19f.) in Form von HPL-Sequenzen seq_{I_i} für den Rumpf b des Lemmas `null` und eine geeignete Umbenennung $R'_{\mathbb{N}}$ von $R_{\mathbb{N}}$.

Lösungsvorschlag

$seq_{I_1} = \langle \{\texttt{?0}(x)\}, \emptyset \Vdash \texttt{f}(0, x) = \texttt{zero}(x) \rangle$
$seq_{I_2} = \langle \{\texttt{?}^{+}(x)\}, \{\texttt{f}(0, {}^{-}(x)) = \texttt{zero}({}^{-}(x))\} \Vdash \texttt{f}(0, x) = \texttt{zero}(x) \rangle$

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

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

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

Lösungsvorschlag

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

Mit $\mathcal{E}_P$ ist $\texttt{f}(0, x) = \texttt{zero}(x) \equiv \texttt{true} \leftrightarrow \texttt{f}(0, x) \equiv \texttt{zero}(x)$. Es reicht also, jeweils zu zeigen:

$\texttt{f}(0, x) \equiv \texttt{zero}(x)$

- $\texttt{?0}(x) \equiv \texttt{true} \to \texttt{f}(0, x) \equiv \texttt{zero}(x)$

$$\begin{aligned}
\texttt{f}(0,x) &\equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(x), 0, 0 \texttt{ + } \texttt{f}(0, {}^{-}(x))\} && (13)\\
&\equiv \texttt{if}_{\mathbb{N}}\{\texttt{true}, 0, 0 \texttt{ + } \texttt{f}(0, {}^{-}(x))\} && (H_1)\\
&\equiv 0 && (8)
\end{aligned}$$

$$\begin{aligned}
\texttt{zero}(x) &\equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(x), 0, \texttt{zero}({}^{-}(x))\} && (14)\\
&\equiv \texttt{if}_{\mathbb{N}}\{\texttt{true}, 0, \texttt{zero}({}^{-}(x))\} && (H_1)\\
&\equiv 0 && (8)
\end{aligned}$$

Also gilt $AX_p \cup \mathcal{E}_P \models \forall x : \mathbb{N}\ \texttt{?0}(x) \equiv \texttt{true} \to \texttt{f}(0, x) \equiv \texttt{zero}(x)$.

- $\texttt{?}^{+}(x) \equiv \texttt{true} \wedge \texttt{f}(0, {}^{-}(x)) = \texttt{zero}({}^{-}(x)) \equiv \texttt{true} \to \texttt{f}(0, x) \equiv \texttt{zero}(x)$

Zunächst formen wir die Induktionshypothese mittels $\mathcal{E}_P$ zu einer geeigneteren Gleichung um: $\texttt{f}(0, {}^{-}(x)) \equiv \texttt{zero}({}^{-}(x))$ (‡)

Außerdem müssen wir aus der Hypothese $\texttt{?}^{+}(x) \equiv \texttt{true}$ eine geeignetere Gleichung herleiten:

$$\begin{aligned}
\texttt{?}^{+}(x) \equiv \texttt{true} &\underset{(11)}{\Leftrightarrow} x = {}^{+}({}^{-}(x)) \equiv \texttt{true}\\
&\underset{\mathcal{E}_P}{\Leftrightarrow} x \equiv {}^{+}({}^{-}(x)) && (11')
\end{aligned}$$

Aus $\texttt{?0}(x) \underset{(10)}{\equiv} x = \texttt{0} \underset{(11')}{\equiv} {}^{+}({}^{-}(x)) = \texttt{0} \underset{(7)}{\equiv} \texttt{false}$ folgt damit:

$$\texttt{?0}(x) \equiv \texttt{false} \qquad (\dagger)$$

$$\begin{aligned}
\texttt{f}(0,x) &\equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(x), 0, 0 \texttt{ + } \texttt{f}(0, {}^{-}(x))\} && (13)\\
&\equiv \texttt{if}_{\mathbb{N}}\{\texttt{false}, 0, 0 \texttt{ + } \texttt{f}(0, {}^{-}(x))\} && (\dagger)\\
&\equiv 0 \texttt{ + } \texttt{f}(0, {}^{-}(x)) && (9)\\
&\equiv 0 \texttt{ + } \texttt{zero}({}^{-}(x)) && (\ddagger)\\
&\equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(0), \texttt{zero}({}^{-}(x)), \ldots\} && (12)\\
&\equiv \texttt{if}_{\mathbb{N}}\{0 = 0, \texttt{zero}({}^{-}(x)), \ldots\} && (10)\\
&\equiv \texttt{if}_{\mathbb{N}}\{\texttt{true}, \texttt{zero}({}^{-}(x)), \ldots\} && (3)\\
&\equiv \texttt{zero}({}^{-}(x)) && (8)
\end{aligned}$$

$$\begin{aligned}
\texttt{zero}(x) &\equiv \texttt{if}_{\mathbb{N}}\{\texttt{?0}(x), 0, \texttt{zero}({}^{-}(x))\} && (14)\\
&\equiv \texttt{if}_{\mathbb{N}}\{\texttt{false}, 0, \texttt{zero}({}^{-}(x))\} && (\dagger)\\
&\equiv \texttt{zero}({}^{-}(x)) && (9)
\end{aligned}$$

Also gilt $AX_p \cup \mathcal{E}_P \models \forall x : \mathbb{N}\ \texttt{?}^{+}(x) \equiv \texttt{true} \wedge (\forall x : \mathbb{N}\ \texttt{f}(0, {}^{-}(x)) = \texttt{zero}({}^{-}(x)) \equiv \texttt{true}) \to \texttt{f}(0, x) \equiv \texttt{zero}(x)$.