Syntax und Semantik von Programmen 3

Modul 7 (v1.0)

Kanonikvorlesung: Foundations of Computing

Heiko Mantel

MAIS, TU Darmstadt, WS10/11

Motivation

Wie beweist man Aussagen über Programme formal?

- basierend auf der formal modellierten Syntax und Semantik
- Fortsetzung von Modul 6

Unterschiedliche Beweistechniken

- Fallunterscheidung (in Modul 6)
- Widerspruchsbeweis (in Modul 6)
- Strukturelle Induktion (in Modul 6)
- Induktion über Herleitungen (in diesem Modul)

Fokus dieses Moduls: Wie beweist man Eigenschaften von Programmiersprachen?

Übersicht: Modul 7

Termbeschreibungen von Herleitungen

Induktionsprinzip

- Induktion über Herleitungen

Deterministische Auswertung von Programmen

- Beweis mit Induktion über Herleitungen

Termbeschreibung von Regeln (1)

Definition

Ein **Regelterm** ist ein Ausdruck folgender Form:

$$\textbf{r-name}(\xi,(\xi_1,..,\xi_n))$$

wobei

- r-name — der Name der Regel,
- ξ — eine Grundinstanz eines Urteils ist und
- $(\xi_1,..,\xi_n)$ — eine endliche Liste von Grundinstanzen von Urteilen ist, die auch die leere Liste () sein kann

Intuition

Sei σ ein beliebiger Zustand. Dann entspricht der Regelterm

$$r+(\langle 5+3,\sigma\rangle\Downarrow 8, (\langle 5,\sigma\rangle\Downarrow 4, \langle 3,\sigma\rangle\Downarrow 4))$$

folgender Grundinstanz von r+:

$$\text{r+}\quad \frac{\langle 5,\sigma\rangle\Downarrow 4 \qquad \langle 3,\sigma\rangle\Downarrow 4}{\langle 5+3,\sigma\rangle \Downarrow 8} \quad 8 = 4+4$$

Termbeschreibung von Regeln (2)

Definition

Die durch eine Kalkülregel

$$\text{r-name}\ \frac{\zeta_1,\ \zeta_2,\ \dots,\ \zeta_n}{\zeta}\ \phi_1,\dots,\ \phi_m$$

repräsentierte Menge von Regeltermen ist definiert als

RTerme(r-name) = { r-name($\zeta\eta$,($\zeta_1\eta$,…,$\zeta_n\eta$))
| $\zeta\eta$,$\zeta_1\eta$,…,$\zeta_n\eta$ enthalten keine Metavariablen
und $\phi_1\eta$,…,$\phi_m\eta$ sind erfüllt }

Beispiel

Für die Kalkülregel r+ gilt zum Beispiel

- r+($\langle 5+3,\sigma\rangle \Downarrow 8$, ($\langle 5,\sigma\rangle \Downarrow 5$, $\langle 3,\sigma\rangle \Downarrow 3$)) $\in$ RTerme(r+)
- r+($\langle 5+3,\sigma\rangle \Downarrow 8$, ($\langle 5,\sigma\rangle \Downarrow 4$, $\langle 3,\sigma\rangle \Downarrow 4$)) $\in$ RTerme(r+)

aber

- r+($\langle 5+X,\sigma\rangle \Downarrow 8$, ($\langle 5,\sigma\rangle \Downarrow 5$, $\langle X,\sigma\rangle \Downarrow 3$)) $\notin$ RTerme(r+), da der Ausdruck 5+X eine Metavariable enthält.

Termbeschreibung von Herleitungen (1)

Definition

Sei ξ eine Instanz eines Urteils ζ. Die **Herleitungen von ξ in einem Kalkül $\mathcal{K}$** (kurz: **$\mathcal{K}$-Herleitung von ξ**) sind induktiv definiert.

- Eine $\mathcal{K}$–Herleitung von ξ ist ein Term der Form
  - **r-name(ξ,($\mathcal{H}_1$,…,$\mathcal{H}_n$))** ,

  wobei
  - es in $\mathcal{K}$ eine Regel folgender Form gibt:

$$\text{r-name} \quad \frac{\zeta_1, \zeta_2, \ldots, \zeta_n}{\zeta} \quad \phi_1,\ldots,\phi_m$$

  - und es eine Substitution η gibt, so dass
    - o $\xi=\zeta\eta$ und
    - o $\phi_1\eta$, … und $\phi_m\eta$ erfüllt sind
    - o ($\mathcal{H}_1$,…,$\mathcal{H}_n$) eine möglicherweise leere Liste von Herleitungen ist, so dass, für jedes $i\in\{1,..,n\}$, $\mathcal{H}_i$ eine Herleitung von $\zeta_i\eta$ ist.

Termbeschreibung von Herleitungen (2)

Definition

Seien $\xi, \xi_1, \ldots, \xi_k$ Instanzen von Urteilen $\zeta, \zeta_1, \ldots, \zeta_k$. Eine **Herleitung von ξ aus $\xi_1, \ldots, \xi_k$ in einem Kalkül $\mathcal{K}$** (kurz: **$\mathcal{K}$-Herleitung von ξ aus $\xi_1, \ldots, \xi_k$**) ist entweder

- der Term ξ, wobei $\xi \in \{\xi_1, \ldots, \xi_k\}$ gilt,

oder

- ein Term der Form **r-name(ξ,($\mathcal{H}_1,\ldots,\mathcal{H}_n$))**, wobei
  - es in $\mathcal{K}$ eine Regel folgender Form gibt:

$$\text{r-name} \quad \frac{\zeta_1, \zeta_2, \ldots, \zeta_n}{\zeta} \quad \phi_1, \ldots, \phi_m$$

  - und es eine Substitution η gibt, so dass
    - o $\xi = \zeta\eta$ und
    - o $\phi_1\eta$, … und $\phi_n\eta$ erfüllt sind
    - o ($\mathcal{H}_1,\ldots,\mathcal{H}_n$) eine möglicherweise leere Liste von Herleitungen ist, so dass, für jedes $i \in \{1,..,n\}$, $\mathcal{H}_i$ eine Herleitung von $\zeta_i\eta$ aus $\xi_1, \ldots, \xi_k$ ist.

Termbeschreibung von Herleitungen (3)

Notation

Wir schreiben

- $\mathcal{H} \Vdash_{\mathcal{K}} \xi$,

um auszudrücken, dass $\mathcal{H}$ eine $\mathcal{K}$-Herleitung von ξ ist, und

- $\Vdash_{\mathcal{K}} \xi$,

um auszudrücken, dass ξ eine $\mathcal{K}$-Herleitung hat. Wenn sich der Kalkül $\mathcal{K}$ aus dem Kontext ergibt, so schreiben wir auch

- $\mathcal{H} \Vdash \xi$ anstatt $\mathcal{H} \Vdash_{\mathcal{K}} \xi$ und
- $\Vdash \xi$ anstatt $\Vdash_{\mathcal{K}} \xi$.

Notation

Die Menge aller $\mathcal{K}$-Herleitungen von ξ wird mit $\mathbf{DER}_{\mathcal{K}}(\xi)$ bezeichnet. Ergibt sich $\mathcal{K}$ aus dem Kontext, so schreiben wir auch $\mathbf{DER}(\xi)$.

Notation

Die Menge aller $\mathcal{K}$-Herleitungen wird mit $\mathbf{DER}_{\mathcal{K}}$ bezeichnet.

Nachtrag zu Modul 5

Notation

Für die Kalküle aus Modul 5 führen wir folgende Bezeichner ein:

- $\mathcal{A}$: der Kalkül zur Herleitung von Instanzen von $\langle a,\sigma\rangle \Downarrow n$
- $\mathcal{B}$: der Kalkül zur Herleitung von Instanzen von $\langle b,\sigma\rangle \Downarrow t$
- $\mathcal{C}$: der Kalkül zur Herleitung von Instanzen von $\langle c,\sigma\rangle \rightarrow \sigma'$

Definition

Sei $\sigma\in\Sigma$ ein Zustand. Dann ist **$\sigma[x\backslash n]$** der Zustand, der der Programmvariablen x den Wert n und jeder anderen Programmvariablen y den Wert $\sigma(y)$ zuordnet.

Übersicht: Modul 7

Termbeschreibungen von Herleitungen

Induktionsprinzip

- Induktion über Herleitungen

Deterministische Auswertung von Programmen

- Beweis mit Induktion über Herleitungen

Induktion über Herleitungen

Unser Ziel

- ein Induktionsprinzip über Herleitungen

Vorgehen

- Definition einer wohlfundierten Relation $\prec$ über Herleitungen
- Instantiierung der wohlfundierten Induktion mit $\prec$

Definition

Die Herleitungen $\mathcal{H}_1,\ldots,\mathcal{H}_n$ sind die **direkten Teilherleitungen** einer Herleitung r-name(ξ,($\mathcal{H}_1,\ldots,\mathcal{H}_n$)).

Definition

Wir definieren $\prec$ als zweistellige Relation auf Herleitungen durch

- $\mathcal{H}_i \prec \mathcal{H}$ genau dann wenn $\mathcal{H}_i$ eine direkte Teilherleitung von $\mathcal{H}$ ist.

Somit haben wir ein Induktionsprinzip für Herleitungen!

Aber, wie sieht das Induktionsprinzip für einen Kalkül aus?

Induktion über Herleitungen in $\mathcal{T}$ (1)

Beweisprinzip der Induktion über Herleitungen in $\mathcal{T}$

Sei P eine einstellige Relation über der Menge aller Herleitungen in $\mathcal{T}$.

Wenn folgende Bedingungen gelten:

- $\forall \sigma \in \Sigma$: P(rsk($\langle$skip,$\sigma\rangle \to \sigma$, ()))
- $\forall \sigma \in \Sigma$: $\forall$x$\in$Loc: $\forall$a$\in$Aexp: $\forall$n$\in$N: $\forall \mathcal{H}1 \in \mathrm{DER}_{\mathcal{A}}(\langle a,\sigma\rangle \Downarrow n)$:
  P(r:=($\langle$x:=a,$\sigma\rangle \to \sigma$[x\n], ($\mathcal{H}$1))
- $\forall \sigma,\sigma',\sigma'' \in \Sigma$: $\forall$c1,c2$\in$Com:
  $\forall \mathcal{H}1 \in \mathrm{DER}_{\mathcal{T}}(\langle c1,\sigma\rangle \to \sigma'')$: $\forall \mathcal{H}2 \in \mathrm{DER}_{\mathcal{T}}(\langle c2,\sigma''\rangle \to \sigma')$:
  [(P($\mathcal{H}$1) $\wedge$ P($\mathcal{H}$2)) $\Rightarrow$ P(r;($\langle$c1;c2,$\sigma\rangle \to \sigma'$, ($\mathcal{H}$1, $\mathcal{H}$2)))]
- $\forall \sigma,\sigma' \in \Sigma$: $\forall$b$\in$Bexp: $\forall$c1,c2$\in$Com:
  $\forall \mathcal{H}1 \in \mathrm{DER}_{\mathcal{B}}(\langle b,\sigma\rangle \Downarrow true)$: $\forall \mathcal{H}2 \in \mathrm{DER}_{\mathcal{T}}(\langle c1,\sigma\rangle \to \sigma')$:
  [(P($\mathcal{H}$2)) $\Rightarrow$ P(rift($\langle$if b then c1 else c2 fi, $\sigma\rangle \to \sigma'$, ($\mathcal{H}$1, $\mathcal{H}$2)))]
- $\forall \sigma,\sigma' \in \Sigma$: $\forall$b$\in$Bexp: $\forall$c1,c2$\in$Com:
  $\forall \mathcal{H}1 \in \mathrm{DER}_{\mathcal{B}}(\langle b,\sigma\rangle \Downarrow false)$: $\forall \mathcal{H}2 \in \mathrm{DER}_{\mathcal{T}}(\langle c2,\sigma\rangle \to \sigma')$:
  [(P($\mathcal{H}$2)) $\Rightarrow$ P(riff($\langle$if b then c1 else c2 fi, $\sigma\rangle \to \sigma'$, ($\mathcal{H}$1, $\mathcal{H}$2)))]

Fortsetzung auf nächster Folie

Induktion über Herleitungen in $\mathcal{C}$ (2)

Beweisprinzip (Fortsetzung):

- $\forall \sigma,\sigma',\sigma'' \in \Sigma$: $\forall b \in$ Bexp: $\forall c1 \in$ Com:
  $\forall \mathcal{H}1 \in DER_{\mathcal{B}}(\langle b,\sigma\rangle \Downarrow true)$:
  $\forall \mathcal{H}2 \in DER_{\mathcal{C}}(\langle c1,\sigma\rangle \rightarrow \sigma'')$: $\forall \mathcal{H}3 \in DER_{\mathcal{C}}(\langle$while b do c1 od$,\sigma''\rangle \rightarrow \sigma')$:
  $[(P(\mathcal{H}2) \wedge P(\mathcal{H}3)) \Rightarrow P($ rwht($\langle$while b do c1 od, $\sigma\rangle \rightarrow \sigma'$, $(\mathcal{H}1,\mathcal{H}2,\mathcal{H}3)))]$
- $\forall \sigma \in \Sigma$: $\forall b \in$ Bexp: $\forall c1 \in$ Com:
  $\forall \mathcal{H}1 \in DER_{\mathcal{B}}(\langle b,\sigma\rangle \Downarrow false)$:
  P(rwhf($\langle$while b do c1 od, $\sigma\rangle \rightarrow \sigma$, $(\mathcal{H}1)$))

dann gilt auch

- $\forall \mathcal{H} \in DER_{\mathcal{C}}$: $P(\mathcal{H})$

Übersicht: Modul 7

Termbeschreibungen von Herleitungen

Induktionsprinzip

- Induktion über Herleitungen

Deterministische Auswertung von Programmen

- Beweis mit Induktion über Herleitungen

Deterministische Berechnung (1)

Theorem

Für alle $c \in Com$ und alle Zustände $\sigma, \sigma', \sigma''$ gilt:
wenn $\langle c,\sigma\rangle \to \sigma'$ und $\langle c,\sigma\rangle \to \sigma''$ herleitbar sind, dann gilt $\sigma' = \sigma''$.

Beweis

- Es genügt zu zeigen, dass
  $\forall c \in Com: \forall \sigma,\sigma',\sigma'' \in \Sigma:$
  $\forall \mathcal{H} \in DER_{\mathcal{T}}(\langle c,\sigma\rangle \to \sigma'): \forall \mathcal{H}' \in DER_{\mathcal{T}}(\langle c,\sigma\rangle \to \sigma''): \sigma' = \sigma''$
- Diese Aussage ist äquivalent zu
  $\forall \mathcal{H} \in DER_{\mathcal{T}}: \forall c \in Com: \forall \sigma,\sigma',\sigma'' \in \Sigma:$
  $[\ \mathcal{H} \in DER_{\mathcal{T}}(\langle c,\sigma\rangle \to \sigma') \Rightarrow \forall \mathcal{H}' \in DER_{\mathcal{T}}(\langle c,\sigma\rangle \to \sigma''): \sigma' = \sigma''\ ]$
- Wir beweisen letztere Aussage per Induktion über $\mathcal{H}$, wobei
  $P(\mathcal{H}) = \forall c \in Com: \forall \sigma,\sigma',\sigma'' \in \Sigma:$
  $[\ \mathcal{H} \in DER_{\mathcal{T}}(\langle c,\sigma\rangle \to \sigma') \Rightarrow \forall \mathcal{H}' \in DER_{\mathcal{T}}(\langle c,\sigma\rangle \to \sigma''): \sigma' = \sigma''\ ]$

Deterministische Berechnung (2)

Beweis (Fortsetzung)

Fall $\forall\sigma^*\in\Sigma$: P(rsk($\langle skip,\sigma^*\rangle\to\sigma^*$, ()))

- Es ist zu zeigen, dass
  $\forall\sigma^*\in\Sigma$: $\forall c\in Com$:$\forall\sigma,\sigma',\sigma''\in\Sigma$:
  $[rsk(\langle skip,\sigma^*\rangle\to\sigma^*,())\in DER(\langle c,\sigma\rangle\to\sigma')\Rightarrow\forall\mathcal{H}'\in DER(\langle c,\sigma\rangle\to\sigma''):\sigma''=\sigma']$
- Seien $c\in Com$ und $\sigma^*,\sigma,\sigma',\sigma''\in\Sigma$ beliebig.
- Aus $rsk(\langle skip,\sigma^*\rangle\to\sigma^*,())\in DER(\langle c,\sigma\rangle\to\sigma')$ folgt, dass $c=skip$ und $\sigma=\sigma'=\sigma^*$.
- Sei $\mathcal{H}'\in DER(\langle c,\sigma\rangle\to\sigma'')$ beliebig.
- Die einzige Regel, in deren Konklusion skip vorkommt, ist rsk.
- Daher muss $\mathcal{H}' = rsk(\langle skip,\sigma\rangle\to\sigma,())$ gelten, und somit gilt $\sigma''=\sigma$.
- Also gilt auch $\sigma''=\sigma=\sigma'$.

Beachte: Diese zwei Schritte werden wir in den nachfolgenden Fällen abkürzen.

Deterministische Berechnung (3)

Beweis (Fortsetzung)

Fall r:=

- Es ist zu zeigen, dass
  $\forall\sigma^*\in\Sigma$: $\forall x\in$ Loc: $\forall a\in$ Aexp: $\forall n\in$ N: $\forall\mathcal{H}1\in \mathrm{DER}_{\mathcal{A}}(\langle a,\sigma^*\rangle\Downarrow n)$:
  $\forall c\in$ Com:$\forall\sigma,\sigma',\sigma''\in\Sigma$:
  [$r{:=}(\langle x{:=}a,\sigma^*\rangle\to\sigma^*[x\backslash n],(\mathcal{H}1))\in \mathrm{DER}(\langle c,\sigma\rangle\to\sigma')$
  $\Rightarrow\forall\mathcal{H}'\in \mathrm{DER}(\langle c,\sigma\rangle\to\sigma'')$:$\sigma''=\sigma'$]
- Seien $\sigma^*\in\Sigma$, $x\in$ Loc, $a\in$ Aexp, $n\in$ N und $\mathcal{H}1\in \mathrm{DER}_{\mathcal{A}}(\langle a,\sigma^*\rangle\Downarrow n)$ beliebig.
- Die Herleitung ist $r{:=}(\langle x{:=}a,\sigma^*\rangle\to\sigma^*[x\backslash n],(\mathcal{H}1))$ und somit gelten: $c = x{:=}a$, $\sigma=\sigma^*$ und $\sigma'=\sigma^*[x\backslash n]$.
- Sei $\mathcal{H}'\in \mathrm{DER}(\langle c,\sigma\rangle\to\sigma'')$ beliebig.
- Nur in der Konklusion der Regel r:= kommt eine Zuweisung vor.
- Daher muss $\mathcal{H}' = r{:=}(\langle x{:=}a,\sigma\rangle\to\sigma[x\backslash m],(\mathcal{H}1'))$ gelten, wobei $\mathcal{H}1'\in \mathrm{DER}_{\mathcal{A}}(\langle a,\sigma\rangle\Downarrow m)$ gilt.
- Da die Auswertung von Ausdrücken in Aexp deterministisch ist (siehe Theorem in Modul 6), muss $m=n$ gelten.
- Also gilt auch $\sigma''= \sigma[x\backslash m] = \sigma[x\backslash n] = \sigma^*[x\backslash n] = \sigma'$.

Deterministische Berechnung (4)

Beweis (Fortsetzung)

Fall r;

- Es ist zu zeigen, dass
  $\forall\sigma^*,\sigma^{*\prime},\sigma^{*\prime\prime}\in\Sigma$: $\forall c1,c2\in Com$:
  $\forall\mathcal{H}1\in DER_{\mathcal{T}}(\langle c1,\sigma^*\rangle\to\sigma^{*\prime\prime})$: $\forall\mathcal{H}2\in DER_{\mathcal{T}}(\langle c2,\sigma^{*\prime\prime}\rangle\to\sigma^{*\prime})$:
  $[\ (P(\mathcal{H}1)\wedge P(\mathcal{H}2))\Rightarrow P(\ r;(\ \langle c1;c2,\sigma^*\rangle\to\sigma^{*\prime},\ (\mathcal{H}1,\ \mathcal{H}2)))\ ]$
  für $P(\mathcal{H}) = \forall c\in Com{:}\forall\sigma,\sigma',\sigma''\in\Sigma$:
  $[\ \mathcal{H}\in DER_{\mathcal{T}}(\langle c,\sigma\rangle\to\sigma')\Rightarrow\forall\mathcal{H}'\in DER_{\mathcal{T}}(\langle c,\sigma\rangle\to\sigma''){:}\sigma'=\sigma''\ ]$
- Seien $\sigma^*,\sigma^{*\prime},\sigma^{*\prime\prime}\in\Sigma$, $c1,c2\in Com$, $\mathcal{H}1\in DER_{\mathcal{T}}(\langle c1,\sigma^*\rangle\to\sigma^{*\prime\prime})$ und $\mathcal{H}2\in DER_{\mathcal{T}}(\langle c2,\sigma^{*\prime\prime}\rangle\to\sigma^{*\prime})$ beliebig.
- Die Herleitung ist $r;(\ \langle c1;c2,\sigma^*\rangle\to\sigma^{*\prime},\ (\mathcal{H}1,\ \mathcal{H}2))$ und somit gelten: $c = c1;c2$, $\sigma=\sigma^*$ und $\sigma'=\sigma^{*\prime}$.
- Sei $\mathcal{H}'\in DER(\langle c,\sigma\rangle\to\sigma'')$ beliebig.
- Nur in der Konklusion der Regel r; kommt sequentielle Komposition vor.
- Daher muss $\mathcal{H}' = r;(\ \langle c1;c2,\sigma\rangle\to\sigma'',\ (\mathcal{H}1',\ \mathcal{H}2'))$ gelten, wobei $\mathcal{H}1'\in DER(\langle c1,\sigma\rangle\to\sigma''')$ und $\mathcal{H}2'\in DER(\langle c2,\sigma'''\rangle\to\sigma'')$ für ein $\sigma'''\in\Sigma$.
- Aus $P(\mathcal{H}1)$, $\mathcal{H}1\in DER(\langle c1,\sigma\rangle\to\sigma^{*\prime\prime})$, $\mathcal{H}1'\in DER(\langle c1,\sigma\rangle\to\sigma''')$ folgt $\sigma'''=\sigma^{*\prime\prime}$.
- Aus $P(\mathcal{H}2)$, $\mathcal{H}2\in DER(\langle c1,\sigma^{*\prime\prime}\rangle\to\sigma^{*\prime})$, $\mathcal{H}2'\in DER(\langle c1,\sigma^{*\prime\prime}\rangle\to\sigma'')$ folgt $\sigma''=\sigma^{*\prime}$.
- Also gilt $\sigma'' = \sigma^{*\prime} = \sigma'$.

Deterministische Berechnung (5)

Beweis (Fortsetzung)

Fall rift

…

Fall riff

…

Siehe Übungsblatt und Musterlösung

Deterministische Berechnung (6)

Beweis (Fortsetzung)

Fall rwhf

- Es ist zu zeigen, dass
  $\forall\sigma^*\in\Sigma$: $\forall b\in$ Bexp: $\forall c1\in$ Com:
  $\forall\mathcal{H}1\in DER_{\mathcal{B}}(\langle b,\sigma^*\rangle\Downarrow false)$:
  [P(rwhf($\langle$while b do c1 od, $\sigma^*\rangle\to\sigma^*$, ($\mathcal{H}$1))]
  für $P(\mathcal{H}) = \forall c\in Com:\forall\sigma,\sigma',\sigma''\in\Sigma$:
  $[\ \mathcal{H}\in DER_{\mathcal{T}}(\langle c,\sigma\rangle\to\sigma') \Rightarrow \forall\mathcal{H}'\in DER_{\mathcal{T}}(\langle c,\sigma\rangle\to\sigma''):\sigma'=\sigma''\ ]$
- Seien $\sigma^*\in\Sigma$, $b\in$ Bexp, $c1\in$ Com und $\mathcal{H}1\in DER_{\mathcal{B}}(\langle b,\sigma^*\rangle\Downarrow false)$ beliebig.
- Die Herleitung ist rwhf($\langle$while b do c1 od, $\sigma^*\rangle\to\sigma^*$, ($\mathcal{H}$1)) und somit gelten: c = while b do c1 od, $\sigma=\sigma^*$ und $\sigma'=\sigma^*$.
- Sei $\mathcal{H}'\in DER(\langle c,\sigma\rangle\to\sigma'')$ beliebig.
- Da die Auswertung von Ausdrücken in Bexp deterministisch ist (siehe Theorem in Modul 6), ist $\langle b,\sigma^*\rangle\Downarrow true$ nicht herleitbar.
- Es muss also $\mathcal{H}'$ = rwhf($\langle$while b do c1 od, $\sigma\rangle\to\sigma$, ($\mathcal{H}1'$)) gelten, wobei $\mathcal{H}1'\in DER(\langle b,\sigma^*\rangle\Downarrow false)$, und somit gilt $\sigma''=\sigma$.
- Somit gilt $\sigma''=\sigma=\sigma^*=\sigma'$.

Deterministische Berechnung (7)

Beweis (Fortsetzung)

Fall rwht

- Es ist zu zeigen, dass
  $\forall\sigma^*,\sigma^{*\prime},\sigma^{*\prime\prime}\in\Sigma$: $\forall b\in$ Bexp: $\forall c1\in$ Com:
  $\forall\mathcal{H}1\in DER_{\mathcal{B}}(\langle b,\sigma^*\rangle\Downarrow true)$:
  $\forall\mathcal{H}2\in DER_{\mathcal{C}}(\langle c1,\sigma^*\rangle\rightarrow\sigma^{*\prime\prime})$: $\forall\mathcal{H}3\in DER_{\mathcal{C}}(\langle \text{while } b \text{ do } c1 \text{ od},\sigma^{*\prime\prime}\rangle\rightarrow\sigma^{*\prime})$:
  $[(P(\mathcal{H}2)\wedge P(\mathcal{H}3)) \Rightarrow P(\text{ rwht}(\langle \text{while } b \text{ do } c1 \text{ od}, \sigma^*\rangle\rightarrow\sigma^{*\prime}, (\mathcal{H}1,\mathcal{H}2,\mathcal{H}3)))]$
  für $P(\mathcal{H}) = \forall c\in Com:\forall\sigma,\sigma',\sigma''\in\Sigma$:
  $[\mathcal{H}\in DER_{\mathcal{C}}(\langle c,\sigma\rangle\rightarrow\sigma') \Rightarrow \forall\mathcal{H}'\in DER_{\mathcal{C}}(\langle c,\sigma\rangle\rightarrow\sigma''):\sigma'=\sigma'']$
- Seien $\sigma^*,\sigma^{*\prime},\sigma^{*\prime\prime}\in\Sigma$, $b\in$ Bexp, $c1\in$ Com, $\mathcal{H}1\in DER_{\mathcal{B}}(\langle b,\sigma^*\rangle\Downarrow true)$, $\mathcal{H}2\in DER_{\mathcal{C}}(\langle c1,\sigma^*\rangle\rightarrow\sigma^{*\prime\prime})$ und $\mathcal{H}3\in DER_{\mathcal{C}}(\langle \text{while } b \text{ do } c1 \text{ od},\sigma^{*\prime\prime}\rangle\rightarrow\sigma^{*\prime})$ beliebig.
- Die Herleitung ist $\text{rwht}(\langle \text{while } b \text{ do } c1 \text{ od}, \sigma^*\rangle\rightarrow\sigma^{*\prime}, (\mathcal{H}1,\mathcal{H}2,\mathcal{H}3))$ und somit gelten: c = while b do c1 od, $\sigma=\sigma^*$ und $\sigma'=\sigma^{*\prime}$.
- Sei $\mathcal{H}'\in DER(\langle c,\sigma\rangle\rightarrow\sigma'')$ beliebig.
- Da die Auswertung von Ausdrücken in Bexp deterministisch ist (siehe Theorem in Modul 6), ist $\langle b,\sigma^*\rangle\Downarrow false$ nicht herleitbar.

Deterministische Berechnung (8)

Beweis (Fortsetzung)

Fall rwht (Fortsetzung)

- Daher muss $\mathcal{H}' = \text{rwht}(\langle \text{while b do c1 od}, \sigma\rangle \to \sigma'', (\mathcal{H}1', \mathcal{H}2', \mathcal{H}3'))$ gelten, wobei $\mathcal{H}1' \in \text{DER}(\langle b,\sigma\rangle \Downarrow \text{true})$, $\mathcal{H}2' \in \text{DER}(\langle c1,\sigma\rangle \to \sigma''')$ und $\mathcal{H}3' \in \text{DER}(\langle \text{while b do c1 od}, \sigma'''\rangle \to \sigma'')$ für ein $\sigma''' \in \Sigma$.
- Aus $P(\mathcal{H}2)$, $\mathcal{H}2 \in \text{DER}(\langle c1,\sigma\rangle \to \sigma^{*''})$ und $\mathcal{H}2' \in \text{DER}_{\mathcal{C}}(\langle c1,\sigma\rangle \to \sigma''')$ folgt $\sigma''' = \sigma^{*''}$.
- Aus $P(\mathcal{H}3)$, $\mathcal{H}3 \in \text{DER}(\langle \text{while b do c1 od}, \sigma^{*''}\rangle \to \sigma^{*'})$ und $\mathcal{H}3' \in \text{DER}(\langle \text{while b do c1 od}, \sigma^{*''}\rangle \to \sigma'')$ folgt $\sigma'' = \sigma^{*'}$.
- Also gilt $\sigma'' = \sigma^{*'} = \sigma'$. **qed**

Übung:

- Welche Probleme treten auf, wenn man versucht, dass Theorem mit struktureller Induktion über Com zu beweisen?

Rückblick

Einige wesentliche Lernziele dieses Moduls

- Beherrschung elementarer Verifikationstechniken:
  - … Fortsetzung von Modul 6 …
  - Induktion über Herleitungen in einem Kalkül
- Fähigkeit verschiedene Repräsentationen von Herleitungen zu verwenden (Termrepräsentation, Baumrepräsentation)

Literatur

Glynn Winskel

The Formal Semantics of Programming Languages; Kapitel 2, 3, 4
The MIT Press, 1993.