Formale Grundlagen der Informatik 3 –

6. Induktion und Rekursion

Christoph Walther
TU Darmstadt

1 Grundlagen von Induktion und Rekursion

1.1 Induktionsprinzipien

Beispiel 1 *(Induktionsprinzipien, vgl. FGdI 1)*

(1) Induktion in $\mathbb{N}$:

$$[\varphi(0) \wedge \forall n{:}\mathbb{N}\ \varphi(n) \Rightarrow \varphi(n+1)] \Rightarrow \forall n{:}\mathbb{N}\ \varphi(n)$$

(2) Induktion in $list[\mathbb{N}]$ (= Listen über $\mathbb{N}$)

$$[\varphi(\text{ø}) \wedge \forall k{:}list[\mathbb{N}], n{:}\mathbb{N}\ \varphi(k) \Rightarrow \varphi(n :: k)] \Rightarrow \forall k{:}list[\mathbb{N}]\ \varphi(k)$$

(3) Induktion in Σ^* (= Menge endlicher Worte über Alphabet Σ mit Leerwort ε)

$$[\varphi(\varepsilon) \wedge \forall w{:}\Sigma^*, a{:}\Sigma\ \varphi(w) \Rightarrow \varphi(aw)] \Rightarrow \forall w{:}\Sigma^* \varphi(w)$$

oder

$$[\varphi(\varepsilon) \wedge \forall w{:}\Sigma^*, a{:}\Sigma\ \varphi(w) \Rightarrow \varphi(wa)] \Rightarrow \forall w{:}\Sigma^*\ \varphi(w)$$

Warum gilt das, was ist das Prinzip?

Definition 1 (Fundierte Menge)

Sei M *eine Menge und* $\succ$ *eine Relation auf* M. *Dann ist* $\succ$ fundiert *und* $(M, \succ)$ *ist eine* fundierte Menge *gdw. gilt:*

> *Es gibt keine* unendliche *Folge* $m_0, m_1, m_2, \ldots$ *mit* $m_i \in M$
> *und* $m_0 \succ m_1 \succ m_2 \succ \ldots$. ■

Beispiel 2 *(Fundierte Mengen)*

(1) $(\mathbb{N}, >)$ ist eine fundierte Menge ($\ldots > 3 > 2 > 1 > 0 \not>$)

(2) $(\mathbb{Z}, >)$ ist *keine* fundierte Menge ($\ldots > 3 > 2 > 1 > 0 > -1 > -2 > \ldots$)

(3) $(\Sigma^*, \gtrdot)$ mit $u \gtrdot v$ gdw. $u = av$ (oder $u = va$) für ein $a \in \Sigma$ ist eine fundierte Menge

(4) $(list[\mathbb{N}], \gtrdot)$ mit $k \gtrdot \ell$ gdw. $k = n :: \ell$ für ein $n \in \mathbb{N}$ ist eine fundierte Menge

(5) $(\mathcal{G}(P), \Rightarrow_P)$ ist keine fundierte Menge (=> Kapitel 5, Abschnitt 2.2)

Allgemeinstes Induktionsprinzip: *Noethersche Induktion*

Satz 2 (Noethersche Induktion)

In fundierten Mengen $(M, \succ)$ *gilt das Induktionsprinzip, d.h. es gilt*

$$[\forall m{:}M\ (\forall m'{:}M\ m \succ m' \Rightarrow \varphi(m')) \Rightarrow \varphi(m)] \Rightarrow \forall m{:}M\ \varphi(m) \qquad (1)$$

Beweis: Behauptung (1) hat die Form $[A] \Rightarrow \forall m{:}M\ \varphi(m)$. Wir führen einen Widerspruchsbeweis, d.h. wir nehmen an, daß $[A]$ gilt, $\forall m{:}M\ \varphi(m)$ jedoch falsch ist. Dann muß $\exists m{:}M\ \neg\varphi(m)$ gelten.

Sei m_0 ein bzgl. $\succ$ minimales Element in M mit $\neg\varphi(m_0)$. Dann gilt $\varphi(m')$ für alle $m' \in M$ mit $m_0 \succ m'$. Mit $[A]$ gilt dann insbesondere

$$(\forall m'{:}M\ m_0 \succ m' \Rightarrow \varphi(m')) \Rightarrow \varphi(m_0)$$

und somit gilt $\varphi(m_0)$. ▼

Hinweis: *Noethersche Induktion* in der fundierten Menge $(\mathbb{N}, >)$ wurde in FGdI 1 als *Werteverlaufsinduktion* bezeichnet.

Alternative Formulierung der *Noetherschen Induktion*

Für eine fundierte Menge $(M, \succ)$ definieren wir:

- $min_{\succ}(M) := \{m \in M | m \not\succ m' \text{ für alle } m' \in M\}$ (= die $\succ$-minimalen Elemente von M)
- $pre_{\succ}(m) := \{m' \in M | m \succ m'\}$ (= alle $\succ$-Vorgänger von $m \in M$)

Damit *Noethersche Induktion* umformuliert**:**

$$\begin{aligned}
&\forall m{:}M\ m \in min_{\succ}(M) \Rightarrow \varphi(m) \wedge \\
&\forall m{:}M\ m \notin min_{\succ}(M) \wedge [\forall m'{:}M\ m' \in pre_{\succ}(m) \Rightarrow \varphi(m')] \Rightarrow \varphi(m) \\
&\Rightarrow \forall m{:}M\ \varphi(m)
\end{aligned} \tag{2}$$

Also: Beweise $\forall m{:}M\ \varphi(m)$ durch

- Beweis von $\varphi(m)$ für alle $\succ$-minimalen Elemente von M, und
- Beweis von $\varphi(m)$ für alle *nicht*- $\succ$-minimalen Elemente von M, wobei $\forall m'{:}M\ m' \in pre_{\succ}(m) \Rightarrow \varphi(m')$ (= *Induktionshypothese*) in diesem Beweis verwendet werden darf.

Beispiel 3 *(Reformulierte Noethersche Induktion)*

(1) Induktion in $\mathbb{N}$:

$$\begin{aligned}&\forall n{:}\mathbb{N}\; n = 0 \Rightarrow \varphi(n) \wedge\\ &\forall n{:}\mathbb{N}\; n \neq 0 \wedge \varphi(n-1) \Rightarrow \varphi(n)\\ &\Rightarrow \forall n{:}\mathbb{N}\; \varphi(n)\end{aligned}$$

(2) Induktion in $list[\mathbb{N}]$ (= Listen über $\mathbb{N}$)

$$\begin{aligned}&\forall k{:}list[\mathbb{N}]\; k = ø \Rightarrow \varphi(k) \wedge\\ &\forall k{:}list[\mathbb{N}]\; k \neq ø \wedge \varphi(tl(k)) \Rightarrow \varphi(k)\\ &\Rightarrow \forall k{:}list[\mathbb{N}]\; \varphi(k)\end{aligned}$$

Vergleich: Induktionsprinzipien aus Beispiel (1) und Beispiel (3)

- Beispiel (1): *Konstruktorinduktion* (Schrittfall $n \mapsto n+1$, $k \mapsto n :: k$)
- Beispiel (3): *Destruktorinduktion* (Schrittfall $n-1 \mapsto n$, $tl(k) \mapsto k$)
- Konstruktorinduktion im allgemeinen *schwächer* als Destruktorinduktion
- **Konsequenz**: Wir verwenden *Destruktorinduktion*

Beispiel 4 *(Destruktorinduktion vs. Konstruktorinduktion)*

- Für nicht-leere Listen $k \in \mathit{list}[\mathbb{N}]$ sei $\mathit{minimum}(k)$ ein minimales Element von k (bzgl. der üblichen $\leq$-Relation auf $\mathbb{N}$).
- Für $n \in \mathbb{N}$ und $k \in \mathit{list}[\mathbb{N}]$ entstehe die Liste $\mathit{remove}(n, k)$ durch Löschen aller Vorkommen von n in k.
- Für Listen $k, \ell \in \mathit{list}[\mathbb{N}]$ gelte:
  $k \gtrdot \ell$ gdw. $k \neq ø \wedge \ell = \mathit{remove}(\mathit{minimum}(k), k)$.
- *Dann gilt*:$(\mathit{list}[\mathbb{N}], \gtrdot)$ ist fundierte Menge (Beweis: *Übung*).
- *Damit*: $\mathit{min}_{\gtrdot}(\mathit{list}[\mathbb{N}]) = \{ø\}$ sowie $\mathit{pre}_{\gtrdot}(k) = \{\mathit{remove}(\mathit{minimum}(k), k)\}$.
- *Induktionsprinzip* nach (2):

$$\begin{aligned}&\forall k{:}\mathit{list}[\mathbb{N}]\ k = ø \Rightarrow \varphi(k) \wedge \\ &\forall k : \mathit{list}[\mathbb{N}]\ k \neq ø \wedge \varphi(\mathit{remove}(\mathit{minimum}(k), k)) \Rightarrow \varphi(k) \\ &\Rightarrow \forall k : \mathit{list}[\mathbb{N}]\ \varphi(k)\end{aligned} \tag{3}$$

Keine Konstruktorinduktion für (3) !

1.2 Das Rekursionsprinzip

Sei $(M, \succ)$ fundierte Menge und sei $f : M \mapsto N$.
Dann gilt mit Satz 2 (ersetze "$\varphi(m)$" durch "$f(m) \in N$"):

$$\begin{aligned} &\forall m{:}M\ [\forall m'{:}M\ m \succ m' \Rightarrow f(m') \in N] \Rightarrow f(m) \in N \\ &\Rightarrow \forall m{:}M\ f(m) \in N \end{aligned} \tag{4}$$

Noethersche Induktion umformuliert:

$$\begin{aligned} &\forall m{:}M\ m \in min_{\succ}(M) \Rightarrow f(m) \in N \wedge \\ &\forall m{:}M\ m \notin min_{\succ}(M) \wedge [\forall m'{:}M\ m' \in pre_{\succ}(m) \Rightarrow f(m') \in N] \Rightarrow f(m) \in N \\ &\Rightarrow \forall m{:}M\ f(m) \in N \end{aligned} \tag{5}$$

Also: $f(m)$ ist für alle $m \in M$ *definiert* (= f ist eine *totale* Funktion) falls

- $f(m)$ für alle $\succ$-minimalen Elemente von M definiert ist, und
- $f(m)$ für alle *nicht*- $\succ$-minimalen Elemente von M definiert ist, wobei "$f(m')$ ist definiert für jedes $m'{:}M$ mit $m' \in pre_{\succ}(m)$" (= *rekursive Aufrufe*) vorausgesetzt werden darf.

Damit: *Rekursive Definitionen sind Anwendungen des Induktionsprinzips* **!**

Beispiel 5 *(Reformulierte Noethersche Rekursion)*

(1) Rekursion in $\mathbb{N}$ (also $f : \mathbb{N} \mapsto N$)

$$\begin{aligned}&\forall n{:}\mathbb{N}\ n = 0 \Rightarrow f(n) \in N \wedge\\&\forall n{:}\mathbb{N}\ n \neq 0 \wedge f(n-1) \in N \Rightarrow f(n) \in N\\&\Rightarrow \forall n{:}\mathbb{N}\ f(n) \in N\end{aligned}$$

Vgl. rekursive Definition von $\leq : \mathbb{N} \times \mathbb{N} \mapsto$ `bool` in der Fallstudie “Sortieren durch Einfügen” (=> **Kapitel 2**).

(2) Rekursion in $list[\mathbb{N}]$ (also $f : list[\mathbb{N}] \mapsto N$)

$$\begin{aligned}&\forall k{:}list[\mathbb{N}]\ k = ø \Rightarrow f(k) \in N \wedge\\&\forall k{:}list[\mathbb{N}]\ k \neq ø \wedge f(tl(k)) \in N \Rightarrow f(k) \in N\\&\Rightarrow \forall k{:}list[\mathbb{N}]\ f(k) \in N\end{aligned}$$

Vgl. rekursive Definition von `isort` $:$ `list`$[\mathbb{N}] \mapsto$ `list`$[\mathbb{N}]$ in der Fallstudie “Sortieren durch Einfügen” (=> **Kapitel 2**).

2 Induktion und Rekursion in *VeriFun*

2.1 Relationenbeschreibungen

- Die Begriffe *fundierte Relation* $\succ$, $min_{\succ}(M)$, $pre_{\succ}(m)$ u.s.w. sind Begriffe der *Semantik*.
- Um diese Begriffe in einem Beweissystem verwenden zu können, müssen sie durch *objektsprachliche Ausdrücke* repräsentiert werden.
- Dies geschieht in *VeriFun* durch sogenannte *Relationenbeschreibungen*.

Definition 3 *(Relationenbeschreibungen)*

Eine atomare *Relationenbeschreibung ist ein Paar* $\langle H, \Delta \rangle$ *mit*

(1) H (= Menge der *Hypothesen*) ist eine endliche Menge von *Literalen*

(2) Δ ist eine endliche Menge von *Substitutionen* (Subst.paare x/x hier erlaubt !)

*Eine (*zusammengesetzte*) Relationenbeschreibung ist eine endliche, nicht-leere Menge* $\{\langle H_1, \Delta_1 \rangle, \ldots, \langle H_n, \Delta_n \rangle\}$ *von atomaren Relationenbeschreibungen mit*

(3) $\bigvee_{i \in \{1,\ldots,n\}} \bigwedge_{h \in H_i} h$ *und* (4) $\bigwedge_{h \in H_i} h \Rightarrow \neg \bigwedge_{h \in H_j} h$ für alle $i \neq j \in \{1, \ldots, n\}$

- (3) und (4): *mindestens* und *höchstens* (also *genau*) eine Konjunktion der Hypothesen einer atomaren Relationenbeschreibungen gilt. ■

Bedeutung:

(1) Die Hypothesenmengen H_i repräsentieren *Teilmengen* M_i von $min_\succ(M)$ und $M \setminus min_\succ(M)$ (bzgl. einer Relation $\succ$ auf M)

(2) Die Substitutionen aus Δ_i repräsentieren Teilmengen von $pre_\succ(\ldots)$ (bzgl. einer Relation $\succ$ auf M)

(3) Mit den Forderungen (3) und (4) wird die *disjunkte Separierung* von M durch die Mengen M_i garantiert (d.h. $M = \bigcup_i M_i$ und $M_i \cap M_j = \emptyset$ für $i \neq j$)

(4) Atomare Relationenbeschreibungen $\langle H, \Delta \rangle$ mit $\Delta = \emptyset$ heißen *nicht-rekursiv* und repräsentieren (Teilmengen) von $min_\succ(M)$

(5) Atomare Relationenbeschreibungen $\langle H, \Delta \rangle$ mit $\Delta \neq \emptyset$ heißen *rekursiv* und repräsentieren (Teilmengen) von $M \setminus min_\succ(M)$ und von $pre_\succ(\ldots)$

Beispiel 6 *(Relationenbeschreibungen)*

(1) Relationenbeschreibung für $\mathbb{N}$ bzgl. der Vorgänger-Relation:

$$R_1 = \{\langle \{n = 0\}, \emptyset \rangle, \langle \{\neg\, n = 0\}, \{\{n/pred(n)\}\} \rangle\}$$

(2) Relationenbeschreibung für $list[@T]$ bzgl. der Restlisten-Relation:

$$R_2 = \{\langle \{k = ø\}, \emptyset \rangle, \langle \{\neg\, k = ø\}, \{\{k/tl(k)\}\} \rangle\}$$

Definition 4 (Instanzen von Relationenbeschreibungen)

Eine Relationenbeschreibung R' ist eine Instanz *einer Relationenbeschreibung R gdw. R' aus R durch Ersetzung der Typen τ der Variablensymbole von R durch Instanzen τ' von τ entsteht.* ■

Definition 5 (Monomorphe und polymorphe Relationenbeschreibungen)

Eine Relationenbeschreibung R ist monomorph *gdw. jeder Typ eines Variablensymbols von R monomorph ist. Eine Relationenbeschreibung R ist* polymorph *gdw. R nicht monomorph ist.* ■

2.2 Semantik von Relationenbeschreibungen

Definition 6 (Durch atomare Relationenbeschreibungen definierte Relation)
Sei

- $A := \langle H, \Delta \rangle$ eine *atomare* und *monomorphe* Relationenbeschreibung,
- $\{y_1, \ldots, y_k\}$ die Menge aller Variablen, die in A vorkommen,
- $x^* := x_1 \ldots x_k$ eine Liste dieser Variablen mit $x_i : \tau_i$ für jedes $i \in \{1, \ldots, k\}$,
- $\mathcal{C}_{\tau_i}$ jeweils die Mengen aller Konstrukturgrundterme des Datentyps τ_i.

Dann wird A und x^* genau eine binäre Relation $>_{A,x^*}$ auf $\mathcal{C}_{\tau_1} \times \ldots \times \mathcal{C}_{\tau_k}$ zugeordnet durch

$$q_1 \ldots q_k >_{A,x^*} r_1 \ldots r_k$$

gdw.

für $\theta := \{x_1/q_1, \ldots, x_k/q_k\}$
1. für alle $h \in H : eval_P(\theta(h)) =$ `true` und
2. für ein $\delta \in \Delta$ und alle i mit $x_i \in DEF(\delta) : eval_P(\theta(\delta(x_i))) = r_i$.

∎

Beispiel 7 *(Durch atomare Relationenbeschreibungen definierte Relation)*

(1) Für die rekursive atomare Relationenbeschreibung

$$A_1 := \langle\{\neg?0(x), \neg?0(y), x > y\}\,, \{\{x/x - y, y/y\}\}\rangle$$

erhält man beispielsweise

$$(8,3) >_{A_1,xy} (5,3) >_{A_1,xy} (2,3) \not>_{A_1,xy}$$

und insbesondere $(0,\ldots) \not>_{A_1,xy}$ sowie $(\ldots,0) \not>_{A_1,xy}$.

(2) Für die rekursive atomare Relationenbeschreibung

$$A_2 := \langle\{\neg?0(x), \neg?0(y), \neg x > y\}\,, \{\{x/x, y/y - x\}\}\rangle$$

erhält man beispielsweise

$$(3,9) >_{A_2,xy} (3,6) >_{A_2,xy} (3,3) >_{A_2,xy} (3,0) \not>_{A_2,xy}$$

und insbesondere $(0,\ldots) \not>_{A_2,xy}$ sowie $(\ldots,0) \not>_{A_2,xy}$.

Definition 7 (Relation einer zusammengesetzten Relationenbeschreibung)
Sei

- $R := \{A_1, \ldots, A_n\}$ eine *zusammengesetzte* und *monomorphe* Relationenbeschreibung,
- $\{y_1, \ldots, y_k\}$ die Menge aller Variablen, die in R vorkommen,
- $x^* := x_1 \ldots x_k$ eine Liste dieser Variablen mit $x_i : \tau_i$ für jedes $i \in \{1, \ldots, k\}$,
- $\mathcal{C}_{\tau_i}$ jeweils die Mengen aller Konstrukturgrundterme des Datentyps τ_i.

Dann wird R und x^* genau eine binäre Relation $>_{R,x^*}$ auf $\mathcal{C}_{\tau_1} \times \ldots \times \mathcal{C}_{\tau_k}$ zugeordnet durch

$$q_1 \ldots q_k >_{R,x^*} r_1 \ldots r_k$$

gdw.

$$q_1 \ldots q_k >_{A,x^*} r_1 \ldots r_k$$

für eine rekursive *atomare Relationenbeschreibung A von R .* ■

Anders gesagt: $>_{R,x^*} \; := \; \bigcup_{A \in R} >_{A,x^*}$

Beispiel 8 *(Relation einer zusammengesetzten Relationenbeschreibungen)*
Für die zusammengesetzte Relationenbeschreibung $R := \{A_1, A_2, A_3, A_4\}$ *mit*

$$\begin{aligned}
A_1 &= \langle \{?0(x)\}, \emptyset \rangle \\
A_2 &= \langle \{\neg ?0(x), ?0(y)\}, \emptyset \rangle \\
A_3 &= \langle \{\neg ?0(x), \neg ?0(y), x > y\}, \{\{x/x-y, y/y\}\} \rangle \\
A_4 &= \langle \{\neg ?0(x), \neg ?0(y), \neg x > y\}, \{\{x/x, y/y-x\}\} \rangle
\end{aligned}$$

erhält man beispielsweise

$$(8,3) >_{R,xy} (5,3) >_{R,xy} (2,3) >_{R,xy} (2,1) >_{R,xy} (1,1) >_{R,xy} (1,0) \not>_{R,xy}$$

denn

- $(8,3) >_{A_3,xy} (5,3) >_{A_3,xy} (2,3)$,
- $(2,3) >_{A_4,xy} (2,1)$,
- $(2,1) >_{A_3,xy} (1,1)$,
- $(1,1) >_{A_4,xy} (1,0)$, und
- $(1,0) \not>_{A_3,xy}$, sowie
- $(1,0) \not>_{A_4,xy}$.

Bemerkung 1 (Nicht-rekursive atomare Relationenbeschreibungen)

- Die durch eine zusammengesetzte Relationenbeschreibung R bzgl. einer Variablenliste x^* definierte Relation $>_{R,x^*}$ ist *unabhängig* von den *nicht-rekursiven* atomaren Relationenbeschreibungen in R.
- *Konsequenz:* Nicht-rekursive atomare Relationenbeschreibungen könnten *weggelassen* werden.
- *Warum dennoch* nicht-rekursive *atomare Relationenbeschreibungen?*
  Aus Relationenbeschreibungen werden Induktionsaxiome gewonnen (=> Abschnitt 2.3), wobei aus den *nicht-rekursiven* atomaren Relationenbeschreibungen die *Basisfälle* eines Induktionsaxioms gebildet werden. Ohne nicht-rekursive atomare Relationenbeschreibungen müßten diese automatisch ergänzt werden. Dies ist zwar immer möglich (warum?), führt jedoch mitunter zu redundanten und damit überflüssigen Beweisverpflichtungen.
- *Kurzum:* Mit nicht-rekursiven atomaren Relationenbeschreibungen erhält man “bessere” Induktionsaxiome.

Definition 8 (Fundierte Relationenbeschreibungen)

Eine (zusammengesetzte) monomorphe *Relationenbeschreibung* R *heißt* fundiert *gdw.* $>_{R,x^*}$ *für* eine *Liste* x^* *der Variablen von* R *eine* fundierte Relation *ist.*

Eine (zusammengesetzte) Relationenbeschreibung R *heißt* fundiert *gdw. jede monomorphe Instanz von* R fundiert *ist.* ■

Bemerkung 2

Mit x^* *wird lediglich die* Reihenfolge der Komponenten *in den* k*-Tupeln* $q_1 \ldots q_k$ *festgelegt.*

- *Es gilt:* Für die Fundiertheit von $>_{R,x^*}$ ist die durch x^* festgelegte Reihenfolge unerheblich.
- *Konsequenz:*
  $>_{R,x^*}$ ist für *eine* Liste x^* der Variablen von R eine *fundierte Relation* gdw.
  $>_{R,x^*}$ ist für *jede* Liste x^* der Variablen von R eine *fundierte Relation*.

2.3 Induktionsaxiome aus Relationenbeschreibungen

Aus einer Relationenbeschreibung kann man unmittelbar ein Induktionsprinzip “ablesen” (vgl. die Induktionsprinzipien aus Beispiel 3 mit den Relationenbeschreibungen aus Beispiel 6):

- Seien $x_1, \ldots, x_k, y_1, \ldots, y_l$ Variable mit $x_i : \tau_i$ und $y_j : \tau'_j$ für Datentypen τ_i und τ'_j
- Sei $R := \{A_1, \ldots, A_n\}$ eine Relationenbeschreibung mit
  – $A_i := \langle H_i, \Delta_i \rangle$ und – $\{x_1, \ldots, x_k\}$ = Menge aller Variablen in R
- Sei b ein boolscher Term, in dem genau die Variablen $\{x_1, \ldots, x_k, y_1, \ldots, y_l\}$ vorkommen
- **Dann:** Für jede atomare Relationenbeschr. A_i wird die *Induktionsformel*[1]

$$\boxed{\begin{aligned}\mathcal{I}_i := \ & \forall x_1{:}\tau_1, \ldots, x_k{:}\tau_k, y_1{:}\tau'_1, \ldots, y_l{:}\tau'_l \\ & \textstyle\bigwedge_{h \in H_i} h \equiv \mathtt{true} \wedge \left[\bigwedge_{\delta \in \Delta_i} \forall y_1{:}\tau'_1, \ldots, y_l{:}\tau'_l \ \delta(b) \equiv \mathtt{true}\right] \Rightarrow b \equiv \mathtt{true}\end{aligned}}$$

  gebildet (die Variablen $y_1, \ldots, y_l$ aus b verbleiben also *allquantifiziert* in den *Induktionshypothesen* $\forall y_1{:}\tau'_1, \ldots, y_l{:}\tau'_l \ \delta(b) \equiv \mathtt{true}$)

[1] “$\equiv$” ist das Gleichheitszeichen der Prädikatenlogik 1. Stufe, also ein *Prädikatensymbol* (=> **Kapitel 9**, Folie 5).

- *Induktionsformeln* $\mathcal{I}_i$ werden durch *HPL*-Sequenzen

$$\boxed{seq_{\mathcal{I}_i} = \left\langle H_i,\ \bigcup_{\delta\in\Delta_i} \forall y_1 : \tau'_1, \ldots, y_l : \tau'_l\ \delta(b)\ \Vdash\ b \right\rangle}$$

  repräsentiert

- Aus den Induktionsformeln $\mathcal{I}_i$ wird das *Induktionsaxiom*

$$\boxed{IndAx_{b,R} :=\ \mathcal{I}_1 \wedge \ldots \wedge \mathcal{I}_n \Rightarrow \forall x_1{:}\tau_1, \ldots, x_k{:}\tau_k, y_1{:}\tau'_1, \ldots, y_l{:}\tau'_l\ b \equiv \texttt{true}}$$

  gebildet.

Es gilt:

Satz 9 (Gültigkeit von Induktionsaxiomen aus Relationenbeschreibungen)
Ist R fundiert, *so ist das* Induktionsaxiom $IndAx_{b,R}$ “wahr”.

- Induktionsaxiom “*wahr*”
  => **Kapitel 12** (Definition 15)**:** *Semantik von* $\mathcal{L}$*-Formeln*

Beispiel 9 *(Induktionsformeln und Induktionsaxiome)*

Für $b := \mathtt{if}\{\mathtt{n} \le \mathtt{m},\ \mathtt{true},\ \mathtt{m} \le \mathtt{n}\}$ *(vgl.* $\mathcal{L}$*-Lemma* $\le$ `_is_total` *aus* ***Kapitel 2****)* *und die Relationenbeschreibung*

$$R_1 = \{\langle\{\mathtt{n=0}\}, \emptyset\rangle, \langle\{\neg\,\mathtt{n=0}\}, \{\{\mathtt{n}/\mathtt{pred(n)}\}\}\rangle\}$$

erhält man für die Induktionsformeln die HPL*-Sequenzen*

$$seq_{\mathcal{I}_1} = \langle\{\mathtt{n=0}\},\ \emptyset \Vdash \mathtt{if}\{\mathtt{n} \le \mathtt{m}, \mathtt{true}, \mathtt{m} \le \mathtt{n}\}\rangle$$

und

$$\begin{aligned} seq_{\mathcal{I}_2} = \quad & \langle\{\neg\,\mathtt{n=0}\}, \\ & \{\forall \mathtt{m}{:}\mathbb{N}\ \mathtt{if}\{\mathtt{pred(n)} \le \mathtt{m},\ \mathtt{true},\ \mathtt{m} \le \mathtt{pred(n)}\}\} \\ & \Vdash\ \mathtt{if}\{\mathtt{n} \le \mathtt{m},\ \mathtt{true},\ \mathtt{m} \le \mathtt{n}\}\rangle \end{aligned}$$

zur Repräsentation des Induktionsaxioms[2]

$$\begin{aligned} & \forall n, m{:}\mathbb{N}\ n = 0 \Rightarrow n \le m \vee m \le n\ \wedge \\ & \forall n, m{:}\mathbb{N}\ n \ne 0 \wedge [\forall m{:}\mathbb{N}\ n-1 \le m \vee m \le n-1 \Rightarrow n \le m \vee m \le n] \\ & \Rightarrow \forall n, m{:}\mathbb{N}\ n \le m \vee m \le n \end{aligned}$$

[2] Zwecks Lesbarkeit verzichten wir hier auf die formal erforderlichen Schreibweisen “$n \le m \equiv \mathtt{true}$”, “$n - 1 \le m \equiv \mathtt{true}$” u.s.w. .

- Um *Variable* in einer Relationenbeschreibungen und in einem Lemma *anzupassen*, dürfen Variable (der Relationenbeschreibung und/oder des Lemmas) *umbenannt* werden

Beispiel 10 *(Induktionsformeln und Induktionsaxiome nach Umbenennung)*
Für $b := \mathtt{if}\{\mathtt{n} \leq \mathtt{m},\ \mathtt{true},\ \mathtt{m} \leq \mathtt{n}\}$ *erhält man aus der Relationenbeschreibung*

$$R_1 = \{\langle\{\mathtt{n = 0}\}, \emptyset\rangle, \langle\{\neg\, \mathtt{n = 0}\}, \{\{\mathtt{n}/\mathtt{pred(n)}\}\}\rangle\}$$

die umbenannte *Relationenbeschreibung*

$$R_1' = \{\langle\{\mathtt{m = 0}\}, \emptyset\rangle, \langle\{\neg\, \mathtt{m = 0}\}, \{\{\mathtt{m}/\mathtt{pred(m)}\}\}\rangle\}$$

und damit für die Induktionsformeln die HPL*-Sequenzen*

$$seq_{\mathcal{I}_1} = \langle\{\mathtt{m = 0}\},\ \emptyset\ \Vdash\ \mathtt{if}\{\mathtt{n} \leq \mathtt{m}, \mathtt{true}, \mathtt{m} \leq \mathtt{n}\}\rangle$$

und

$$\begin{aligned} seq_{\mathcal{I}_2} = \quad & \langle\{\neg\, \mathtt{m = 0}\}, \\ & \{\forall \mathtt{n}{:}\mathbb{N}\ \mathtt{if}\{\mathtt{n} \leq \mathtt{pred(m)},\ \mathtt{true},\ \mathtt{pred(m)} \leq \mathtt{n}\}\} \\ & \Vdash\ \mathtt{if}\{\mathtt{n} \leq \mathtt{m},\ \mathtt{true},\ \mathtt{m} \leq \mathtt{n}\}\rangle \end{aligned}$$

Fazit:

- Um *Induktionsbeweise* in *VeriFun* zu führen, müssen *fundierte Relationenbeschreibungen* bereitgestellt werden (=> **Kapitel 7**).