Sequenzenkalkül

Sequenz
Alles von der Form

$$\Phi \Rightarrow \Psi$$

Bedeutung
1. Aus der Konjunktion der Formeln in Φ folgt die Disjunktion der Formeln in Ψ.
2. $\Rightarrow \Psi$
Disjunktion der Formeln in Ψ wahr (allgemeingültig)
3. $\Phi \Rightarrow$
Die Konjunktion der Formeln in Φ falsch (nicht erfüllbar).

Aussagenlogik

α-Regeln

$$\frac{\Phi, X, Y \Rightarrow \Psi}{\Phi, X \wedge Y \Rightarrow \Psi} \qquad \frac{\Phi \Rightarrow X, Y, \Psi}{\Phi \Rightarrow X \vee Y, \Psi}$$

β-Regeln

$$\frac{\begin{array}{c}\Phi_1, X \Rightarrow \Psi_1 \\ \Phi_2, Y \Rightarrow \Psi_2\end{array}}{\Phi_1, \Phi_2, X \vee Y \Rightarrow \Psi_1, \Psi_2} \qquad \frac{\begin{array}{c}\Phi_1 \Rightarrow X, \Psi_1 \\ \Phi_2 \Rightarrow Y, \Psi_2\end{array}}{\Phi_1, \Phi_2 \Rightarrow X \wedge Y, \Psi_1, \Psi_2}$$

Aussagenlogik

$$\frac{\Phi, \neg X \Rightarrow \Psi}{\Phi \Rightarrow X, \Psi} \qquad \frac{\Phi \Rightarrow \neg X, \Psi}{\Phi, X \Rightarrow \Psi}$$

Aussagenlogik

Die Schnittregel

$$\frac{\Phi_1 \Rightarrow X, \Psi_1 \quad \Phi_2, X \Rightarrow \Psi_2}{\Phi_1, \Phi_2 \Rightarrow \Psi_1, \Psi_2}$$

Spezialfall des Schnitts: Modus Ponens

(1) $\Rightarrow X$
(2) $X \Rightarrow Y$
(3) $\Rightarrow Y$

abgeleitete Regel

$$\frac{\Phi_1 \Rightarrow X, \Psi_1 \quad \Phi_2, X \Rightarrow \Psi_2}{\Phi_1, \Phi_2 \Rightarrow Y, \Psi_1, \Psi_2}$$

Beweisführung in KeY

Start
: zu beweisende Sequenz: Regelkonklusio

Suche nach
: Prämissen

Beweis gefunden – Beweiszweig erfolgreich
wenn etwa Sequenz der Form

$$\Phi, X \Rightarrow X, \Psi \qquad\qquad \Phi \Rightarrow t \doteq t, \Psi_1$$
$$\Phi, X \Rightarrow \neg\neg X, \Psi \qquad\qquad \Phi, \neg t \doteq t \Rightarrow \Psi_1$$

erhalten.

Prädikatenlogik

γ-Regeln

$$\frac{\Phi, [Z]^t_x, \forall x\, Z \Rightarrow \Psi}{\Phi, \forall x\, Z \Rightarrow \Psi} \qquad\qquad \frac{\Phi \Rightarrow [Z]^t_x, \exists x\, Z, \Psi}{\Phi \Rightarrow \exists x\, Z, \Psi}$$

δ-Regeln

$$\frac{\Phi \Rightarrow [Z]^c_x, \forall x\, Z, \Psi}{\Phi \Rightarrow \forall x\, Z, \Psi} \qquad\qquad \frac{\Phi, [Z]^c_x, \exists x\, Z \Rightarrow \Psi}{\Phi, \exists x\, Z \Rightarrow \Psi}$$

Hier ausreichend: t Grundterm, c Konstantenzeichen
Gleichungen

$$\frac{\Phi, s \doteq t \Rightarrow \Psi}{\Phi\{s \leftarrow t\}, s \doteq t \Rightarrow \Psi\{s \leftarrow t\}}$$

Nicht jedes Vorkommen von s muß durch t ersetzt werden.
Regeln für die Symmetrie vorhanden.

Compilerkorrektheit

Anweisung in konkreter Syntax
Syntaxanalyse
Anweisung in abstrakter Syntax: *Quellsprache*
Übersetzung
Anweisung in der *Zielsprache*

Die Quellsprache

Beschränkung auf Zuweisungen wie

$$x := y_1 + y_2 + y_3$$

x nicht auf der rechten Seite

In abstrakter Syntax

$$mk\text{-}sexp(x, vcons(y_1, vcons(y_2, vcons(y_3, t_\varepsilon))))$$

Zielsprache und Übersetzer

$$mk\text{-}sexp(x, vcons(y_1, vcons(y_2, vcons(y_3, t_\varepsilon))))$$

wird übersetzt in

$$x := 0;\ x := x + y_1;\ x := x + y_2;\ x := x + y_3$$

Übersetzer
abstrakt spezifiziert durch

$$gen\text{-}texp\colon Sexp \to Texp$$

Beweisaufgaben

1. *gen-texp* übersetzt syntaktisch korrekte Anweisung der Quellsprache wird in eine syntaktisch korrekte Anweisungsfolge der Zielsprache.

2. *gen-texp* ist semantiktreu.

Hier betrachten wir nur die erste Aufgabe.

Der Übersetzer

(abstrakt) festgelegt durch

$$\forall se\colon Sexp\ gen\text{-}texp(se) = f(s\text{-}l(se), s\text{-}r(se), t_\varepsilon)$$

Selektoren

$s\text{-}l$	linke Seite
$s\text{-}l$	rechte Seite

einer Zuweisung der Quellsprache.

Hilfsfunktion

$$f\colon Var \times Vars \times Tlist \to Texp$$

Der Übersetzer

Hilfsfunktion f

$$f\colon Var \times Vars \times Tlist \to Texp$$

rekursiv im zweiten Argument.

1. $vars = v_\varepsilon$

$$\forall x\colon Var\ (\forall tli\colon Tlist\ f(x, v_\varepsilon, tli) = mk\text{-}texp(mk\text{-}ass(x), tli))$$

$mk\text{-}ass(x)$
erzeugt aus x die Initialisierung $x := 0$

Der Übersetzer

Hilfsfunktion f

$$f\colon Var \times Vars \times Tlist \to Texp$$

2. $vars \neq v_\varepsilon$

$$\forall x\colon Var\ (\forall vs\colon Vars\ (\forall tli\colon Tlist\ (\forall z\colon Var\ (\forall vs_1\colon Vars$$
$$vs = vcons(z, vs_1)$$
$$\to f(x, vs, tli) = f(x, vs_1, conc_1(tli, mk\text{-}rasg(x, x, z)))))))$$

$mk\text{-}rasg(x, x, z)$
erzeugt die Zuweisung $x := x + z$
$conc_1(tli, rasg)$
hängt die Zuweisung *rasg* am Ende von *tli* ein.

Korrektheit

Syntaktisch korrekte Anweisungen gekennzeichnet durch die Prädikate

Wf-Sexp	Quellsprache
Wf-Texp	Zielsprache

Zu beweisen

$$\forall s\ (Wf\text{-}Sexp(s) \to Wf\text{-}Texp(gen\text{-}texp(s)))$$

Korrektheitsaussage: Beweis

$$\forall s\ (\mathit{Wf\text{-}Sexp}(s) \to \mathit{Wf\text{-}Texp}(\mathit{gen\text{-}texp}(s)))$$

1. Einführung von f

Hilfssatz 1

$$\forall x\colon \mathit{Var}\ \forall \mathit{vars}\colon \mathit{Vars}\ (\neg \mathit{In}(x, \mathit{vars}) \to \mathit{Wf\text{-}Texp}(f(x, \mathit{vars}, t_\varepsilon)))$$

In vernünftigen deutschen Sätzen:
Kommt x nicht in der Variablenfolge $vars$ vor, dann ist
$f(x, vars, t_\varepsilon)$ eine korrekte Anweisungsfolge der Zielsprache.

Korrektheitsaussage: Beweis

Nachweis von Hilfssatz 1

Fallunterscheidung bezüglich des zweiten Arguments von f.

Hilfssatz 2. *Wf-Texp-tleer*

$$\forall x\colon \mathit{Var}\ \mathit{Wf\text{-}Texp}(f(x, v_\varepsilon, t_\varepsilon))$$

Hilfssatz 3. *Wf-Texp-Nicht-tleer*

$$\forall x\colon \mathit{Var}\ \forall \mathit{vs}\colon \mathit{Vars}\ \neg \mathit{vs} = v_\varepsilon \wedge \neg \mathit{In}(x, \mathit{vs}) \to \mathit{Wf\text{-}Texp}(f(x, \mathit{vs}, t_\varepsilon))$$