Der Beweiskalkül für die Quantorenlogik

Schlussregeln

Fallunterscheidung, FU: $$\frac{\begin{array}{c}(\varphi \to \psi)\\ (\neg\varphi \to \psi)\end{array}}{\psi}$$

Widerspruch, Wid: $$\frac{\begin{array}{c}(\neg\varphi \to \psi)\\ (\neg\varphi \to \neg\psi)\end{array}}{\varphi}$$

Modus Ponens, MP: $$\frac{\begin{array}{c}\varphi\\ (\varphi \to \psi)\end{array}}{\psi}$$

Allregel, $\forall$: für alle S-Terme t $$\frac{\forall x\varphi}{\varphi\frac{t}{x}}$$

Identitätsregel, $\equiv$: für alle S-Terme t $$\frac{}{t \equiv t}$$

Substitutionsregel, Sub: für alle S-Terme s, t $$\frac{\begin{array}{c}\varphi\frac{s}{x}\\ s \equiv t\end{array}}{\varphi\frac{t}{x}}$$

Texte

Eine Folge $T_0, \ldots, T_{n-1}$ ist ein *Text* gdw es für jedes $i < n$ einen Ausdruck $\varphi_i \in L^S$ gibt mit:

$T_i = \varphi_i$ [" es gilt φ_i "],
oder $T_i => \varphi_i$ [" angenommen φ_i "],
oder $T_i =< \varphi_i$ [" also φ_i "],
oder $T_i =>$.

Ordne dem Text *lokale Voraussetzungen* V_i, *Zeiger* z_i; und Mengen B_i *belegter Variablen* zu:

$V_o = \emptyset,\ z_0 = -\infty,\ B_0 = \emptyset,$
$T_i = \varphi_i$ impliziert $V_{i+1} = V_i \cup \{\varphi_i\},\ z_{i+1} = z_i,\ B_{i+1} = B_i \cup \mathrm{Fr}(\varphi_i),$
$T_i => \varphi_i$ impliziert $V_{i+1} = V_i \cup \{\varphi_i\},\ z_{i+1} = i,\ B_{i+1} = B_i \cup \mathrm{Fr}(\varphi_i),$
$T_i =< \varphi_i$ impliziert $V_{i+1} = V_{z_i} \cup \{\varphi_i\},\ z_{i+1} = z_{z_i},\ B_{i+1} = B_{z_i} \cup \mathrm{Fr}(\varphi_i),$
$T_i =>$ impliziert $V_{i+1} = V_i\ ,\ z_{i+1} = i\ ,\ B_{i+1} = B_i.$

Beweise

Ein Text $T_0, \dots, T_{n-1}$ mit V_i, z_i, B_i wie oben ist ein *Beweis* gdw für $i < n$ und $\varphi_i \in L^S$ gilt:

1. $T_i = \varphi_i$ impliziert, dass $\varphi_i \in V_i$ oder dass es $\psi_0, \dots, \psi_{l-1} \in V_i$ gibt, so dass $\dfrac{\psi_0 \dots \psi_{l-1}}{\varphi_i}$ Instanz einer Schlussregel ist.

2. $T_i = < \varphi_i$ impliziert, dass $z_i \geq 0$ [eine $>$-Klammer wird geschlossen].

3. $T_i = < \varphi_i$ und $T_{z_i} => \varphi_{z_i}$ impliziert, dass es Ausdrücke $\mathcal{X}, \psi \in L^S$, paarweise verschiedene Variablen $x_0, \dots, x_{l-1}$ und paarweise verschiedene Variablen $y_0, \dots, y_{l-1}$ gibt, so dass $\varphi_{z_i} = \mathcal{X}\frac{y_0 \dots y_{l-1}}{x_0 \dots x_{l-1}}$, $\varphi_{i-1} = \psi\frac{y_0 \dots y_{l-1}}{x_0 \dots x_{l-1}}$, $\varphi_i = \forall x_0 \dots \forall x_{l-1}(\mathcal{X} \to \psi)$ und $y_0, \dots, y_{l-1} \notin B_{z_i} \cup \mathrm{Fr}(\mathcal{X}) \cup \mathrm{Fr}(\psi)$.

4. $T_i = < \varphi_i$ und $T_{z_i} =>$ impliziert, dass es einen Ausdruck $\psi \in L^S$, paarweise verschiedene Variablen $x_0, \dots, x_{l-1}$ und paarweise verschiedene Variablen $y_0, \dots, y_{l-1}$ gibt, so dass $\varphi_{i-1} = \psi\frac{y_0 \dots y_{l-1}}{x_0 \dots x_{l-1}}$, $\varphi_i = \forall x_0 \dots \forall x_{l-1}\psi$ und $y_0, \dots, y_{l-1} \notin B_{z_i} \cup \mathrm{Fr}(\psi)$.

$$
\begin{array}{lcll}
Z_i & : & > \mathcal{X}\frac{\vec{y}}{\vec{x}} & > \\
 & & \vdots & \vdots \\
i-1 & : & \psi\frac{\vec{y}}{\vec{x}} & \psi\frac{\vec{y}}{\vec{x}} \\
i & : & < \forall \vec{x}(\mathcal{X} \to \psi) & < \forall \vec{x}\psi
\end{array}
$$

$T_0, \dots, T_{n-1}$ ist ein *Beweis von* φ gdw $T_{n-1} = \varphi$ und $z_{n-1} = -\infty$.

Notation, Beispiel

0 :	$>$
1 :	$> \ v_0 \equiv v_1.$
2 :	$\quad (v_0 \equiv v_3)\frac{v_1}{v_3}$ nach 1.
3 :	$\quad > v_1 \equiv v_2.$
4 :	$\qquad (v_0 \equiv v_3)\frac{v_2}{v_3}$ nach (Sub), 2,3.
5 :	$\qquad v_0 \equiv v_2$ nach 4.
6 :	$\quad < (v_1 \equiv v_2 \to v_0 \equiv v_2)$
7 :	$< (v_0 \equiv v_1 \to (v_1 \equiv v_2 \to v_0 \equiv v_2))$
8 :	$< \forall v_0 \forall v_1 \forall v_2 (v_0 \equiv v_1 \to (v_1 \equiv v_2 \to v_0 \equiv v_2))$
9 :	$\forall v_0 \forall v_1 \forall v_2 (v_0 \equiv v_1 \to (v_1 \equiv v_2 \to v_0 \equiv v_2))$ nach 8.

Das gleiche Beispiel in der Mizar-MSE-Sprache:

```
environ
        reserve x,y,z for set;
begin
        a: now let x,y,z;
                b: now assume b1: x=y;
                        c: now assume c1: y=z;
                        thus x=z by b1,c1;
                        end;
                        thus y=z implies x=z by c;
                end;
                thus x=y implies (y=z implies x=z) by b;
        end;
        for x,y,z holds x=y implies (y=z implies x=z) by a;
```

Dieser Beweis wir von Mizar-MSE als korrekt akzeptiert:

```
!! MIZAR-MSE UNIX version 2.2 Dep of Comp Sci, Univ of Alberta !!
environ
        reserve x,y,z for set;
begin
        a: now let x,y,z;
                b: now assume b1: x=y;
                        c: now assume c1: y=z;
                        thus x=z by b1,c1;
                        end;
                        thus y=z implies x=z by c;
                end;
                thus x=y implies (y=z implies x=z) by b;
        end;
        for x,y,z holds x=y implies (y=z implies x=z) by a;
!!
!! Thanks, OK
!! ----------
```

In dem Mizar-Kalkül kann auch das Behauptung-Beweis-Format benutzt werden, und übliche Abkürzungen sind möglich:

```
environ
        reserve x,y,z for set;
begin

Transitivity: for x,y,z holds x=y implies (y=z implies x=z)

proof
        let x,y,z;
        assume b1: x=y;
        assume c1: y=z;
        thus x=z by b1,c1;
end
```