Bemerkungen zu $\mathcal{P}$

Bezeichnungen

a) B Beweis zu $s = t$ in (E, R).
B' Beweis zu $s = t$ in (E', R').
$\rightsquigarrow$ B, B' heißen **äquivalent**.

b) B kein V-Beweis gdw
B enthält Teilbeweis der Form

$$\underset{\substack{\uparrow \\ \textbf{E-Schritt}}}{t_i \longmapsto\!\!\!\!\dashv\ t_{i+1}} \quad \text{oder} \quad \underset{\substack{\uparrow \\ \textbf{Spitze}\text{ (peak)}}}{t_{i-1} \longleftarrow t_i \longrightarrow t_{i+1}}$$

Ziel

$\mathcal{P}$ bewirkt eine Zustandstransformation $(E_0, R_0), (E_1, R_1), \ldots$ so, dass jeder Beweis B in (E_0, R_0) im „Grenzsystem“ (E^∞, R^∞) einen äquivalenten V-Beweis B' hat.

Definition von $\mathcal{P}$

Definition 3.23 Inferenzsystem $\mathcal{P}$

Sei $\succ$ eine Reduktionsordnung. Das Inferenzsystem $\mathcal{P} = \mathcal{P}_\succ$ besteht aus folgenden Regeln:

(P1) Orientieren:

$$\frac{(E \cup \{s \doteq t\}, R)}{(E, R \cup \{s \to t\})} \quad \text{falls } s \succ t$$

(P2) Generieren:

$$\frac{(E, R)}{(E \cup \{s = t\}, R)} \quad \text{falls } s \ {}_R\!\!\longleftarrow u \longrightarrow_R t$$

(P3) Simplifizieren einer Gleichung:

$$\frac{(E \cup \{s \doteq t\}, R)}{(E \cup \{u = t\}, R)} \quad \text{falls } s \longrightarrow_R u$$

(P4) Löschen:

$$\frac{(E \cup \{s = s\}, R)}{(E, R)}$$

Definition von $\mathcal{P}$ (Forts.)

(P5) Simplifizieren einer rechten Seite:

$$\frac{(E, R \cup \{s \to t\})}{(E, R \cup \{s \to u\})} \quad \text{falls } t \longrightarrow_R u$$

(P6) Simplifizieren einer linken Seite

$$\frac{(E, R \cup \{s \to t\})}{(E \cup \{u = t\}, R)} \quad \begin{array}{l} \text{falls } s \longrightarrow_R u \text{ mit } l \to r \text{ in } R \\ \text{und } s \blacktriangleright l \end{array}$$

Wir schreiben $(E, R) \vdash_{\mathcal{P}} (E', R')$, wenn man (E', R') aus (E, R) in einem Schritt aus $\mathcal{P}$ herleiten kann.

Eigenschaften E_1 und E_2 von $\mathcal{P}$ (1)

1. Ziel

E_1: Erhaltung der Invarianzen.

Lemma 3.14

Sei $\mathcal{P} = \mathcal{P}_{\succ}$. Sei $(E, R) \vdash_{\mathcal{P}} (E', R')$.

a) Gilt $R \subseteq \succ$, so gilt auch $R' \subseteq \succ$.

b) Es gilt $=_{E \cup R} \; = \; =_{E' \cup R'}$.

Beweis: Betrachte die 6 Inferenzregeln einzeln.

2. Ziel

E_2: Verkleinerung von Beweisen.

a) schwache Form $\longrightarrow$ Lemma 3.17 (siehe später)

b) starke Form $\longrightarrow$ Lemma 3.18 (siehe später)

$\Rightarrow$ Wir benötigen Beweisordnungen.

Beweisordnungen

Definition 3.24

Eine Partialordnung $\succ_0$ auf Beweisen ist eine **Beweisordnung**, falls gilt

1. $\succ_0$ ist Noethersch.
2. $\succ_0$ ist verträglich mit Substitutionen

$$B \succ_0 B' \rightsquigarrow \sigma(B) \succ_0 \sigma(B')$$

3. $\succ_0$ ist verträglich mit der Termstruktur

$$B \succ_0 B' \rightsquigarrow B_{t,p} \succ_0 B'_{t,p}$$

4. $\succ_0$ ist verträglich mit der Beweisstruktur

$$B \succ_0 B' \rightsquigarrow B_1 B B_2 \succ_0 B_1 B' B_2$$

Beachte

Sei B Beweis zu $u = v$ in (E, R). Dann gilt:

- $\sigma(B)$ ist Beweis zu $\sigma(u) = \sigma(v)$ in (E, R).
- $B_{t,p}$ ist Beweis zu $t[p \leftarrow u] = t[p \leftarrow v]$ in (E, R).
- $B_1 B B_2$ ist Beweis zu $s = t$ in (E, R),
  falls B_1 Beweis zu $s = u$ in (E, R) ist,
  B_2 Beweis zu $v = t$ in (E, R) ist,
  B Beweis zu $u = v$ in (E, R) ist.

Beweisordnung: Zentrale Eigenschaft

Lemma 3.15

Sei $\succ_0$ eine Beweisordnung.

Zu jedem „elementaren“ Beweis B_0 zu $u = v$ in (E, R) der Form

$u \vdash\!\!\!\longrightarrow\!\!\dashv_E v$	$u = v$ in E
$u \longrightarrow_R v$	$u \to v$ in R
$u \;{}_R\!\longleftarrow w \longrightarrow_R v$	kritsches Tripel in R

gebe es einen Beweis B'_0 zu $u = v$ in (E', R') mit $B_0 \succeq_0 B'_0$.

Dann gibt es zu jedem Beweis B in (E, R) einen äquivalenten Beweis B' in (E', R') mit $B \succeq_0 B'$.

Beachte zu den „elementaren“ B_0 in der Voraussetzung:

- Sie haben eine sehr spezielle Form.
- Jeder Beweis B besteht aus endlich vielen dieser B_0.

Beweisordnung: $\succ_{\mathcal{P}}$

Sei $\succ$ die feste Reduktionsordnung.

Definition 3.25

Sei $B = (t_0, b_1, t_1, \ldots, t_{n-1}, b_n, t_n)$ ein Beweis.

a) Sei c_i das Quadrupel

$$c_i = \begin{cases} (\{t_{i-1}\}, t_{i-1}/p, l, t_i) & t_{i-1} \longrightarrow t_i \;\; b_i = (l \to r, p) \\ (\{t_i\}, t_i/p, l, t_{i-1}) & t_{i-1} \longleftarrow t_i \;\; b_i = (r \leftarrow l, p) \\ (\{t_{i-1}, t_i\}, -, -, -) & t_{i-1} \longmapsto\!\!\!\dashv t_i \;\; b_i = (u = v, p) \end{cases}$$

Dann ist
$c(B) = \{c_1, \ldots, c_n\}$ die **Komplexität von** B.

b) Definiere Ordnung $\succ_q$ auf den Quadrupeln durch

$$c = (A, s, l, t) \succ_q (A', s', l', t') = c'$$

$$\begin{array}{llll} \text{gdw} & A \succ\!\!\succ A' & \text{oder} & \\ & A = A', & s >_{TT} s' & \text{oder} \\ & A = A', & s \equiv s', & l \succ l' \quad \text{oder} \\ & A = A', & s \equiv s', & l \equiv l' \quad t \succ t' \end{array}$$

c) Definiere die **Ordnung** $\succ_{\mathcal{P}}$ auf Beweisen.
$B \succ_{\mathcal{P}} B'$ gdw $c(B) \succ\!\!\succ_q c(B')$
$B \succeq_{\mathcal{P}} B'$ gdw $B \succ_{\mathcal{P}} B' \vee B = B'$

Eigenschaften von $\mathcal{P}$ (2)

Lemma 3.16

$\succ_{\mathcal{P}}$ ist eine Beweisordnung.

Beweis: Nachrechnen.

Lemma 3.17

Sei $(E, R) \vdash (E', R')$ und B ein Beweis zu $s = t$ in (E, R).

Dann gibt es einen Beweis B' zu $s = t$ in (E', R') mit $B \succeq_{\mathcal{P}} B'$.

Gilt $(E, R) \vdash (E', R')$ mit Inferenzregel (2) und Spitze $s \leftarrow u \to t$ und benutzt B diese Spitze, so gilt $B \succ_{\mathcal{P}} B'$.

Beweis:

Ist B auch ein Beweis in (E', R'), so kann man $B' = B$ wählen. Ist dies nicht der Fall, so wurde durch den Inferenzschritt eine Gleichung aus E gerichtet, gelöscht oder simplifiziert oder eine Regel aus R simplifiziert, die in E angewandt wurde. Wir zeigen, dass dies zu einem Beweis B' mit $B \succ_{\mathcal{P}} B'$ führt.

Idee: Wegen Lemma 3.15 reicht es zu zeigen, dass die Behauptung für die „elementaren" Beweise gilt. Wir betrachten die Inferenz-Regeln von $\mathcal{P}$ einzeln.

Beachte: $\succ_q$ ist auf 4 Tupeln definiert.

Beweis zu Lemma 3.17

(P1) Orientieren
$B = s \vdash\!\!\dashv t \succ_{\mathcal{P}} B' = s \longrightarrow t$
1. Komponente verkleinert: $\{s, t\} \succ\!\!\succ \{s\}$

(P2) Generieren
$B = s \longleftarrow u \longrightarrow t \succ_{\mathcal{P}} B' = s \vdash\!\!\dashv t$
1. Komponente verkleinert: $\{u\} \succ\!\!\succ \{s, t\}$

(P3) Simplifizieren einer Gleichung
$B = s \vdash\!\!\dashv t \succ_{\mathcal{P}} B' = s \longrightarrow u \vdash\!\!\dashv t$
1. Komponente verkleinert: $\{s, t\} \succ\!\!\succ \{s\}, \{u, t\}$

(P4) Löschen
$B = s \vdash\!\!\dashv s \succ_{\mathcal{P}} B' =$ leer

(P5) Simplifizieren rechte Seite
$B = s \longrightarrow t \succ_{\mathcal{P}} B' = s \longrightarrow u \longleftarrow t$
$c(s \longrightarrow t) \succ_{\mathcal{P}} c(s \longrightarrow u)$ 4. Komponente.
$c(s \longrightarrow t) \succ_{\mathcal{P}} c(u \longleftarrow t)$ 1. Komponente.

(P6) Simplifizieren linke Seite
$B = s \longrightarrow t \succ_{\mathcal{P}} B' = s \longrightarrow u \vdash\!\!\dashv t$
Alle Komponenten von $\succ_q$ benötigt.

Fairness

Motivation

Eine Strategie zur Anwendung der Inferenz-Regeln heißt **fair**, falls keine Inferenz unendlich lange warten muss.

Definition 3.26

Sei $(E_i, R_i)_{i \in \mathbb{N}}$ eine $\mathcal{P}$-Ableitung.

$$E^\infty = \bigcup_{i \geq 0} \bigcap_{j \geq i} E_j \qquad R^\infty = \bigcup_{i \geq 0} \bigcap_{j \geq i} R_j$$

Die $\mathcal{P}$-Ableitung ist **fair**, falls gilt:

(1) $CP(R^\infty) \subseteq \bigcup_{i \geq 0} E_i$ und

(2) $E^\infty = \varnothing$

Vervollständigungsalgorithmen

Definition 3.27

Ein Algorithmus $\mathcal{A}$, der auf Zuständen (E_i, R_i) arbeitet, heißt ein $\mathcal{P}$-**Vervollständigungsverfahren**, falls gilt

a) $\mathcal{A}$ macht nur $\mathcal{P}$-Inferenzen.

b) $\mathcal{A}$ erzeugt nur faire $\mathcal{P}$-Ableitungen.

Eingabe:	$(E, \succ)$
Start:	$(E_0, R_0) = (E, \emptyset)$
Ausgabe:	$(E_n, R_n) = (\emptyset, R)$ oder
	(E^∞, R^∞), falls $\mathcal{A}$ nicht hält.

Beachte

Erlaubt man zusätzlich

c) $\mathcal{A}$ fügt Gleichung $u = v$ mit $u =_E v$ ein,
so bleiben alle Ergebnisse erhalten.

Denn: Dies verkleinert Beweise schwach.

Eigenschaften von $\mathcal{P}$ (3)

Lemma 3.18

Sei $(E_i, R_i)_{i \in \mathbb{N}}$ eine faire $\mathcal{P}$-Ableitung.
Zu jedem Beweis B zu $u = v$ in (E_i, R_i), der kein V-Beweis ist, gibt es $j \geq i$ und Beweis B' zu $u = v$ in (E_j, R_j) mit $B \succ_{\mathcal{P}} B'$.

Beweis-Idee:

Jeder $\mathcal{P}$-Inferenz-Schritt verkleinert B schwach.

Jeder E-Schritt und jede Spitze wird (wegen der Fairness) einmal bearbeitet. Dies verkleinert B echt.