3.2 All-quantifizierte Ziele

Problem

Gegeben: $Ax = \{s_i = t_i \mid i = 1, \dots, n\}$ $s_i, t_i \in \mathsf{Term}(F, V)$
$u = v$ $u, v \in \mathsf{Term}(F)$
Frage: Wie zeigt man $u =_{Ax} v$?

Beachte

a) Sei $\longrightarrow$ grundkonvergent auf $\mathsf{Term}(F)$ und $=_{Ax} = \stackrel{*}{\longleftrightarrow}$ auf $\mathsf{Term}(F)$. Dann gilt $u =_{Ax} v$ gdw $u \downarrow v$.
b) Die Vervollständigung von Ax liefert ein konvergentes $\longrightarrow$, es reicht aber die Grundkonvergenz.
c) Die Vervollständigung kann divergieren oder abbrechen.
Wie vermeidet man dies?

Beispiel

Sei $F = \{0, s, +\}$ und

$$\begin{aligned} R : & x + 0 \rightarrow x \\ & x + s(y) \rightarrow s(x + y) \\ & (x + y) + z \rightarrow x + (y + z) \end{aligned}$$

Dann ist R grundkonfluent, aber nicht konfluent.

Bezeichnungen

$s = t$ ist eine **Gleichung**.

$s \rightarrow t$ ist eine **Regel**.

$s \doteq t$ steht für $s = t$ oder $t = s$.

$t[u]_\pi$ steht für $t[\pi \leftarrow u]$ mit $\pi \in \mathsf{Pos}(t)$.

$\longrightarrow$ ist eine **Reduktionsrelation** auf $\mathsf{Term}(F, V)$, falls $u \longrightarrow v$ impliziert $\sigma(u) \longrightarrow \sigma(v)$ und $t[u]_\pi \longrightarrow t[v]_\pi$.

Eine Ordnung $\succ$ auf $\mathsf{Term}(F, V)$ ist eine **Reduktionsordnung**, falls sie eine Noethersche Reduktionsrelation ist.

Sie ist eine **Grund-Reduktionsordnung**, falls sie total auf $\mathsf{Term}(F)$ ist.

$>_{TT}$ ist die **Teiltermordnung**.

$s \rhd t$ gdw es gibt σ mit $s >_{TT} \sigma(t)$ oder $s \equiv \sigma(t)$, aber s und t sind nicht gleich bis auf Variablenumbenennung.

Beachte

Jede LPO und jede KBO mit totaler Präzedenz ist eine Grund-Reduktionsordnung.

Behandlung von unrichtbaren Gleichungen

Sei $\succ$ eine Reduktionsordnung.
R ein Regelsystem mit $R \subseteq \succ$.
E ein Gleichungssystem.

Intention

Richtbare Instanzen von Gleichungen $u = v$ in E kann man zum Simplifizieren benutzen.

Gleichungen können auf Term(F) zu lokalen Divergenzen führen. Diese müssen durch kritische Paare überdeckt werden.

Bezeichnung

$E^{\succ} = \{\sigma(u) \to \sigma(v) \mid u \doteq v \text{ in } E, \sigma(u) \succ \sigma(v)\}$

$R(E) = R \cup E^{\succ}$

Definition 3.2.

Seien $u = v$ und $l = r$ zwei Gleichungen. Sei $\pi \in$ Pos(l), $l/\pi \notin V$ und $\sigma =$ mgu$(u, l/\pi)$. Dann ist

$$\langle \sigma(r), \sigma(l)[\sigma(v)]_\pi \rangle$$

ein **kritisches Paar**, falls $\sigma(r) \not\succ \sigma(l) \not\prec \sigma(l)[\sigma(v)]_\pi$.

Sei CP(R, E) die Menge aller kritischen Paare zu Gleichungen aus $R \cup E$.

Bemerkungen zu kritischen Paaren

Sei $\longrightarrow \; = \; \longrightarrow_{R(E)}$.

1. Bemerkung

Sei $t_1 \longleftarrow t \longrightarrow t_2$ mit $t, t_1, t_2 \in$ Term(F) eine echte Überlappung

und $t \longrightarrow t_1$ mit $l = r$, τ bei $\pi' = \lambda$, $t/\lambda \equiv \tau(l) \succ \tau(r)$
$t \longrightarrow t_2$ mit $u = v$, τ bei $\pi' = \pi$, $t/\pi \equiv \tau(u) \succ \tau(v)$

Dann ist $\langle t_1, t_2 \rangle$ eine Instanz des kritischen Paares $\langle \sigma(r), \sigma(l)[\sigma(v)]_\pi \rangle$ zu $u = v$ und $l = r$. Die kritischen Paare überdecken also die echten Überlappungen auf Term(F).

2. Bemerkung

Es gilt $s \not\succ t$ gdw ($t \succ s$ oder $s \equiv t$ oder
s, t sind $\succ$-unvergleichbar).

3. Bemerkung (zu den kritischen Paaren)

Ist $l \succ r$, so ist $\sigma(l) \succ \sigma(r)$, also $\sigma(r) \not\succ \sigma(l)$.

Ist $u \succ v$, so ist $\sigma(l) \equiv \sigma(l)[\sigma(u)]_\pi \succ \sigma(l)[\sigma(v)]_\pi$.

Also: Ist $E = \emptyset$, so stimmt CP(R, E) mit der klassischen Menge CP(R) überein.

Das Inferenzsystem $\mathcal{U}$: Motivation

Idee

Das Inferenzsystem für die KB-Vervollständigung so modifizieren, dass sie nicht abbricht.

Dies liefert UKB (unfailing KB-completion).

Dazu bei Eingabe Ax:

Die richtbaren Gleichungen in R speichern.

Die unrichtbaren Gleichungen in E speichern.

Simplifizieren mit $R(E) = R \cup E^{\succ}$.

Kritische Paare mit R und E bilden: CP(R, E).

Beachte

Dies vermeidet den Abbruch der Vervollständigung, nicht aber die Divergenz.

Beweistechnik für die Vollständigkeit und Korrektheit: Ansatz der Beweisverkleinerung (auf Grundbeweisen).

Das Inferenzsystem $\mathcal{U}$: Definition

Definition 3.3.

Sei $\succ$ eine Grund-Reduktionsordnung.

$\mathcal{U} = \mathcal{U}_{\succ}$ besteht aus folgenden Regeln:

1. Richten einer Gleichung
   $(R, E \cup \{s \doteq t\}) \vdash (R \cup \{s \rightarrow t\}, E)$
   falls $s \succ t$

2. Erzeugen einer neuen Gleichung
   $(R, E) \vdash (R, E \cup \{s = t\})$
   falls $s \longleftarrow_{R \cup E} u \longrightarrow_{R \cup E} t$ und $s \not\succ u$ und $t \not\succ u$

3. Simplifizieren einer Gleichung
   $(R, E \cup \{s = t\}) \vdash (R, E \cup \{u = t\})$
   falls
   - $s \longrightarrow_R u$,
   - $s \longrightarrow_{E^{\succ}} u$ mit $l = r \in E$ und $s \rhd l$ oder
   - $s \longrightarrow_{R(E)} u$ und $t \succ s$

Das Inferenzsystem $\mathcal{U}$: Definition (Forts.)

4. Löschen einer trivialen Gleichung
   $(R, E \cup \{s = s\}) \vdash (R, E)$

5. Subsumieren einer Gleichung
   $(R, E \cup \{s = t\}) \vdash (R, E)$
   falls $s \vdash\!\dashv_E t$

6. Simplifizieren einer Regel rechts
   $(R \cup \{s \to t\}, E) \vdash (R \cup \{s \to u\}, E)$
   falls $t \longrightarrow_{R(E)} u$

7. Simplifizieren einer Regel links
   $(R \cup \{s \to t\}, E) \vdash (R, E \cup \{u = t\})$
   falls $s \longrightarrow_{R(E)} u$ mit $l \to r$ und $s \rhd l$

Bemerkungen zu $\mathcal{U}$

Bemerkung

Regel (2) wird nur angewendet mit $\langle s, t\rangle \in \mathrm{CP}(R, E)$.

Eine $\mathcal{U}$-**Ableitung** (für E) ist eine Folge $(R_i, E_i)_{i\in\mathbb{N}}$ mit $(R_i, E_i) \vdash (R_{i+1}, E_{i+1})$ und $(R_0, E_0) = (\emptyset, E)$.

Lemma 3.1

Sei $(R_i, E_i)_{i\in\mathbb{N}}$ eine $\mathcal{U}$-Ableitung für E. Dann gilt

a) $R_i \subseteq \succ$.

b) $=_E \;=\; =_{R_i \cup E_i}$ auf $\mathrm{Term}(F, V)$.

Ziel (+)

Sei $\longrightarrow_i \;=\; \longrightarrow_{R_i(E_i)}$.

Für eine „faire“ $\mathcal{U}$-Ableitung $(R_i, E_i)_{i\in\mathbb{N}}$ gilt

$u =_E v \text{ gdw } \exists i \in \mathbb{N} : u \downarrow_i v$

Bemerkung

Dies gilt. Beweis hierzu später.

Zunächst: Verfeinerung des Ansatzes.

Beispiel

Problem

Ax: $x + y = y + x \qquad (x + y) + z = x + (y + z)$

Ziel: Zeige $(a + b) + (a + c) =_{Ax} a + (a + (b + c))$

Sei

$t_1 + t_2 + \cdots + t_n \equiv t_1 + (t_2 + \cdots + (t_{n-1} + t_n) \ldots)$

$\succ$ die LPO zur Präzedenz $+ >_F a >_F b >_F c$.

Dann

$\mathcal{U}$ divergiert mit Eingabe Ax, und es wird für fast jede Permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ die folgende Gleichung erzeugt

$$x_1 + x_2 + \cdots + x_n = x_{\pi(1)} + x_{\pi(2)} + \cdots + x_{\pi(n)}$$

Das sind sehr viele Gleichungen. Wir zeigen, dass sie fast alle redundant sind.

Beispiel (Forts.)

Anfang der Vervollständigung mit $\mathcal{U}$ liefert

$R : (x + y) + z \to x + (y + z)$
$E : x + y = y + x$
$\quad x + (y + z) = y + (x + z)$

Dies System ist bereits grundkonvergent auf Term(F).

Es gilt z. B. mit $\longrightarrow \; = \; \longrightarrow_{R(E)}$

$$\begin{array}{ll}
(a + b) + (a + c) & \longrightarrow a + (b + (a + c)) \longrightarrow b + (a + (a + c)) \\
& \longrightarrow b + (a + (c + a)) \longrightarrow b + (c + (a + a)) \\
& \longrightarrow c + (b + (a + a)) \\
a + (a + (b + c)) & \overset{*}{\longrightarrow} c + (b + (a + a))
\end{array}$$

Also gilt $(a + b) + (a + c) =_{Ax} a + (a + (b + c))$.

Redundanz-Elimination

Bemerkung

Das Inferenzsystem $\mathcal{U}$ erzeugt viele „unnötige“ Gleichungen. Sie verursachen einerseits Arbeit, helfen aber andererseits beim Simplifizieren (Säubern der Datenbasis).

Fragen

1. Was heißt „unnötig“?
2. Wie erkennt man unnötige Gleichungen?
3. Kann man sie zum Simplifizieren verwenden, ohne mit ihnen kritische Paare zu bilden?

Ansatz

Beweistechnik für das Ziel $(+)$: Verkleinerung von Grundbeweisen.

Also: $s = t$ heißt **unnötig** in (R, E), falls es für jede Grundinstanz $\sigma(s) = \sigma(t)$ in (R, E) einen kleineren Beweis gibt als den 1-Schritt-Beweis mit $s = t$.

Ziel

Antwort JA auf Frage 3.

Eine Beweisordnung (1)

Sei $\succ$ eine Grundreduktionsordnung.

Bemerkung

Wir arbeiten mit Tripeln (R, E, G)

R enthält die gerichteten Gleichungen, also $R \subseteq \succ$.
E enthält die ungerichteten Gleichungen.
G enthält die redundanten Gleichungen.

Definition 3.4.

Ein **Grundbeweis** zu $s = t$ in (R, E, G) hat die Form

$$P = (t_0, \varrho_1, t_1, \ldots, \varrho_n, t_n)$$

mit $t_i \in \text{Term}(F)$, $t_0 \equiv s$, $t_n \equiv t$ und $t_{i-1} \varrho_i t_i$
mit
$\varrho_i \in \{\longrightarrow_R, \longleftarrow_R, \longrightarrow_{E^\succ}, \longleftarrow_{E^\succ}, \vdash\!\dashv_E, \longrightarrow_{G^\succ}, \longleftarrow_{G^\succ}, \vdash\!\dashv_G\}$.

Beachte

$\succ$ ist total auf $\text{Term}(F)$.
Also gilt für alle $t_i, t_{i+1} \in \text{Term}(F)$:
$t_i \succ t_{i+1}$, $t_i \equiv t_{i+1}$ oder $t_{i+1} \succ t_i$.

Eine Beweisordnung (2)

Definition 3.5.

Die Komplexität eines Beweisschritts $s\varrho t$ ist

$$c(s\varrho t) = \begin{cases} (\{s\}, l, \{t\}) & \text{falls } s \longrightarrow_R t \text{ mit } l \to r \\ (\{t\}, l, \{s\}) & \text{falls } s \longleftarrow_R t \text{ mit } l \to r \\ (\{s\}, l, \{t, \max\}) & \text{falls } s \longrightarrow_{(E\cup G)^{\succ}} t \text{ mit } l = r \\ (\{t\}, l, \{s, \max\}) & \text{falls } s \longleftarrow_{(E\cup G)^{\succ}} t \text{ mit } l = r \\ (\{s, t\}, -, -) & \text{falls } s \vdash\!\dashv_{E\cup G} t \end{cases}$$

Dabei ist $\max$ ein neues Symbol mit $\max \succ t$ für alle $t \in$ Term(F).

Die Ordnung $\succ_t$ auf den Tripeln $c(s\varrho t)$ ist die lexikographische Kombination $\succ_t = (\succ\!\!\succ, \rhd, \succ\!\!\succ)$. Hier ist $\succ\!\!\succ$ die Multimengenerweiterung der festen Grundreduktionsordnung $\succ$.

Die Komplexität eines Beweises $P = (t_0, \varrho_1, t_1, \ldots, \varrho_n, t_n)$ ist

$$c(P) = \{c(t_{i-1}\varrho_i t_i) \mid i = 1, \ldots, n\}$$

Die Beweisordnung $\succ_{\mathcal{P}}$ ist

$$P \succ_{\mathcal{P}} P' \text{ gdw } c(P) \succ\!\!\succ_t c(P')$$

Präzisierung der Redundanz

Definition 3.6.

$s = t$ heißt in (R, E) **redundant**, falls für jede Grundsubstitution σ gilt:

i) $\sigma(s) \equiv \sigma(t)$ oder
ii) es gibt Beweis P zu $\sigma(s) = \sigma(t)$ in (R, E) mit
$\sigma(s) \longrightarrow_{\{s=t\}^{\succ}} \sigma(t) \succ_{\mathcal{P}} P$ oder
$\sigma(t) \longrightarrow_{\{s=t\}^{\succ}} \sigma(s) \succ_{\mathcal{P}} P$

Schreibweise $s = t \succ_{\mathcal{P}} R(E)$.

Lemma 3.2

Sei $s = t \succ_{\mathcal{P}} R(E \cup \{s = t\})$.
Dann gibt es zu jedem Grundbeweis $\sigma(s)\varrho\sigma(t)$ einen echt kleineren Grundbeweis ohne Schritte mit $s = t$.
Insbesondere folgt $s = t \succ_{\mathcal{P}} R(E)$.

Also

Sei $E' = E \cup \{s = t\}$. Aus $s = t \succ_{\mathcal{P}} R(E')$ folgt $=_{R\cup E'} = =_{R\cup E}$ auf den Grundtermen Term(F).

Die Elimination einer redundanten Gleichung ist semantisch korrekt (ändert nicht die Gleichheit auf Grundtermen).

Beweis zu Lemma 3.2

Sei $E' = E \cup \{s = t\}$, $\sigma \in \mathsf{GSub}(s = t)$.

Nach Voraussetzung gibt es einen Beweis P in (R, E') mit $\sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P$.

Wir zeigen durch Induktion nach $\succ_{\mathcal{P}}$, dass es solch einen Beweis in (R, E) gibt:

Sei $\sigma'(s)\varrho'\sigma'(t)$ ein Beweisschritt in P.

Also $\sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P \succeq_{\mathcal{P}} \sigma'(s)\varrho'\sigma'(t)$.

Also gibt es (nach IV) P' in (R, E) zu $\sigma'(s)\varrho'\sigma'(t)$ mit $\sigma'(s)\varrho'\sigma'(t) \succ_{\mathcal{P}} P'$.

Ersetze alle $\sigma'(s)\varrho'\sigma'(t)$ in P durch die P'.

Es entsteht P_0 zu $\sigma(s)\varrho\sigma(t)$ in (R, E) mit

$$\sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P \succeq_{\mathcal{P}} P_0\ .$$

Nach Definition 3.6 folgt $s = t \succ_{\mathcal{P}} R(E)$.

Das Inferenzsystem $\mathcal{G}$

Definition 3.7.

Das Inferenzsystem $\mathcal{G}$ besteht aus folgenden Regeln.

1. Richten einer Gleichung
   $(R, E \cup \{s \doteq t\}, G) \vdash (R \cup \{s \to t\}, E, G)$
   falls $s \succ t$

2. Erzeugen einer neuen Gleichung
   $(R, E, G) \vdash (R, E \cup \{s = t\}, G)$
   falls $s \longleftrightarrow_{R\cup E} u \longleftrightarrow_{R\cup E} t$ und $s \not\succ u$ und $t \not\succ u$

3. Simplifizieren einer Gleichung
   $(R, E \cup \{s \doteq t\}, G) \vdash (R, E \cup \{u = t\}, G)$
   falls
   - $s \longrightarrow_R u$ oder
   - $s \longrightarrow_{(E\cup G)^{\succ}} u$ mit $l = r \in E \cup G$ und $s \rhd l$ oder
   - $s \longrightarrow_{R(E\cup G)} u$ und $t \succ s$

4. Löschen einer trivialen Gleichung
   $(R, E \cup \{s = s\}, G) \vdash (R, E, G)$

5. Subsumieren einer Gleichung
   $(R, E \cup \{s = t\}, G) \vdash (R, E, G)$
   falls $s \vdash\!\dashv_{E\cup G}\, t$

Das Inferenzsystem $\mathcal{G}$ (Forts.)

6. Verschieben einer redundanten Gleichung von E nach G
   $(R, E \cup \{s = t\}, G) \vdash (R, E, G \cup \{s = t\})$
   falls $s = t \succ_{\mathcal{P}} R(E \cup G)$

7. Simplifizieren einer Regel rechts
   $(R \cup \{s \to t\}, E, G) \vdash (R \cup \{s \to u\}, E, G)$
   falls $t \longrightarrow_{R(E \cup G)} u$

8. Simplifizieren einer Regel links
   $(R \cup \{s \to t\}, E, G) \vdash (R, E \cup \{u = t\}, G)$
   falls $s \longrightarrow_{R(E \cup G)} u$ mit $l = r$ und $s \rhd l$

Bezeichnung

Wir schreiben $(R, E, G) \vdash (R', E', G')$, falls (R', E', G') mit $\mathcal{G}$ aus (R, E, G) in einem Schritt hergeleitet werden kann.

Eine $\mathcal{G}$-**Ableitung** ist eine Folge $(R_i, E_i, G_i)_{i \in \mathbb{N}}$ mit $(R_i, E_i, G_i) \vdash (R_{i+1}, E_{i+1}, G_{i+1})$ für alle $i \geq 0$. Es ist eine $\mathcal{G}$-**Ableitung für** E, falls $(R_0, E_0, G_0) = (\varnothing, E, \varnothing)$.

Ergebnisse zu $\mathcal{G}$ (1)

Sei $(R_i, E_i, G_i)_{i \in \mathbb{N}}$ eine $\mathcal{G}$-Ableitung zur Eingabe E.

Der Korrektheits- und Vollständigkeitsbeweis zu $\mathcal{G}$ läuft parallel zu dem für die normale KB-Vervollständigung.

$\mathcal{G}$ ist korrekt:

Lemma 3.3

a) $R_i \subseteq \succ$
b) $=_E \; = \; =_{R_i \cup E_i \cup G_i}$ auf Term(F, V).

$\mathcal{G}$ verkleinert Grundbeweise schwach:

Lemma 3.4

Zu jedem Grundbeweis P zu $u = v$ in (R_i, E_i, G_i) gibt es einen Grundbeweis P' zu $u = v$ in $(R_{i+1}, E_{i+1}, G_{i+1})$ mit $P \succeq_{\mathcal{P}} P'$.

Die Gleichungen in G_i sind redundant:

Lemma 3.5

Für alle $s = t$ in G_i gilt $s = t \succ_{\mathcal{P}} R_i(E_i)$.

Beweis zu Lemma 3.5

Sei $\mathbf{P}$ die Menge aller Grundbeweise in (R_i, E_i, G_i). Mit Induktion nach $\succ_{\mathcal{P}}$ zeigen wir:

> Für jeden Grundbeweis $P \in \mathbf{P}$ gibt es einen Grundbeweis P' in $(R_i, E_i, \emptyset)$ mit $P \succeq_{\mathcal{P}} P'$. Wird in P eine Gleichung aus G_i benutzt, gilt sogar $P \succ_{\mathcal{P}} P'$.

Wird in P keine Gleichung aus G_i benutzt, kann man $P' = P$ wählen.

Sei $\sigma(s)\varrho\sigma(t)$ ein Beweisschritt in P mit $s = t$ in G_i.

Es sei j der Zeitpunkt, zu dem $s = t$ (mit Regel 6) von E nach G verschoben wurde. Es gibt dann in (R_j, E_j, G_j) einen Grundbeweis P_0 für $\sigma(s) = \sigma(t)$, der kleiner als $\sigma(s)\varrho\sigma(t)$ ist.

Also $P \succeq_{\mathcal{P}} \sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P_0$.

Also gibt es (nach Lemma 3.4) P_1 in (R_i, E_i, G_i) zu $\sigma(s)\varrho\sigma(t)$ mit $P_0 \succeq_{\mathcal{P}} P_1$.

Es ist $P \succ_{\mathcal{P}} P_1$, also gibt es zu P_1 nach IV einen Grundbeweis P_1', der keine G_i-Schritte enthält, mit $\sigma(s)\varrho\sigma(t) \succ_{\mathcal{P}} P_1 \succeq_{\mathcal{P}} P_1'$.

Ersetze so alle Beweisschritte der Art $\sigma(s)\varrho\sigma(t)$ in P durch solche P_1'.

Es entsteht P' zu P in $(R_i, E_i, \emptyset)$ mit $P \succeq_{\mathcal{P}} P'$. Wird mindestens ein G_i-Schritt ersetzt, gilt sogar $P \succ_{\mathcal{P}} P'$.

Daraus folgt die Behauptung.

Ergebnisse zu $\mathcal{G}$ (2)

Beachte

a) Gleichungen in G werden nie simplifiziert. Sie dienen aber zum Simplifizieren.

b) Lemma 3.5 ist das zentrale Resultat über die Redundanz. Es bricht den Zykel: $s = t$ in G simplifiziert die Regel $l \longrightarrow r$, die benutzt wurde, um $s = t$ von E nach G zu verschieben.

Folgerung

Sei $u =_E v$ eine Grundgleichung. Es gibt Beweise $(P_i)_{i\in\mathbb{N}}$ zu $u = v$ in $(R_i, E_i, \emptyset)$ mit $P_i \succeq_{\mathcal{P}} P_{i+1}$.

Also gilt auch $=_E \; = \; =_{R_i \cup E_i}$ auf den Grundtermen.

Ziel

Unter einer Fairnessbedingung der $\mathcal{G}$-Ableitung verkleinert $\mathcal{G}$ die Grundbeweise echt.