Erweiterungsregeln (2)

Definition 4.17

Seien $l \to r$ in R und $v = w$ in A Variablen-disjunkt.
$p \in O(v) \quad v/p \notin V$
$l, v/p$ A-unifizierbar.
Dann ist $v[p \leftarrow l] \to v[p \leftarrow r]$ die **Erweiterungsregel** zu $l \to r$, $v = w$, p.

$EXT_A(R)$ ist die Menge aller Erweiterungsregeln zu R und A.

Beachte

1. Nur Test auf „A-unifizierbar“ nötig, keine Berechnung von vollständiger Menge Σ von A-Unifikatoren.
2. Es gilt $v[p \leftarrow l] =_R v[p \leftarrow r]$
   „Die Regel ist gültig“.
3. Die Erweiterungsregel führt alle kritischen Paare zu $(l \to r, w = v, p)$ zusammen:

$$\begin{tikzcd} \sigma(v) \arrow[d, "A"'] & =_A & \sigma(v[p \leftarrow l]) \arrow[d, "l \to r"] \\ \sigma(w) \arrow[rr, "R.A"] & & \sigma(v[p \leftarrow r]) \end{tikzcd}$$

   denn $\sigma(w) =_A \sigma(v) =_A \sigma(v[p \leftarrow l]) \longrightarrow \sigma(v[p \leftarrow r])$.

Das Inferenzsystem $\mathcal{A}$

Ziel Transformation $(E, A) \leadsto (R, A)$ mit

- $R.A$ ist CR modulo A.
- $=_{R \cup A} \; = \; =_{E \cup A}$

Sei

A festes Gleichungssystem.
$\succ$ A-verträgliche Reduktionsordnung.

Ansatz

$\mathcal{A}$ arbeitet auf Tripeln (Zuständen) (E, N, S)
mit $R = N \cup S \subseteq \succ$,
S geschützte Regeln,
N nicht-geschützte Regeln.

Startzustand zur Eingabe $(E, A, \succ)$:
$(E_0, N_0, S_0) = (E, \varnothing, \varnothing)$

Das Inferenzsystem $\mathcal{A}$

Das Inferenzsystem $\mathcal{A} = \mathcal{A}_{A,\succ}$ besteht aus folgenden Regeln:

(A1) Generieren:

$$\frac{(E, N, S)}{(E \cup \{s = t\}, N, S)} \quad \text{falls } s \;{}_{R \cup A}\!\longleftarrow u \longrightarrow_{R.A} t$$

(A2) Erweitern:

$$\frac{(E, N, S)}{(E, N, S \cup \{l \to r\})} \quad \text{falls } l \to r \text{ in } EXT_A(R)$$

(A3) Orientieren:

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

(A4) Schützen:

$$\frac{(E, N \cup \{s \to t\}, S)}{(E, N, S \cup \{s \to t\})}$$

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

(A5) Löschen:

$$\frac{(E \cup \{s \doteq t\}, N, S)}{(E, N, S)} \quad \text{falls } s \stackrel{*}{\longleftrightarrow}_A t$$

(A6) Simplifizieren einer Gleichung:

$$\frac{(E \cup \{s \doteq t\}, N, S)}{(E \cup \{u = t\}, N, S)} \quad \text{falls } s \longrightarrow_{R/A} u$$

(A7) Simplifizieren einer rechten Seite:

$$\frac{(E, N \cup \{s \to t\}, S)}{(E, N \cup \{s \to u\}, S)} \quad \text{falls } t \longrightarrow_{R/A} u$$

$$\frac{(E, N, S \cup \{s \to t\})}{(E, N, S \cup \{s \to u\})} \quad \text{falls } t \longrightarrow_{R/A} u$$

(A8) Simplifizieren einer linken Seite:

$$\frac{(E, N \cup \{s \to t\}, S)}{(E \cup \{u = t\}, N, S)} \quad \begin{array}{l}\text{falls } s \longrightarrow_{R.A} u \\ \text{mit } l \to r \text{ und } s \rhd l\end{array}$$

$\rhd$ ist eine beliebige Noethersche Partialordnung.

Beweisordnung für $\mathcal{A}$

Definition 4.18

Ein **Beweis** zu $s = t$ in (E, N, S) ist

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

mit $s \equiv t_0, t \equiv t_n, t_{i-1} *_i t_i$
$*_i \in \{\longleftrightarrow_E, \longleftrightarrow_A, \longrightarrow_N, {}_N\longleftarrow, \longrightarrow_S, {}_S\longleftarrow\}$
$b_i = (u_i = v_i, p_i, *_i, \beta_i)$

Sei β_i geeignet aus $\{0, 1, 2\}$ (s. Buch).

Beweisordnung $\succ_{\mathcal{A}}$ (zu $\succ, A$)

Definition 4.19

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

a) Definiere $c_i = c(t_{i-1}, b_i, t_i)$ geeignet als 5-Tupel (s. Buch), $c(B) = \{c_1, \ldots, c_n\}$.
b) Definiere Ordnung $\succ_q$ auf 5-Tupeln
$\succ_q = (\succ\!\succ, \rhd, >_{\mathbb{N}}, >_{\mathbb{N}}, \succ)$
c) $B \succ_{\mathcal{A}} B'$ gdw $c(B) \succ\!\succ_q c(B')$

Definition 4.20

Ein **V-Beweis modulo** A hat die Form:
$s \xrightarrow{*}_{R.A} s_0 =_A t_0 \ {}_{R.A}\xleftarrow{*} t.$

Ergebnis zu $\mathcal{A}$

Definition 4.21

Eine $\mathcal{A}$-Ableitung $(E_i, N_i, S_i)_{i \in \mathbb{N}}$ heißt **fair**, falls gilt

(1) $E^\infty = \varnothing$
(2) $CP_A(R^\infty) \subseteq \bigcup_{i \geq 0} E_i$
(3) $EXT_A(R^\infty) \subseteq \bigcup_{i \geq 0} S_i$

Lemma 4.11

a) Die Inferenzregeln von $\mathcal{A}$ sind korrekt.
b) $\mathcal{A}$ ist bei Einhaltung der Fairness stark Beweis-verkleinernd.

Satz 4.8.

Gegeben sei ein $\mathcal{A}$-faires Vervollständigungsverfahren.
Es breche bei Eingabe von $(E, A, \succ, \rhd)$ nicht ab und liefere das Grenzsystem $R = R^\infty$. Dann gilt $=_{E \cup A} = =_{R \cup A}$ und $R.A$ ist konvergent modulo A.

Probleme mit Erweiterungsregeln (1)

Erinnerung: Für die $\mathcal{A}$-Fairness muss man:

1. Alle Gleichungen in den E_i behandeln.
2. Zu allen persistenten Regeln die kritischen Paare bilden.
3. Zu allen persistenten Regeln die Erweiterungsregeln bilden.

Problem: Divergenz wegen 3.

Beispiel

R: $f(x) + f(y) \to f(x+y)$

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

$\succ$: Polynomordnung mit $\varphi(f)(x) = x+1$, $\varphi(+)(x,y) = x+y$

$\rightsquigarrow \quad (f(x)+f(y))+z_1 \to f(x+y)+z_1$

$\rightsquigarrow \quad ((f(x)+f(y))+z_1)+z_2 \to (f(x+y)+z_1)+z_2$

$\rightsquigarrow \quad (((f(x)+f(y))+z_1)+z_2)+z_3 \to ((f(x+y)+z_1)+z_2)+z_3$

Probleme mit Erweiterungsregeln (2)

Problem allgemeiner

$R : f(s,t) \to u \qquad A : f(f(x,y),z) = f(x,f(y,z))$

Dies führt schon zur Divergenz.

Lösungsidee

Erweiterungsregeln zu Erweiterungsregeln sind unnötig.

(manchmal, z. B. im AC-Fall)

Voraussetzung ab jetzt:

A ist Menge von AC-Axiomen:

$$A : f(f(x,y),z) = f(x,f(y,z))$$
$$f(x,y) = f(y,x) \quad f \in F_{\mathrm{AC}} \subseteq F$$

Also $l \to r$ mit $l \equiv f(s,t)$ liefert

a) mit Kommutativität $l \to r$
b) mit Assoziativität $f(l,z) \to f(r,z)$
$f(x,l) \to f(x,r)$

als Erweiterungsregeln. Beachte, dass die 2 Regeln unter b) äquivalent sind, also eine davon weggelassen werden kann.

Erweitertes Regelsystem zu R (1)

Sei $\quad \overset{\circ}{\longrightarrow}_{R/A} = \longrightarrow_{R/A} \cup =_A$

(also $s \overset{\circ}{\longrightarrow}_{R/A} t$ gdw $s \longrightarrow_{R/A} t$ oder $s =_A t$

und $s \overset{*\,\circ}{\longrightarrow}_{R/A}$ gdw $s \overset{*}{\longrightarrow}_{R/A} t$ oder $s =_A t$).

Definition 4.22

Sei $l \to r$ in R, $l \equiv f(s,t)$, $f \in F_{\mathsf{AC}}$.

Die Erweiterungsregeln $f(l,x) \to f(r,x)$ ist **überflüssig in** R, falls es $u \to v$ in R und σ gibt mit $f(l,x) =_A \sigma(u)$ und $f(r,x) \overset{*\,\circ}{\longrightarrow}_{R/A} \sigma(v)$.

Dann ist

$$f(l,x) \longrightarrow_{R/A} \sigma(v) \ {}_{R/A}\overset{\circ\,*}{\longleftarrow} f(r,x)$$

ein V-Beweis mod A zu $f(l,x) = f(r,x)$.

Also ist die Regel $f(l,x) \to f(r,x)$ „überflüssig“.

Erweitertes Regelsystem zu R (2)

Definition 4.23

$R^e = R \cup \{s \to t \mid s \to t$ in $EXT_A(R)$,
$s \to t$ nicht überflüssig$\}$

ist das **erweiterte Regelsystem** zu R.

Beachte

1. $s \to t$ aus $EXT_A(R)$ muss man schrittweise aufnehmen, falls noch nicht überflüssig.
2. Sei $l \to r$ in R, $l \equiv f(s,t)$ und $f(l,x) \to f(r,x)$ schon aufgenommen. Dann ist $f(x,l) \to f(x,r)$ überflüssig (nachrechnen!), also nicht in R^e aufzunehmen.

Lemma 4.12

Es gilt stets $(R^e)^e = R^e$.

„Erweiterungsregeln von Erweiterungsregeln sind überflüssig“.

Beispiel zu R^e

Sei

R: $x + s(y) \to s(x + y)$
$\quad x \cdot x^{-1} \to 1 \qquad\qquad +, \cdot$ sind AC

1. Regel: $l \equiv x + s(y)$, $r \equiv s(x + y)$

Die Erweiterungsregel ist $l + z \to r + z$.

Mit $\sigma = \{x \leftarrow x + z\}$ gilt

$$\left.\begin{array}{l} l + z =_{\text{AC}} \sigma(l) \to \sigma(r) \equiv s((x + z) + y) \\ r + z \equiv s(x + y) + z \longrightarrow_{R/A} s((x + y) + z) \end{array}\right\} =_A$$

Also ist $l + z \to r + z$ überflüssig.

Beispiel zu R^e (Forts.)

2. Regel: $l \equiv x \cdot x^{-1}$, $r \equiv 1$

Die 1. Erweiterungsregel $(x \cdot x^{-1}) \cdot y \to 1 \cdot y$ ist nicht überflüssig.

Sei $l_1 \equiv (x \cdot x^{-1}) \cdot y$, $r_1 \equiv 1 \cdot y$, $\sigma = \{y \leftarrow y \cdot z\}$.

Für die 2. Erweiterungsregel $l_1 \cdot z \to r_1 \cdot z$ gilt

$$\begin{array}{l} l_1 \cdot z \equiv ((x \cdot x^{-1}) \cdot y) \cdot z =_{\text{AC}} \sigma(l_1) \to 1 \cdot (y \cdot z) \\ r_1 \cdot z \equiv (1 \cdot y) \cdot z \longrightarrow^{\circ}_{R/A} 1 \cdot (y \cdot z) \end{array}$$

Also ist $l_1 \cdot z \to r_1 \cdot z$ überflüssig.

Also

R^e: $x + s(y) \to s(x + y)$
$\quad x \cdot x^{-1} \to 1$
$\quad (x \cdot x^{-1}) \cdot y \to 1 \cdot y$

Ergebnis zu R^e

Sei A eine Menge von AC-Axiomen.

Satz 4.9.

Sei $(E_0, N_0, S_0) = (E, \varnothing, \varnothing)$.

Sei $(E_i, N_i, S_i)_{i \in \mathbb{N}}$ eine $\mathcal{A}$-Ableitung mit

1. $E^\infty = \varnothing$
2. $CP_A(R^\infty) \subseteq \bigcup_{i \geq 0} E_i$
3. $(R^\infty)^e \subseteq \bigcup_{i \geq 0} S_i$

Dann ist $R^\infty.A$ konvergent modulo A und es gilt $=_{E \cup A} \; = \; =_{R^\infty \cup A}$.

Also:

Nur zu den $l \to r$ in R^∞ muss man eine Erweiterungsregel bilden.
(Keine Erweiterungsregel zu Erweiterungsregel bilden!)

Beispiele

Sei

R: $x + 0 \to x \qquad x \cdot 1 \to x$
A: $+, \cdot$ sind AC
$\succ$ Polynom-Ordnung zu
$\varphi(0) = \varphi(1) = 1 \quad \varphi(+) = \varphi(\cdot)$=Addition

Es gilt mit $\longrightarrow = \overset{\circ}{\longrightarrow}_{R/A}$

$CP_A(R)$:

$$\begin{tikzcd}[column sep=small] & 0+0 \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\ 0 & & 0 \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] & 1 \cdot 1 \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\ 1 & & 1 \end{tikzcd}$$

R^e:

$$\begin{tikzcd} (x+0)+y \arrow[r] \arrow[d, equal, "A"] & x+y \arrow[d, equal] \\ \sigma(x+0) \arrow[r] & \sigma(x) \end{tikzcd} \qquad \begin{tikzcd} (x \cdot 1) \cdot y \arrow[r] \arrow[d, equal, "A"] & x \cdot y \arrow[d, equal] \\ \sigma'(x \cdot 1) \arrow[r] & \sigma'(x) \end{tikzcd}$$

mit $\sigma = \{x \leftarrow x + y\}$ $\qquad$ mit $\sigma' = \{x \leftarrow x \cdot y\}$

Also

Beide Regeln machen ihre Erweiterungsregeln überflüssig.

$R.A$ ist konvergent mod A.

Beispiel: Gruppen

Sei

E: $x + 0 = x$ $\quad x + -(x) = 0$

A: $+$ ist AC

$\succ$: Polynomordnung: $\varphi(0) = 2 \quad \varphi(-)(x) = x^2$

$\varphi(+)(x, y) = x + y$

Die Vervollständigung liefert R:

(1) $x + 0 \to x$

(2) $x + -(x) \to 0$

(3) $(x + -(x)) + y \to y$ als $(2)^e$

(4) $-(0) \to 0$ $\quad 0 \ {}_{R.A}\!\longleftarrow -(0) + 0 \longrightarrow_R -(0)$

(5) $-(-(x)) \to x$ $\quad CP_A(2, 3)$

(6) $y + -(x + y) \to -(x)$ $\quad CP_A(3, 3)$

(7) $-(x + y) \to -(x) + -(y)$ $\quad CP_A(6, 3)$

Die Regel (7) löscht (6).

Beispiel: Gruppen (Forts.)

zu(5) $\underbrace{(x + -(x)) + -(-(x))} =_A x + \underbrace{(-(x) + -(-(x)))}$

$$(x + -(x)) + -(-(x)) \xrightarrow[R]{(3)} -(-(x))$$

$$x + (-(x) + -(-(x))) \xrightarrow[R]{(2)} x + 0 \xrightarrow[R]{(1)} x$$

zu(7) $\underbrace{(y + -(y)) + -(x + y)} =_A \underbrace{(y + -(x + y))} + -(y)$

$$(y + -(y)) + -(x + y) \xrightarrow[R]{(3)} -(x + y)$$

$$(y + -(x + y)) + -(y) \xrightarrow[R]{(6)} -(x) + -(y)$$