Lokale Kriterien für CR-Eigenschaft

Voraussetzung:

a) $\mathsf{Var}(u) = \mathsf{Var}(v)$ für alle $u = v$ in A.
b) $u = v$ in A, falls $v = u$ in A, also $\longrightarrow_A = \longmapsto\!\!\dashv_A$.

Definition 4.5

R heißt **links-linear**, falls

$$l \to r \text{ in } R, x \in \mathsf{Var}(l) \rightsquigarrow |l|_x = 1$$

Definition 4.6

Kritische Paare:

$CP(R) =$	Menge der kritischen Paare zu den $l_1 \to r_1$ und $l_2 \to r_2$ mit $l_i \to r_i$ in R.
$CP(R, A) =$	Menge der kritischen Paare zu den $l \to r$ in R und den $u = v$ in A.

Beispiel

R: $f(a) + f(b) \to a + b$ $\qquad A : a = b$

$$\Rightarrow \quad \begin{array}{ll} f(a) + f(a) = a + b & \text{in } \mathsf{CP}(R, A) \\ f(b) + f(b) = a + b & \end{array}$$

Ergebnisse (1)

Lemma 4.3 (Kritisches-Paar-Lemma)

Sei R links-linear.

Aus $s \;{}_R\!\!\longleftarrow u \longrightarrow_{R \cup A} t$ folgt

(i) $s \downarrow_{=A} t$ oder (ii) $s \longleftrightarrow_{CP(R)} t$ oder (iii) $s \longleftrightarrow_{CP(R,A)} t$

Beweis-Skizze: Die Divergenzanalyse liefert:

a) Variablen-Überlappung: unkritisch, nachrechnen!
b) Echte Uberlappung: Behandlung wie früher mit $CP(R)$ und $CP(R, A)$.
c) Nicht-Überlappung: $s \downarrow_R t$ bzw. $\downarrow_{=A}$ wie früher.

Beachte: Die Voraussetzung „R links-linear" ist wichtig.

Beispiel

R : $f(x, x) \to x \qquad A : a = b$

$$\rightsquigarrow \quad \begin{array}{c} f(a,a) \longmapsto\!\!\dashv f(a,b) \quad \textbf{nicht } a \downarrow_{=A} f(a,b) \\ \swarrow \\ a \end{array}$$

Ergebnisse (2)

Erinnerung (Setze $\sim \; = \; =_A$)

Sei $\longrightarrow_{R/A}$ terminierend, (1)
$\longrightarrow_R \subseteq \longrightarrow \subseteq \longrightarrow_{R/A}$, (2)
$s \longleftarrow u \longrightarrow t$ impliziert $s \downarrow_\sim t$, (3)
$s \;_A\!\longleftarrow u \longrightarrow t$ impliziert $s \downarrow_\sim t$. (4)
Dann ist $\longrightarrow$ CR mod $\sim$.

Satz 4.4.

Sei R links-linear,
$R \subseteq \succ$, $\succ$ A-verträgliche Reduktionsordnung,
$\langle s, t \rangle \in CP(R) \cup CP(R, A) \rightsquigarrow s \downarrow_\sim t$.
Dann ist $\longrightarrow_R$ CR modulo A.

Beweis:

Es gilt (3), (4) nach dem Kritischen-Paar-Lemma.
(2) ist trivial.
(1) gilt wegen $R \subseteq \succ$.

4.2.2 Das Inferenzsystem $\mathcal{L}$

Ziel

Vervollständigung von R mod A, falls R links-linear ist.

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

$\mathcal{L}$ arbeitet auf Paaren (E, R) mit $R \subseteq \succ$.

Beachte: $s \;_A\!\longleftarrow u \longrightarrow t \rightsquigarrow s \succ t$.
$\trianglerighteq$ ist die Umschließungsordnung.

Generelles Vorgehen

Sei sig $= (S, F, \tau)$ fest.
$E \cup A$ Gleichungssystem über sig.
(E_i, R_i) ein Zustand (Gleichungs-/Regelsystem).

Definition 4.7

Ein **V-Beweis mod A** zu $s = t$ in (E_i, R_i) hat die Form:

$$s \xrightarrow{*}_{R_i} s' =_A t' \; {}_{R_i}\xleftarrow{*} t$$

Also

Verbotene Muster im V-Beweis:

$u \longmapsto\!\!\dashv_{E_i} v$	E-Schritt
$u \; {}_{R_i}\!\longleftarrow w \longrightarrow_{R_i} v$	Spitze
$u \longmapsto\!\!\dashv_A w \longrightarrow_{R_i} v$	Klippe
$(u \; {}_{R_i}\!\longleftarrow w \longmapsto\!\!\dashv_A v$	Klippe)

Ziel

$(E, A) \rightsquigarrow (R, A)$ mit

Aus $s =_{E \cup A} t$ folgt $s \xrightarrow{*}_R s' =_A t' \; {}_R\xleftarrow{*} t$

Das Inferenzsystem $\mathcal{L}$

Definition 4.8

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

(M1) Orientieren:

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

(M2) Generieren:

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

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

(M3) Simplifizieren:

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

(M4) Löschen:

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

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

(L1) Simplifizieren rechts:

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

(L2) Simplifizieren links:

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

(M2) wird in der Praxis nur mit $\langle s, t \rangle \in CP(R) \cup CP(R, A)$ angewendet!

$\mathcal{L}$ verkleinert Beweise (1)

Seien $A, \succ$ fest.

Definition 4.9

Ein **Beweis** zu $s = t$ in (E, R) ist eine Folge
$B = (t_0, b_1, t_1, \ldots, b_n, t_n)$ mit $s \equiv t_0$, $t \equiv t_n$,
$t_{i-1} * t_i$, $i = 1, \ldots, n$, $* \in \{\longleftrightarrow_A, \longleftrightarrow_E, \longrightarrow_R, {}_R\!\longleftarrow\}$

$$\begin{array}{rll} b_i & = (l \to r, p) & \text{falls } t_{i-1} \longrightarrow_R t_i \text{ mit } l \to r \\ & = (r \leftarrow l, p) & \text{falls } t_{i-1} \; {}_R\!\longleftarrow t_i \text{ mit } l \to r \\ & = (u = v, E) & \text{falls } t_{i-1} \longleftrightarrow_E t_i \text{ mit } u = v \\ & = (u = v, A) & \text{falls } t_{i-1} \longleftrightarrow_A t_i \text{ mit } u = v \end{array}$$

B heißt ein **V-Beweis mod** A, falls

$$t_0 \xrightarrow{*}_R t_i =_A t_j \; {}_R\!\xleftarrow{*} t_n$$

Beachte: $\succ$ ist auch Ordnung auf A-Äquivalenzklassen:

$$[s] \succ [t] \text{ gdw } s \succ t$$

$\mathcal{L}$ verkleinert Beweise (2)

Ziel Geeignete Beweisordnung $\succ_{\mathcal{L}}$.

Sei min neu, d. h. $\mathrm{min} \notin$ Term(F, V).
$t \succ \mathrm{min}$ für alle $t \in$ Term(F, V).

Definition 4.10

Die Komplexität c_i von (t_{i-1}, b_i, t_i) ist ein 4-Tupel:

$$c_i = \begin{cases} (\{[t_{i-1}], [t_i]\}, -, -, -) & \text{falls } t_{i-1} \longleftrightarrow_E t_i \\ (\{[t_i], [\mathrm{min}]\}, -, -, -) & \text{falls } t_{i-1} \longleftrightarrow_A t_i \\ (\{[t_{i-1}]\}, t_{i-1}/p, l, t_i) & \text{falls } t_{i-1} \longrightarrow_R t_i \\ (\{[t_i]\}, t_i/p, l, t_{i-1}) & \text{falls } t_{i-1} \;{}_R\!\longleftarrow t_i \end{cases}$$

Die Komplexität von B ist:

$$c(B) = \{c_1, \ldots, c_n\}$$

Setze Ordnung $\succ_q$ auf den c_i:

$\succ_q = (\succ\!\succ, >_{TT}, \,\bullet\!\!>, \succ)$ $\quad \bullet\!\!> =$ Subsumptionordnung

Dann ist die Beweisordnung $\succ_{\mathcal{L}}$:

$$B \succ_{\mathcal{L}} B' \text{ gdw } c(B) \succ\!\succ_q c(B')$$

Lemma 4.4

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

$\mathcal{L}$ verkleinert Beweise (3)

Lemma 4.5

Sei $(E, R) \vdash_{\mathcal{L}} (E', R')$. Es gilt

a) Aus $R \subseteq \succ$ folgt $R' \subseteq \succ$.

b) $=_{R \cup E \cup A} \; = \; =_{R' \cup E' \cup A}$

Lemma 4.6

Sei $(E, R) \vdash_{\mathcal{L}} (E', R')$. Sei B Beweis zu $s = t$ in (E, R).
Es gibt einen Beweis B' zu $s = t$ in (E', R') mit $B \succeq_{\mathcal{L}} B'$ (d. h. $B = B'$ oder $B \succ_{\mathcal{L}} B'$). Benutzt B die Spitze $s \;{}_{R \cup A}\!\longleftarrow u \longrightarrow_R t$ und $(E, R) \vdash (E', R')$ die Regel (M2) mit der Spitze, so gilt $B \succ_{\mathcal{L}} B'$.

Beweis-Skizze:

(M1) $s \longleftrightarrow_E t \succ_{\mathcal{L}} s \longrightarrow_{R'} t$

(M2) $s \;{}_R\!\longleftarrow u \longrightarrow_R t \succ_{\mathcal{L}} s \longleftrightarrow_{E'} t$
$s \;{}_A\!\longleftarrow u \longrightarrow_R t \succ_{\mathcal{L}} s \longrightarrow_{R'} t$

(M3) $s \longleftrightarrow_E t \succ_{\mathcal{L}} s \longrightarrow_{R'/A} u \longleftrightarrow_{E'} t$

(M4) $s \longleftrightarrow_E t \succ_{\mathcal{L}} s \overset{*}{\longleftrightarrow}_A t$

(L1) $s \longrightarrow_R t \succ_{\mathcal{L}} s \longrightarrow_{R'} u \;{}_{R'/A}\!\longleftarrow t$

(L2) $s \longrightarrow_R t \succ_{\mathcal{L}} s \longrightarrow_{R'} u \longleftrightarrow_{E'} t$

$\mathcal{L}$ verkleinert Beweise (4)

Definition 4.11

Fairness

Die $\mathcal{L}$-Ableitung $(E_i, R_i)_{i\in\mathbb{N}}$ ist fair, falls

1. $E^\infty = \varnothing$
2. R^∞ ist links-linear
3. $CP(R^\infty) \subseteq \bigcup_{i\geq 0} E_i$
4. $CP(R^\infty, A) \subseteq \bigcup_{i\geq 0} R_i$

mit

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

$\mathcal{L}$ verkleinert Beweise (5)

Definition 4.12

$\mathcal{A}$ ist ein $\mathcal{L}$-**Vervollständigungsverfahren**, falls

- Eingabe $(E, A, \succ)$,
- $\mathcal{A}$ berechnet mit Start $(E_0, R_0) = (E, \varnothing)$ nur faire $\mathcal{L}$-Ableitungen.

Beachte

- Links-Linearität nur von R^∞ gefordert, nicht von allen R_i.
- $R^\infty \subseteq \succ$.
- E^∞ muss leer sein.
- V-Beweise mod A gesucht.

$\mathcal{L}$ verkleinert Beweise (6)

Lemma 4.7

Sei $(E_i, R_i)_{i\in\mathbb{N}}$ eine faire $\mathcal{L}$-Ableitung,
B Beweis zu $s = t$ in (E_j, R_j),
B kein V-Beweis mod A.

Dann gibt es $k \geq j$ und einen Beweis B' zu $s = t$ in (E_k, R_k) mit $B \succ_{\mathcal{L}} B'$.

Satz 4.5.

Sei $\mathcal{A}$ ein $\mathcal{L}$-Vervollständigungsverfahren.

$\mathcal{A}$ breche mit Eingabe $(E, A, \succ)$ nicht ab. Dann ist R^∞ CR mod A und es gilt $R^\infty \subseteq \succ$ und $=_{E\cup A} \; = \; =_{R^\infty \cup A}$.

Beachte

1. $\longrightarrow \; = \; \longrightarrow_R$ (A ist nicht beteiligt).
2. Sei $\longrightarrow_R$ CR mod A, $\longrightarrow_R$ terminierend und $=_A$ entscheidbar. Dann ist $=_{R\cup A}$ entscheidbar.

Beispiel

Sei

$E: \neg(x \wedge y) = \neg x \vee \neg y$
$\quad\;\; \neg(x \vee y) = \neg x \wedge \neg y$

A : AC-Axiome zu $\wedge$ und $\vee$

$\succ$: Polynom-Ordnung zu
$\varphi(\neg)$=Quadrat-Funktion,
$\varphi(\wedge) = \varphi(\vee)$=Summenfunktion.
Dies **ist** A-verträglich.

Dann ergibt sich

R	E	
$(1)\neg(x \wedge y) \to \neg x \vee \neg y$ $(2)\neg(x \vee y) \to \neg x \wedge \neg y$	$-$	
$(3)\neg(y \wedge x) \to \neg x \vee \neg y$ $(4)\neg(y \vee x) \to \neg x \wedge \neg y$	$-$	$(1) + (2)$ +Kommutativ-Gesetze
$\neg(x \wedge (y \wedge z)) \to \neg(x \wedge y) \vee \neg z$ $\neg(x \vee (y \vee z)) \to \neg(x \vee y) \wedge \neg z$ $\neg(x \wedge (y \wedge z)) \to \neg z \vee \neg(x \wedge y)$ $\neg(x \vee (y \vee z)) \to \neg z \wedge \neg(x \vee y)$ ...	$-$	$(1) - (4)$ +Assoziativ-Gesetze
$(1) - (4)$	$-$	Simplifizieren+Löschen

R bestehend aus (1)-(4) ist terminierend und CR mod A.

Beispiel für Divergenz

$E: \max(x,0) = x$
$\quad \max(s(x), s(y)) = s(\max(x,y))$
$A: \max$ ist AC

$\succ$: Polynomordnung mit
$\quad \varphi(s)(x) = x+1 \quad \varphi(0) = 1$
$\quad \varphi(\max)(x,y) = x \cdot y$

Die Vervollständigung liefert

$$
\begin{array}{ll}
(1) & \max(x,0) \to x \\
(2) & \max(0,x) \to x \\
(3) & \max(s(x), s(y)) \to s(\max(x,y)) \\
(4) & \max(s(y), s(x)) \to s(\max(x,y)) \\
(5) & \max(s(x), \max(z_1, s(y))) \to \max(s(\max(x,y)), z_1) \\
 & \vdots \\
(5') & \max(s(x), \max(z_1, \max(z_2, s(y)))) \\
 & \qquad \to \max(s(\max(x,y)), \max(z_1, z_2)) \\
 & \vdots \\
(5'') & \max(s(x), \max(z_1, \max(z_2, \max(z_3, s(y))))) \\
 & \qquad \to \max(s(\max(x,y)), \max(z_1, \max(z_2, z_3)))
\end{array}
$$

Also Divergenz!

Ausweg: $\longrightarrow_R$ verstärken zu $\longrightarrow_{R.A}$
Dann $(5')$, $(5'')$ löschen mit Regel (5).

4.3 A-Vervollständigung für beliebige Regeln

Problem

Gegeben: E, A Gleichungssysteme.

Gesucht: R, $\longrightarrow$, so dass $\longrightarrow$ ist CR mod A.

Frage

Wie wählt man $\longrightarrow$ zu R, A?

Beachte

$\longrightarrow = \longrightarrow_R$ ist zu schwach!

Beispiel

$R: f(x,x) \to g(x) \qquad A: a = b$

$\Rightarrow$ $CP(R) = \varnothing = CP(R, A)$
$\longrightarrow_R$ ist nicht CR mod A,
denn $f(a,b) \; {}_A\!\!\longleftrightarrow f(a,a) \longrightarrow g(a)$
Dies ist eine Variablenüberlappung!

$\Rightarrow$ 1) Variablenüberlappungen sind kritisch.
2) Es gibt i. Allg. unendlich viele Variablenüberlappungen.

Ausweg: $\longrightarrow = \longrightarrow_{R.A}$