Neue Problemstellung

Gegeben: E, A Gleichungssysteme.

Gesucht: R mit (1) $R.A$ ist CR mod A.
(2) $=_{E \cup A} \; = \; =_{R \cup A}$.
(3) R/A ist terminierend.

Beispiel

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

$\rightsquigarrow R : f(x,x) \to g(x)$
R erfüllt die Forderungen.

z.B.

$$\begin{tikzcd} & f(a,a) \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\ g(a) \arrow[rr, phantom, "=_A"] & & g(b) \end{tikzcd} \qquad \begin{tikzcd} & f(a,a) \arrow[dr, "R.A"] & \\ f(a,b) \arrow[ur, "A"] \arrow[rr, "R.A"'] & & g(b) \end{tikzcd}$$

Beachte:

$\longrightarrow_R$ ist **nicht** CR mod A

$$\begin{tikzcd} & f(a,a) \arrow[dl, "R"'] \arrow[r, leftrightarrow, "A"] & f(b,a) \\ g(a) & & \end{tikzcd}$$

$g(a), f(b,a)$ sind irreduzibel, $g(a) \neq_A f(b,a)$.

Test auf CR-Eigenschaft mod A

Erinnerung: Sei $\sim \; = \; =_A$, $\longrightarrow \; = \; \longrightarrow_{R.A}$.

Satz 4.6.

Sei R/A terminierend (1)
Aus $s \longleftarrow u \longrightarrow t$ folgt $s \downarrow_\sim t$ (2)
Aus $s \;{}_A\!\!\longleftrightarrow u \longrightarrow t$ folgt $s \downarrow_\sim t$ (3)
Dann ist $\longrightarrow$ CR mod A.

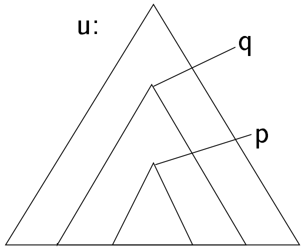
Frage: Wie testet man (2), (3) ?

Definition 4.13

Sei $u \longrightarrow_{R \cup A} s$ mit $l \to r$ bei $p \in O(u)$.
$u \longrightarrow_{R.A} t$ mit $l' \to r'$ bei $q \in O(u)$.

Der 1. Beweisschritt liegt **(echt) unterhalb** dem 2. Beweisschritt, falls q (echtes) Anfangswort von p ist.

Beispiel



Es liegt $u \longrightarrow_{R \cup A} s$ unterhalb von $u \longrightarrow_{R.A} t$.

Es liegen alle A-Schritte in $u \longrightarrow_{R.A} t$ unterhalb von q.

Kritische Beweismuster

Definition 4.14

Eine **Spitze** hat die Form

$$s \;{}_R\!\longleftarrow\; u \longrightarrow_{R.A} t$$

Der 1. Beweisschritt liegt **nicht** echt unterhalb dem 2. Beweisschritt.

Eine **Klippe** hat die Form

$$s \;{}_A\!\longleftarrow\; u \longrightarrow_{R.A} t$$

Der 1. Beweisschritt liegt **nicht** unterhalb dem 2. Beweisschritt.

Beachte

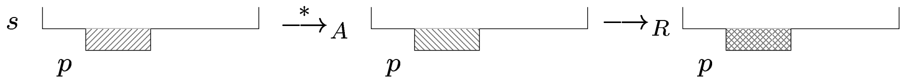
1. Wir setzen A als symmetrisch voraus, d. h. $\longrightarrow_A = \longleftrightarrow_A$.
2. Wir bezeichnen auch die symmetrischen Varianten als Spitzen/Klippen.
3. Sei $s \;{}_A\!\overset{*}{\longleftarrow}\; u \longrightarrow_{R.A} t$, alle A-Schritte seien unterhalb vom $R.A$-Schritt. Dann gilt $s \longrightarrow_{R.A} t$.

Lemma 4.8

Gilt $s \downarrow_\sim t$ für jede Spitze und Klippe $s \;{}_{R\cup A}\!\longleftarrow\; u \longrightarrow_{R.A} t$, so ist $\longrightarrow_{R.A}$ lokal konfluent mod A und lokal kohärent mod A.

Bemerkung zu Spitzen/Klippen

Zu $\longrightarrow_{R.A}$: Sei $s \;{}_p\!\longrightarrow_{R.A} t$ bei $p \in O(s)$.



Zu Klippen: Sei $s \;{}_A\!\longleftarrow_q\; u \;{}_p\!\longrightarrow_{R.A} t$ (*)

1. $q \geq p$ (d. h. q unter p):
   Es gilt $s \longrightarrow_{R.A} t$ (*) ist keine Klippe.
2. $q < p$: Dann gilt i. Allg. nicht $s \downarrow_\sim t$. (*) **ist** eine Klippe.

Zu Spitzen: Sei $s \;{}_{R.A}\!\longleftarrow_q\; u \;{}_p\!\longrightarrow_{R.A} t$, o.B.d.A. $q \leq p$ (+)

Es gilt 1) oder 2)

1) $s \;{}_R\!\longleftarrow_q\; u' \;{}_A\!\overset{*}{\longleftarrow}_{\geq p}\; u \;{}_p\!\longrightarrow_{R.A} t$
   Es gilt $s \;{}_R\!\longleftarrow_q\; u' \;{}_p\!\longrightarrow_{R.A} t$ Dies **ist** eine Spitze.
2) $s \;{}_{R.A}\!\longleftarrow_q\; u'' \;{}_A\!\longleftarrow_{<p}\; u' \;{}_A\!\overset{*}{\longleftarrow}_{\geq p}\; u \;{}_p\!\longrightarrow_{R.A} t$
   Es gilt $u'' \;{}_A\!\longleftarrow_{<p}\; u' \;{}_p\!\longrightarrow_{R.A} t$ Dies **ist** eine Klippe.

Also

Es reicht, Klippen + Spitzen zu beseitigen!

Lokale Divergenzanalyse

Sei $s \;_{R\cup A}\!\longleftarrow u \longrightarrow_{R.A} t$ eine Spitze/Klippe.

1. Beweisschritt bei $p \in O(u)$ mit $l_1 \to r_1$.
2. Beweisschritt bei $q \in O(u)$ mit $l_2 \to r_2$.

1. Fall

$u/p, u/q$ seien disjunkte Teilterme von u. Dies ist eine Nicht-Überlappung.

Es gilt $s \longrightarrow_{R.A} \circ \;_{R\cup A}\!\longleftarrow t$, also $s \downarrow_\sim t$.

2. Fall

u/q ist Teilterm von u/p (echter Teilterm, falls Klippe).

Dies ist eine **Überlappung**. Es gilt $q = p \cdot p'$

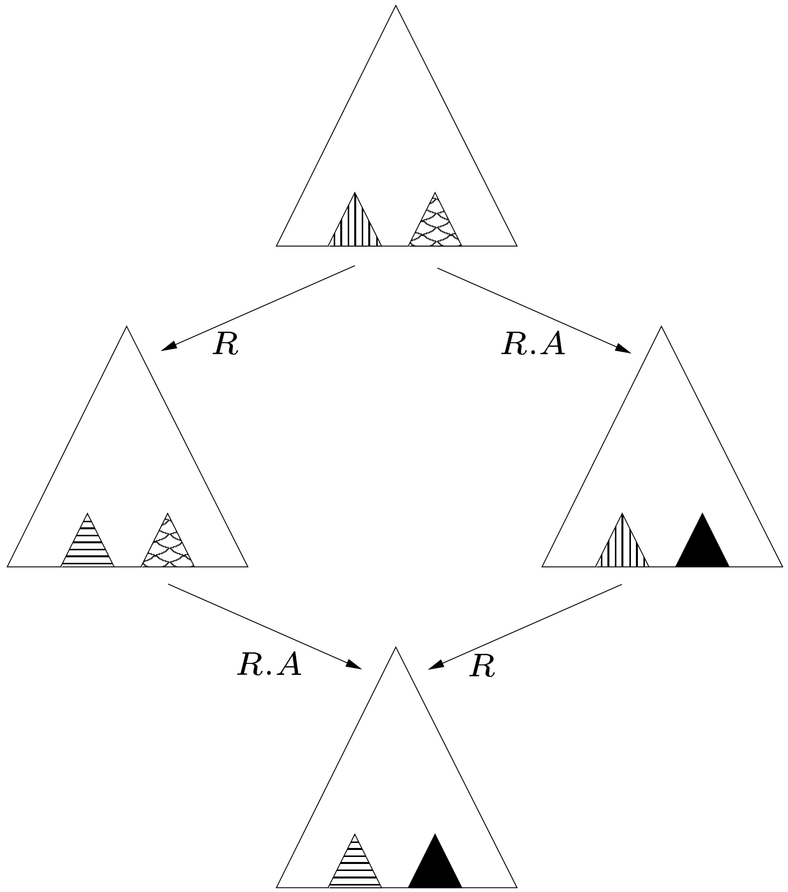
a) $p' \in O(l_1) \wedge l_1/p' \notin V$
Dies ist eine **echte Überlappung** $\sigma(l_1/p') =_A \sigma(l_2)$

$$\begin{tikzcd}
\sigma(l_1) \arrow[d, "R \cup A"'] & =_A & \sigma(l_1[p' \leftarrow l_2]) \arrow[d, "R"] \\
\sigma(r_1) & & \sigma(l_1[p' \leftarrow r_2])
\end{tikzcd}$$

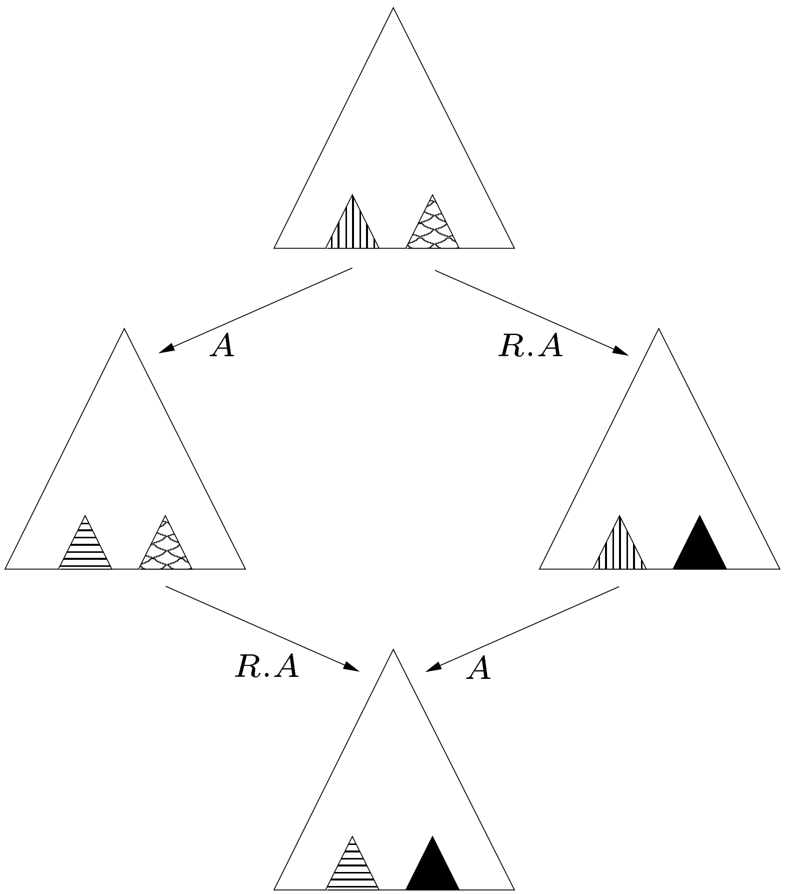
Durch kritisches Paar abfangen.

b) $p' \notin O(l_1)$ oder $p' \in O(l_1) \wedge l_1/p' \in V$
Dies ist eine **Variablen-Überlappung**. Es gilt $s \downarrow_\sim t$ (siehe später).

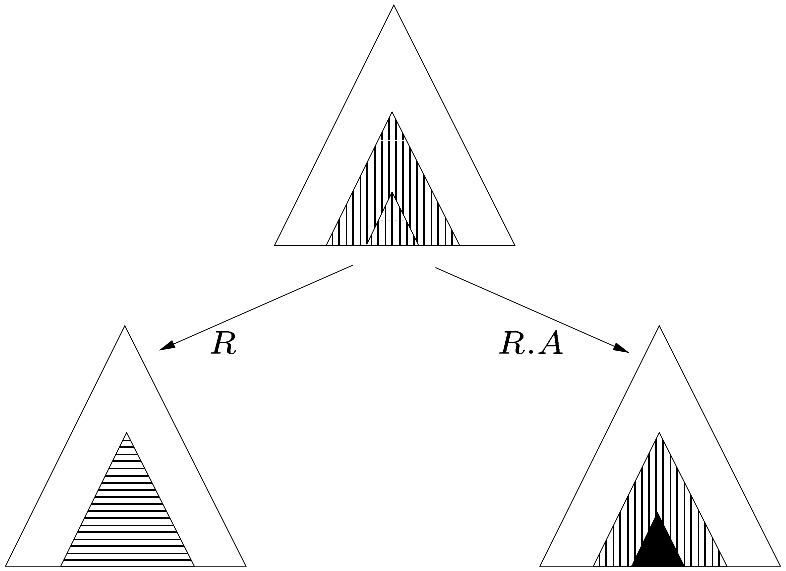
Divergenzanalyse zu $\longrightarrow_{R.A}$, 1. Fall



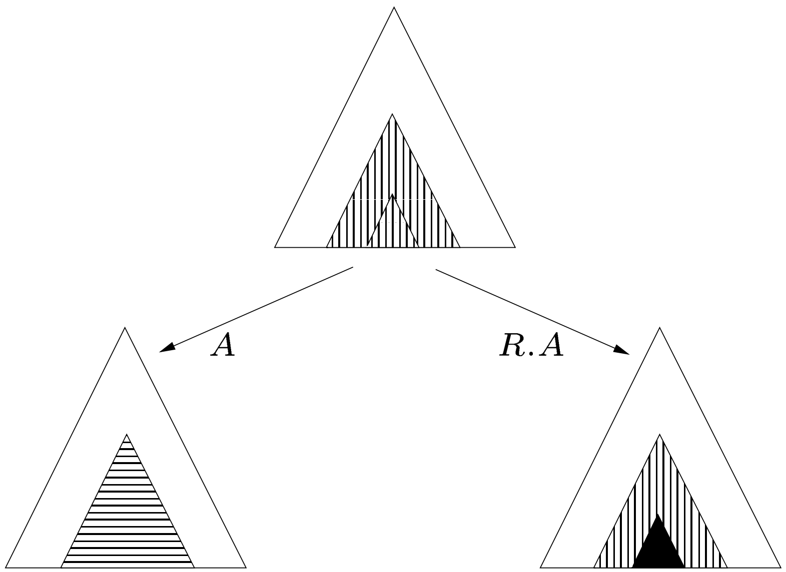
Divergenzanalyse zu $\longrightarrow_{R.A}$, 1. Fall (Forts.)



Divergenzanalyse zu $\longrightarrow_{R.A}$, 2. Fall



Divergenzanalyse zu $\longrightarrow_{R.A}$, 2. Fall (Forts.)



Variablen-Überlappungen

Lemma 4.9

Ist $s \ {}_{R\cup A}\!\longleftarrow \ u \longrightarrow_{R.A} t$ eine Variablen-Überlappung, so gilt $s \downarrow_{\sim} t$.

Beweis am Beispiel: Sei $\sim \; = \; =_A$ und $\longrightarrow \; = \; \longrightarrow_{R.A}$

a) Spitze: $f(x,x) \to g(x,x,x)$, $l \to r$, $l \sim \bar{l}$

$$\begin{tikzcd}
& f(\bar{l},\bar{l}) \arrow[dl, "R"] \arrow[dr] & \\
g(\bar{l},\bar{l},\bar{l}) \arrow[d, "*"] & & f(r,\bar{l}) \arrow[d] \\
g(r,r,r) & & f(r,r) \arrow[ll]
\end{tikzcd}$$

Variablen-Überlappungen (Forts.)

b) Klippe: $f(x,x) = g(x,x,x), \quad l \to r, \quad l \sim \bar{l}$

$$\begin{tikzcd}[column sep=small]
& f(\bar{l},\bar{l}) \arrow[dl, "A"'] \arrow[dr] & \\
g(\bar{l},\bar{l},\bar{l}) \arrow[d, "*"] & & f(r,\bar{l}) \arrow[d, "*"] \\
g(r,r,r) & =_A & f(r,r)
\end{tikzcd}$$

Erinnerung an die Voraussetzung

$u = v$ in $A \rightsquigarrow \mathsf{Var}(u) = \mathsf{Var}(v)$

Echte Überlappungen

Beispiel

R: $x + 0 \to x$ $\qquad A : x + y = y + x$
$\quad y + 1 \to f(y)$

Es gilt

$$\begin{tikzcd}[column sep=small]
& 1+0 \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\
1 & & f(0)
\end{tikzcd}
\quad \text{denn} \quad
\begin{tikzcd}[column sep=small]
1+0 \arrow[d, "R"'] & =_A & 0+1 \arrow[d, "R"] \\
1 & & f(0)
\end{tikzcd}$$

$\Rightarrow$ Die linken Seiten der Regeln $x+0$ und $y+1$ sind A-**unifizierbar**:

$$\sigma = \{x \leftarrow 1, y \leftarrow 0\} \rightsquigarrow \sigma(x+0) =_A \sigma(y+1)$$

Definition 4.15

s, t heißen A-**unifizierbar**, falls es σ gibt mit $\sigma(s) =_A \sigma(t)$.
Dann heißt σ ein A-**Unifikator** zu s, t.

Sei $\sigma \mathrel{\underline{\gtrdot}}_A \tau(V_0)$ gdw $\exists \varrho : \sigma(x) =_A \varrho(\tau(x))$ für alle $x \in V_0$.

Sei Σ eine Menge von A-Unifikatoren zu s, t.

a) Σ heißt **vollständig**: Zu jedem A-Unifikator τ gibt es $\sigma \in \Sigma$ mit $\tau \mathrel{\underline{\gtrdot}}_A \sigma(\mathsf{Var}(s,t))$.

b) Σ heißt **minimal**:
$\sigma, \tau \in \Sigma \rightsquigarrow \sigma, \tau$ sind bezüglich $\mathsf{Var}(s,t)$ $\mathrel{\underline{\gtrdot}}_A$-unvergleichbar.

Bemerkung: A-Unifikation

Unifikationsproblem zu A

Gegeben: $s, t \in \mathsf{Term}(F, V)$.
Frage: Sind s, t A-unifizierbar?
(Zusatz: Berechne vollständige Menge von A-Unifikatoren: $\Sigma_{s,t}$)

Satz 4.7.

1. Sei A Menge von AC-Axiomen. Dann gilt:
   Die A-Unifikation ist entscheidbar.
   $\Sigma_{s,t}$ ist berechenbar.
   $\Sigma_{s,t}$ kann $2^{2^{O(n)}}$ Elemente haben $n = |s| + |t|$.
2. Sei A Menge von Kommutativitäts-Axiomen. Dann ist die A-Unifikation leicht.
3. Sei A: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ Distributivität
   $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ Distributivität
   $(x + y) + z = x + (y + z)$ Assoziativität

   Es gibt Konstanten. Dann ist die A-Unifikation unentscheidbar.

Beispiel: A-Unifikation

Sei $s \equiv f(x, g(a, b))$ $\quad t \equiv f(g(y, b), x)$

a) $A = \varnothing$ (syntaktische Unifikation)

$$\sigma_1 = \{x \leftarrow g(a, b), y \leftarrow a\} = \mathsf{mgu}(s, t)$$

b) $A : f(x, y) = f(y, x)$ „f ist kommutativ"
σ_1 und $\sigma_2 = \{y \leftarrow a\}$ sind A-Unifikatoren.

c) $A : f(x, y) = f(y, x) \quad f(x, f(y, z)) = f(f(x, y), z)$,
d. h. „f ist AC"
$\Sigma = \{\sigma_2\}$ ist vollständige + minimale Menge von A-Unifikatoren.

d) $A : f(x, f(y, z)) = f(f(x, y), z)$ „f ist assoziativ"
- $\mu_0 = \sigma_1 = \{x \leftarrow g(a, b), y \leftarrow a\}$
- $\mu_{i+1} = \{x \leftarrow f(g(a, b), \mu_i(x)), y \leftarrow a\}$
- $\Sigma = \{\mu_i \mid i \in \mathbb{N}\}$ ist vollständige und minimale Menge von A-Unifikatoren.

z. B. $\mu_1 = \{x \leftarrow f(g(a, b), g(a, b)), y \leftarrow a\}$,
$u :\equiv g(a, b)$
$\mu_1(s) \equiv f(f(u, u), u) =_A f(u, f(u, u)) \equiv \mu_1(t)$

A-kritische Paare

Definition 4.16

Seien $l \to r$ und $s \to t$ Variablen-disjunkt,
$p \in O(l)$ $l/p \notin V$,
Σ vollständige Menge von A-Unifikatoren zu l/p, s,
$\sigma \in \Sigma$.

Dann gilt

$$\begin{tikzcd} & \sigma(l) \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\ \sigma(r) & & \sigma(l[p \leftarrow t]) \end{tikzcd}$$

und $\langle \sigma(r), \sigma(l[p \leftarrow t]) \rangle$ heißt ein A-**kritisches Paar** zu den Regeln (und Σ), genauer: von $s \to t$ auf $l \to r$.

$CP_A(R)$ ist die Menge der A-kritischen Paare von Regeln $l \to r$ in R auf $s \to t$ in R.

$CP_A(R, A)$ ist die Menge der A-kritischen Paare von Regeln $l \to r$ auf $s \to t$ mit (i) $l \to r$ in R und (ii) $s \doteq t$ in A.

Beachte

$CP_A(R, A)$ entsteht durch das Überlappen von Regeln auf Gleichungen. Es müssen keine Gleichungen auf Regeln überlappt werden.

Beispiele: A-kritische Paare (1)

Sei

R: $f(x+y) \to g(x,y)$
A: $(x+y)+z = x+(y+z)$
$x+y = y+x$

Es ergibt sich z. B.

$CP_A(R)$:

$$\begin{tikzcd} & f(x+y) \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\ g(x,y) & & g(y,x) \end{tikzcd} \qquad \begin{tikzcd} & f((x'+y')+z') \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\ g(x'+y',z') & & g(x',y'+z') \end{tikzcd}$$

Wegen

$$\begin{array}{ll} x+y =_A^? u+v & x+y =_A^? u+v \\ \sigma = \{u \leftarrow y, v \leftarrow x\} & \sigma = \{x \leftarrow x'+y', y \leftarrow z', \\ & u \leftarrow x', v \leftarrow y'+z'\} \end{array}$$

Beachte

$x+y =_A^? u+v$ hat viele Lösungen!

$CP_A(R, A) = \varnothing$

Also

Nur Regeln auf Regeln und Regeln auf Gleichungen überlappen, nicht Gleichungen auf Regeln!

Beispiele: A-kritische Paare (2)

Sei

R: $f(x) + f(y) \to g(x, y)$
A: $x + y = y + x$
$\quad (x + y) + z = x + (y + z)$

Es ergibt sich z. B.

$CP_A(R)$:

$$\begin{tikzcd}[column sep=small] & f(x)+f(y) \arrow[dl, "R"'] \arrow[dr, "R.A"] & \\ g(x,y) & & g(y,x) \end{tikzcd}$$

$CP_A(R, A)$:

$$\begin{tikzcd}[column sep=small] & (f(x)+f(y))+z \arrow[dl, "A"'] \arrow[dr, "R.A"] & \\ f(x)+(f(y)+z) & & g(x,y)+z \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] & x+(f(y)+f(z)) \arrow[dl, "A"'] \arrow[dr, "R.A"] & \\ (x+f(y))+f(z) & & x+g(y,z) \end{tikzcd}$$

$$\begin{tikzcd}[column sep=small] & f(x)+f(y) \arrow[dl, "A"'] \arrow[dr, "R.A"] & \\ f(y)+f(x) \arrow[rr, "R.A"'] & & g(x,y) \end{tikzcd}$$

Beachte

Überlappungen „Regel auf Gleichung bei $p = \lambda$“ sind generell unkritisch!

Erweitertes Kritisches-Paar Lemma

Lemma 4.10

a) Zu jeder echten Überlappung

$$s \;{}_R\!\longleftarrow u \longrightarrow_{R.A} t$$

bei der der 1. Beweisschritt oberhalb des 2. stattfindet, gibt es einen Beweis

$$s =_A s' \longleftrightarrow_{CP_A(R)} t' =_A t.$$

b) Zu jeder echten Überlappung

$$s \;{}_A\!\longleftarrow u \longrightarrow_{R.A} t$$

bei der der 1. Beweisschritt echt oberhalb des 2. stattfindet, gibt es einen Beweis

$$s =_A s' \longleftrightarrow_{CP_A(R,A)} t' =_A t.$$

Beachte

Dies behandelt die nicht-trivialen a) Spitzen, b) Klippen.

Ansatz für die Vervollständigung

Idee: Kritische Paare bilden + verarbeiten.

Beispiel

Sei

R: (1) $a \to c$ A: $a = f(e)$
(2) $b \to d$ $e = b$

$\succ =$ KB-Ordnung zu
$\varphi(a) = 3 \quad \varphi(b) = \varphi(e) = 2$
$\varphi(c) = \varphi(d) = \varphi(f) = 1$

Dann ist $\succ$ A-verträglich.

Es gilt

$CP_A(R) = \varnothing$

$CP_A(R, A)$: Es gilt z. B.

$$\begin{tikzcd}[column sep=small] & f(e) \arrow[dl, "A"'] \arrow[dr, "R.A"] & \\ a & & f(d) \end{tikzcd}$$

Dies liefert
(3) $a \to f(d)$
(1) und (3) liefert $c = f(d)$, also
(4) $f(d) \to c$

Dann löscht (4) Regel (3). Also:

R': (1), (2), (4)
$R'.A$ ist CR mod A!

Erweiterungsregeln (1)

Ziel

Behandlung von Klippen.

Beispiel

$R : f(x) + f(y) \to f(x + y) \qquad l \to r$
$A : (x + y) + z = x + (y + z) \qquad u = v$

$u/1$ ist mit l A-unifizierbar.

Das kritische Paar $f(x) + (f(y) + z) = f(x + y) + z$
ist äquivalent zu $(f(x) + f(y)) + z \to f(x + y) + z$

Dies ist mit $l \to r$ reduzierbar zu

$$f(x + y) + z = f(x + y) + z$$

Also:

Die Regel $l + z \to r + z$ wird stets erzeugt (Erweiterungsregel zu $l \to r$).

Sie muss man vor der Simplifikation mit $l \to r$ schützen!