# 4 Termersetzung modulo einer Kongruenz

## 4.1 Die CR-Eigenschaft modulo $A$

**Problem**

Sei spec $=$ (sig, $E$), $E$ enthält unrichtbare Gleichungen.

Gesucht $\longrightarrow$, so dass $\longrightarrow$ in jedem $[t]_E$ (fast) eindeutige Normalformen bestimmt.

**Typisches Beispiel**

$E$ enthält AC-Axiome für $f$:

$$f(x,y) = f(y,x)$$

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



# Lösungsansätze

**1. Ansatz**: UKB-Vervollständigung

Zu schwach, divergiert häufig,

z. B. $E_0 : x + y = y + x \qquad (x+y)+z = x+(y+z)$

$\Rightarrow$ UKB-Vervollständigung divergiert.

**2. Ansatz**: Termersetzung modulo $A$

a) $E_0 = E \cup A$ nicht richtbaren Anteil $A$ isolieren.

b) $(E, A) \rightsquigarrow (R, A)$ $\longrightarrow$ benutzt $R$ und $A$.

c) CR-Eigenschaft modulo $A$

also

$$\begin{tikzcd} s \arrow[r, phantom, "=_{E\cup A}"] \arrow[d, "*"'] & t \arrow[d, "*"] \\ \exists s_0, t_0 : s_0 \arrow[r, phantom, "=_A"] & t_0 \end{tikzcd}$$

$\longrightarrow$ berechnet Normalformen modulo $A$.

Annahme: Die $A$-Gleichheit ist leicht zu behandeln.

## Beispiele

**Natürliche Zahlen**

$E$: $x + 0 = x$ $\quad$ $\min(0, y) = 0$

$x + s(y) = s(x + y)$ $\quad$ $\min(s(x), s(y)) = s(\min(x, y))$

$x \cdot 0 = 0$

$x \cdot s(y) = (x \cdot y) + x$

$+, \cdot, \min$ sind AC

**Aussagenlogik**

$E$: $x \wedge 0 = 0$ $\quad$ $x \vee 0 = x$

$x \wedge 1 = x$ $\quad$ $x \vee 1 = 1$

$x \wedge x = x$ $\quad$ $x \vee x = x$

$\wedge, \vee$ sind AC

**Kommutative Gruppen**

$E$: $x + 0 = x$

$x + -x = 0$

$+$ ist AC



## Wahl für $\longrightarrow$

**Sei** $R$ Regelsystem über sig,
$A$ Gleichungssystem über sig.

**Definition 4.1**

$\longrightarrow_R$: $\quad s \longrightarrow_R t$ gdw $\quad$ es gibt $l \to r, p, \sigma$:
$s/p \equiv \sigma(l)$, $t \equiv s[p \leftarrow \sigma(r)]$

$\longrightarrow_{R.A}$: $\quad s \longrightarrow_{R.A} t$ gdw $\quad$ es gibt $l \to r, p, \sigma$:
$s/p =_A \sigma(l)$, $t \equiv s[p \leftarrow \sigma(r)]$

$\longrightarrow_{R/A}$: $\quad s \longrightarrow_{R/A} t$ gdw $\quad$ es gibt $s', t'$:
$s =_A s' \longrightarrow_R t' =_A t$

also $\longrightarrow_{R/A} \; = \; =_A \circ \longrightarrow_R \circ =_A$

## Bemerkungen zur Wahl von $\longrightarrow$ (1)

**Bemerkung**

Zu $\longrightarrow_R$:
Dies ist definiert wie bisher, es berücksichtigt $A$ gar nicht.

Zu $\longrightarrow_{R.A}$:
Hier darf man zunächst den Redex $s/p$ mit $A$ so umschreiben, dass er eine Instanz $\sigma(l)$ der linken Seite einer Regel $l \to r$ ist, und dann die Regel anwenden.

Zu $\longrightarrow_{R/A}$:
Hier darf man zunächst den ganzen Term $s$ mit $A$ so umschreiben, dass er eine Instanz $\sigma(l)$ der linken Seite einer Regel $l \to r$ als Teilterm enthält, und dann die Regel anwenden.

**Beispiel**

**Sei** $R : a + b \to c \qquad A: \begin{array}{l} x + y = y + x \\ (x+y)+z = x+(y+z) \end{array}$

a) $s \equiv (b + a) + a$ ist $\longrightarrow_R$-irreduzibel, aber
$s \longrightarrow_{R.A} c + a$, denn $s/1 \equiv b + a =_A a + b$

b) $s \equiv (b + b) + a$ ist $\longrightarrow_R$- und $\longrightarrow_{R.A}$-irreduzibel, aber
$s \longrightarrow_{R/A} b + c$, denn $s =_A b + (a + b) \longrightarrow_R b + c$
$s \longrightarrow_{R/A} c + b$, denn $s =_A (a + b) + b \longrightarrow_R c + b$



## Bemerkungen zur Wahl von $\longrightarrow$ (2)

**Beachte**

a) $\longrightarrow_R \subseteq \longrightarrow_{R.A} \subseteq \longrightarrow_{R/A}$
Die Reduktionsrelation $\longrightarrow_R$ ist die schwächste und $\longrightarrow_{R/A}$ ist die stärkste von diesen 3 Möglichkeiten.
$\longrightarrow_{R.A}$ ist ein guter Kompromiss zwischen Mächtigkeit und Berechnungsaufwand.

b) Für $A = \varnothing$ gilt $\longrightarrow_R = \longrightarrow_{R.A} = \longrightarrow_{R/A}$.
Dies ist also eine Verallgemeinerung der Termersetzung ohne unterliegende Theorie $A$.

c) Für $\longrightarrow \in \{\longrightarrow_R, \longrightarrow_{R.A}, \longrightarrow_{R/A}\}$ gilt
$(\longleftrightarrow \cup \vdash\!\!\!\longrightarrow\!\!\dashv_A)^* = =_{R\cup A}$

**Voraussetzung ab jetzt**

$$\longrightarrow_R \subseteq \longrightarrow \subseteq \longrightarrow_{R/A}$$

Dann gilt $(\longleftrightarrow \cup \vdash\!\!\!\longrightarrow\!\!\dashv_A)^* = =_{R\cup A}$

## Berechnung von $\longrightarrow_R, \longrightarrow_{R.A}, \longrightarrow_{R/A}$

a) $s$ ist mit $l \to r$ $\longrightarrow_R$-reduzierbar $\mathrm{gdw}$
es gibt $p \in O(s)$ und Match von $l$ auf $s/p$.

b) $\sigma$ ist $A$-**Match** von $l$ auf $t$ $\mathrm{gdw}$ $t =_A \sigma(l)$.
$s$ ist mit $l \to r$ $\longrightarrow_{R.A}$-reduzierbar $\mathrm{gdw}$
es gibt $p \in O(s)$ und $A$-Match von $l$ auf $s/p$.

c) $s$ ist mit $l \to r$ $\longrightarrow_{R/A}$-reduzierbar $\mathrm{gdw}$
es gibt $s' \in [s]_A$ mit $s'$ ist $\longrightarrow_R$-reduzierbar.

Also: $\longrightarrow_R$-Reduzierbarkeit ist leicht.
$\longrightarrow_{R.A}$-Reduzierbarkeit ist mittel-schwer
(entscheidbar, falls $A$ nur aus AC-Axiomen besteht).
$\longrightarrow_{R/A}$-Reduzierbarkeit ist oft sehr schwer.

Häufig gute Wahl: $\longrightarrow \, = \, \longrightarrow_{R.A}$



## Eigenschaften von $\longrightarrow$

**Wunsch**

1. $\longrightarrow_{R/A}$ ist terminierend.
2. $\longrightarrow$ hat die CR-Eigenschaft modulo $A$.

**Definition 4.2**

$\longrightarrow$ hat die **CR-Eigenschaft modulo $A$**
(kurz: ist **CR modulo $A$**), falls gilt

$$(\longleftrightarrow \cup \vdash\!\!\!\longrightarrow\!\!\!\dashv_A)^* \subseteq \xrightarrow{*} \circ =_A \circ \xleftarrow{*}$$

Im Bild

$$\begin{tikzcd} s \arrow[d, "*"'] & =_{R \cup A} & t \arrow[d, "*"] \\ \exists s_0, t_0 : s_0 & =_A & t_0 \end{tikzcd}$$

## Abstrakte Reduktionssysteme

| **Sei**: | | **dies entspricht**: |
|---|---|---|
| $\mathcal{E}$ | Menge | Term$(F, V)$ |
| $\longrightarrow$ | Relation | $\longrightarrow$ |
| $\vdash\!\!\!\longrightarrow\!\!\!\dashv$ | symmetrische Relation | $\vdash\!\!\!\longrightarrow\!\!\!\dashv_A$ |
| $\sim$ | $= \vdash\!\!\!\longrightarrow\!\!\!\dashv^*$ | $=_A$ |
| $\models\!\!\!\Longrightarrow\!\!\!\dashv$ | $= \longleftrightarrow \cup \vdash\!\!\!\longrightarrow\!\!\!\dashv$ | |
| $\approx$ | $= \models\!\!\!\Longrightarrow\!\!\!\dashv^*$ | $=_{R \cup A}$ |
| $\longrightarrow_\sim$ | $= \sim \circ \longrightarrow \circ \sim$ | $\longrightarrow_{R/A}$ |
| $\downarrow_\sim$ | $= \xrightarrow{*} \circ \sim \circ \xleftarrow{*}$ | zusammenführbar modulo $\sim$ |



## Abstrakte Reduktionssysteme (Forts.)

**Definition 4.3**

$\longrightarrow$ ist **CR mod** $\sim$: Aus $s \approx t$ folgt $s \downarrow_\sim t$

$\longrightarrow$ ist **konfluent mod** $\sim$: Aus $s \xleftarrow{*} u \xrightarrow{*} t$ folgt $s \downarrow_\sim t$

$\longrightarrow$ ist **lokal konfluent mod** $\sim$: Aus $s \longleftarrow u \longrightarrow t$ folgt $s \downarrow_\sim t$

$\longrightarrow$ ist **kohärent mod** $\sim$: Aus $s \xleftarrow{*} u \sim t$ folgt $s \downarrow_\sim t$

$\longrightarrow$ ist **lokal kohärent mod** $\sim$: Aus $s \longleftarrow u \vdash\!\!\!\longrightarrow\!\!\!\dashv t$ folgt $s \downarrow_\sim t$

$$\begin{tikzcd} & s \arrow[d, "*"'] & \approx & t \arrow[d, "*"] \\ \exists : & s_0 & \sim & t_0 \end{tikzcd}$$

CR
mod $\sim$

$$\begin{tikzcd} & u \arrow[dl] \arrow[dr] & \\ s \arrow[d, "*"'] & & t \arrow[d, "*"] \\ s_0 & \sim & t_0 \end{tikzcd}$$

lokal konfluent
mod $\sim$

$$\begin{tikzcd} & u \arrow[dl] & \vdash\!\!\!\longrightarrow\!\!\!\dashv & t \arrow[dd, "*"] \\ s \arrow[d, "*"'] & & & \\ s_0 & & \sim & t_0 \end{tikzcd}$$

lokal kohärent
mod $\sim$

## Kriterien für die CR-Eigenschaft

**Beachte:**

a) Sei $\vdash\!\!\dashv \, = \emptyset$, also $\sim \, = \mathrm{id}$.

   1) Dann haben wir die Situation wie in Kapitel 1.
      $\longrightarrow$ ist stets kohärent mod $\sim$

   2) $\longrightarrow$ ist CR mod $\sim$ $\,\mathrm{gdw}\,$ $\longrightarrow$ ist konfluent mod $\sim$

b) Aber für $\vdash\!\!\dashv \, \neq \emptyset$ gilt 2) nicht:

$$\begin{array}{ccccc}
a_0 & \vdash\!\!\dashv & b_0 & & c_0 \\
\downarrow & & \downarrow & & \downarrow \\
a_1 & & b_1 & \vdash\!\!\dashv & c_1 \\
\downarrow & & \downarrow & & \downarrow \\
a_2 & \vdash\!\!\dashv & b_2 & & c_2 \\
\downarrow & & \downarrow & & \downarrow \\
a_3 & & b_3 & \vdash\!\!\dashv & c_3 \\
\downarrow & & \downarrow & & \downarrow
\end{array}$$

$\Rightarrow \longrightarrow$ ist konfluent und kohärent mod $\sim$, aber nicht CR mod $\sim$.

**Satz 4.1.**

Sei $\longrightarrow$ terminierend.
Dann gilt $\longrightarrow$ ist CR mod $\sim$

$\mathrm{gdw}$ $\longrightarrow$ ist konfluent mod $\sim$ und
$\longrightarrow$ ist kohärent mod $\sim$.



## Lokale Kriterien für die CR-Eigenschaft

**Beachte** für $\vdash\!\!\dashv \, = \emptyset$ gilt das Newman-Lemma

Ist $\longrightarrow$ terminierend, so gilt:
$\longrightarrow$ ist CR $\mathrm{gdw}$ $\longrightarrow$ ist lokal konfluent.

**Hier**: Man benötigt zusätzlich

a) $\longrightarrow_\sim$ ist terminierend.

b) $\longrightarrow$ ist lokal kohärent.

**Beispiel 1**

Sei $a \longleftarrow b \xleftarrow{\vdash\dashv} c \xrightarrow{\vdash\dashv} d \longrightarrow e$

Dann: $\longrightarrow$ ist terminierend, $\longrightarrow_\sim$ **nicht** terminierend
(z. B. $c \longrightarrow_\sim c$).
$\longrightarrow$ ist lokal konfluent mod $\sim$.
$\longrightarrow$ ist lokal kohärent mod $\sim$.
$\longrightarrow$ ist **nicht** CR mod $\sim$.

**Beispiel 2**

Sei $a \longleftarrow b \vdash\!\!\dashv c$

Dann: $\longrightarrow_\sim$ ist terminierend.
$\longrightarrow$ ist lokal konfluent mod $\sim$, **nicht** lokal kohärent mod $\sim$.
$\longrightarrow$ ist **nicht** CR mod $\sim$.

## Ergebnisse

**Satz 4.2.**

Sei $\longrightarrow_\sim$ terminierend. Dann gilt:

$\longrightarrow$ ist CR mod $\sim$

$\text{gdw}$ $\longrightarrow$ ist lokal konfluent mod $\sim$ und
$\longrightarrow$ ist lokal kohärent mod $\sim$.

Beweis-Idee:

$\succ = \xrightarrow{+}_\sim$ ist Noethersche Partialordnung.

Induktion auf $(\mathsf{Mult}(\mathcal{E}), \succ\!\succ)$ zeigt, dass für alle $B \in \mathsf{Mult}(\mathcal{E})$ $P(B)$ gilt mit

$P(B)$ gdw $\{s_1, \ldots, s_n\} \subseteq B \wedge s_1 \models\!\!\!=\!\!\!\dashv s_2 \models\!\!\!=\!\!\!\dashv \cdots \models\!\!\!=\!\!\!\dashv s_n$
impliziert $s_1 \downarrow_\sim s_n$

Also $s \approx t \leadsto s \downarrow_\sim t$.



## Ergebnisse (Forts.)

Instanziierung für die Termersetzung:

**Satz 4.3.**

Sei $\longrightarrow_{R/A}$ terminierend.

Dann gilt für jedes $\longrightarrow$ mit $\longrightarrow_R \subseteq \longrightarrow \subseteq \longrightarrow_{R/A}$:

$\longrightarrow$ ist CR mod $A$

$\text{gdw}$ $\longrightarrow$ ist lokal konfluent mod $A$ und
$\longrightarrow$ ist lokal kohärent mod $A$.

## Termination von $R/A$ wird benötigt

**Beachte**

Sei $\longrightarrow_{R/A}$ terminierend. Ist $\longrightarrow_{R.A}$ lokal konfluent und lokal kohärent mod $A$, so ist $\longrightarrow_{R.A}$ CR mod $A$.

Es reicht **nicht**, dass $\longrightarrow_{R.A}$ terminierend ist. Dies gilt auch, wenn $R$ und $A$ Variablen-frei sind.

**Beispiel**

$R$: $a \to b$ $\qquad$ $A$: $f^2(a) = f^2(b)$

$\quad f(b) \to c$ $\qquad\quad f^2(a) = c$

1. $\longrightarrow_R$ und $\longrightarrow_{R.A}$ sind terminierend.
2. $R$ ist links-linear.
   $CP(R) = \varnothing, \quad CP(R, A)$ enthält 3 Paare.
   $R$ und $R.A$ sind lokal konfluent und lokal kohärent mod $A$ (siehe später).
3. $R.A$ ist nicht kohärent mod $A$, also auch nicht CR mod $A$:
   $c \longmapsto\!\!\dashv f^2(a) \longmapsto\!\!\dashv f^2(b) \longrightarrow f(c)$, nicht $c \downarrow_\sim f(c)$ in $R.A$
4. $R/A$ ist nicht terminierend:
   $f^2(b) \longrightarrow_{R/A} f^2(b)$, denn $f^2(b) =_A f^2(a) \longrightarrow_R f^2(b)$



## Bemerkungen

1. Satz 4.3 gilt z. B. für $\longrightarrow \, = \, \longrightarrow_R$ und $\longrightarrow \, = \, \longrightarrow_{R.A}$.
2. Unklar ist noch der Test auf
   - $\longrightarrow$ ist lokal konfluent mod $A$
   - $\longrightarrow$ ist lokal kohärent mod $A$
3. Wie zeigt man: „$\longrightarrow_{R/A}$ ist terminierend“?

**Beachte**

$\longrightarrow_{R/A}$ definiert $\mapsto_R$ auf den $A$-Äquivalenzklassen $[t]_A \quad (= [t])$

$$[s] \mapsto_R [t] \text{ gdw } s \longrightarrow_{R/A} t$$

($\mapsto_R$ ist wohl definiert!)

**Definition 4.4**

Die Partialordnung $\succ$ heißt $A$-**verträglich** , falls

$$s =_A s' \succ t' =_A t \quad \leadsto s \succ t$$

## Bemerkungen (Forts.)

**Lemma 4.1**

a) Ist $\longrightarrow_{R/A}$ terminierend,
so ist $\succ \; = \; \stackrel{+}{\longrightarrow}_{R/A}$ eine $A$-verträgliche Reduktionsordnung.

b) Ist $R \subseteq \succ$ und $\succ$ eine $A$-verträgliche Reduktionsordnung,
so ist $\longrightarrow_{R/A}$ terminierend.

c) Ist $\longrightarrow_{R/A}$ terminierend,
so sind auch $\longrightarrow_{R}$ und $\longrightarrow_{R.A}$ terminierend.



## AC-verträgliche Ordnungen

**Beispiel**

$R$: $x + 0 \to x$ $\quad$ $A$: $x + y = y + x$
$\quad x + s(y) \to s(x + y)$ $\quad (x+y)+z = x+(y+z)$

$\succ$: Polynom-Ordnung zu

$$\varphi(0) = 2, \quad \varphi(s)(x) = x + 1, \quad \varphi(+)(x, y) = x \cdot y$$

Übung: Es gilt

1) $R \subseteq \succ$

2) $\succ$ ist $A$-verträglich.

**Frage**

Wieso Ass-Gleichung nicht in $R$?

**Lemma 4.2**

Es gibt keine C-verträgliche Reduktionsordnung die Ass richtet.

Beweis: Ann. $(x + y) + z \succ x + (y + z)$ C-verträglich.

$$\begin{aligned} \rightsquigarrow (x+y)+z =_C (y+x)+z \succ y+(x+z) &=_C (x+z)+y \\ =_C (z+x)+y \succ z+(x+y) &=_C (x+y)+z \end{aligned}$$

$\rightsquigarrow (x + y) + z \succ (x + y) + z \qquad \lightning$

## 4.2 $A$-Vervollständigung für links-lineare Regeln

### 4.2.1 Lokale Konfluenzkriterien für $\longrightarrow_R$

**Problem**

Gegeben: $E$, $A$.

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

**Frage**: Was wählt man als $\longrightarrow$?

Idee: 1) $\longrightarrow \; = \; \longrightarrow_R$.

2) Kritische Paare zu $R \cup A$ bilden.

**Problem**: $\longrightarrow_R$ ist i. Allg. zu schwach.

Aber (vergleiche mit Satz 4.3):

1. Abschwächung von $s \downarrow t$ zu $s \downarrow_{=_A} t$ hilft: $\longrightarrow_R$ ist lokal konfluent mod $=_A$.
2. Ist $R$ links-linear, so ist $\longrightarrow_R$ stark genug: $\longrightarrow_R$ ist lokal kohärent mod $=_A$.



## Beispiel

**Sei**

$$
\begin{array}{lll}
R: & x + 0 \to x & x + s(y) \to s(x + y) \\
 & 0 + x \to x & s(y) + x \to s(x + y) \\
A: & x + y = y + x &
\end{array}
$$

**Es gilt**

$\longrightarrow_R$ **ist** CR mod $A$, $\longrightarrow_R$ ist **nicht** CR: z. B.

$$
\begin{tikzcd}
 & s(x) + s(y) \arrow[dl] \arrow[dr] & \\
s(s(x) + y) \arrow[d] & & s(s(y) + x) \arrow[d] \\
t_1 \equiv s^2(y + x) & & s^2(x + y) \equiv t_2
\end{tikzcd}
$$

$t_1 =_A t_2$, nicht $t_1 \downarrow_R t_2$

**Generelles Vorgehen für die Vervollständigung**

Beweis-Transformation:

Zu $s =_{E \cup A} t$ einen V-Beweis mod $A$ erzeugen.