

Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2019/2020

Termersetzungssysteme

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK

Definition

Termersetzungssysteme sind spezielle Reduktionssysteme. Ist E eine endliche Menge von Gleichungen über der Signatur Σ , dann nennen wir das Reduktionssystem

$$(\text{Term}_{\Sigma}, \rightarrow_E^1)$$

ein *Termersetzungssystem*.

Da dieses durch Σ und E eindeutig bestimmt ist, sprechen wir kürzer vom *Termersetzungssystem* (Σ, E) .

Kanonisches Termersetzungssysteme

Theorem

(Σ, E) sei ein kanonisches Termersetzungssystem.

- 1. Zu jedem Term t gibt es genau einen irreduziblen Term $\text{irr}(t)$ mit $t \rightarrow_E \text{irr}(t)$.*
- 2. Für beliebige Terme s, t gilt:*

$$E \models s \doteq t \Leftrightarrow \text{irr}(s) = \text{irr}(t).$$

- 3. Die Gültigkeit einer Gleichung in der Theorie von E ist entscheidbar.*

Spezialfall des Satzes über kanonische Reduktionssysteme.

Ein einfaches kanonisches Termersetzungssystem

E_{GBT} :

$$\begin{array}{ll} 0 \wedge x &= 0 & 1 \wedge x &= x \\ x \wedge 0 &= 0 & x \wedge 1 &= x \\ 0 \vee x &= x & 1 \vee x &= 1 \\ x \vee 0 &= x & x \vee 1 &= 1 \end{array}$$

Für jeden variablenfreien Booleschen Term t gilt

$$\begin{array}{l} t \rightarrow_{E_{GBT}} 0 \\ \text{oder} \\ t \rightarrow_{E_{GBT}} 1. \end{array}$$

Definition

Ein Paar (t_1, t_2) von Termen heißt *kritisches Paar* von (Σ, E) , wenn existieren: Gleichungen $l_1 \doteq r_1$ und $l_2 \doteq r_2$, die Varianten von Gleichungen in E sind; ferner ein Term u und eine Substitution μ , so dass gilt:

- ▶ u ist Unterterm von l_1 , u ist keine Variable

Der Term $\mu(l_1)$ heißt dabei eine *Überlagerung* von l_1 mit l_2 .

Definition

Ein Paar (t_1, t_2) von Termen heißt *kritisches Paar* von (Σ, E) , wenn existieren: Gleichungen $l_1 \doteq r_1$ und $l_2 \doteq r_2$, die Varianten von Gleichungen in E sind; ferner ein Term u und eine Substitution μ , so dass gilt:

- ▶ u ist Unterterm von l_1 , u ist keine Variable
- ▶ u ist mit l_2 unifizierbar, und μ ist ein $\text{mgu}(u, l_2)$

Der Term $\mu(l_1)$ heißt dabei eine *Überlagerung* von l_1 mit l_2 .

Definition

Ein Paar (t_1, t_2) von Termen heißt *kritisches Paar* von (Σ, E) , wenn existieren: Gleichungen $l_1 \doteq r_1$ und $l_2 \doteq r_2$, die Varianten von Gleichungen in E sind; ferner ein Term u und eine Substitution μ , so dass gilt:

- ▶ u ist Unterterm von l_1 , u ist keine Variable
- ▶ u ist mit l_2 unifizierbar, und μ ist ein $\text{mgu}(u, l_2)$
- ▶ $t_1 = \mu(r_1)$ (nach der Gleichung $l_1 \doteq r_1$)

Der Term $\mu(l_1)$ heißt dabei eine *Überlagerung* von l_1 mit l_2 .

Definition

Ein Paar (t_1, t_2) von Termen heißt *kritisches Paar* von (Σ, E) , wenn existieren: Gleichungen $l_1 \doteq r_1$ und $l_2 \doteq r_2$, die Varianten von Gleichungen in E sind; ferner ein Term u und eine Substitution μ , so dass gilt:

- ▶ u ist Unterterm von l_1 , u ist keine Variable
- ▶ u ist mit l_2 unifizierbar, und μ ist ein $\text{mgu}(u, l_2)$
- ▶ $t_1 = \mu(r_1)$ (nach der Gleichung $l_1 \doteq r_1$)
- ▶ t_2 entsteht aus $\mu(l_1)$, indem dort genau ein Vorkommen von $\mu(l_2)$ durch $\mu(r_2)$ ersetzt wird (nach der Gleichung $l_2 \doteq r_2$).

Der Term $\mu(l_1)$ heißt dabei eine *Überlagerung* von l_1 mit l_2 .

Theorem

Ein Termersetzungssystem (Σ, E) ist

*lokal konfluent
genau dann, wenn
jedes kritische Paar (t_1, t_2) konfluent ist
d.h. ein t existiert mit $t_1 \rightarrow_E t, t_2 \rightarrow_E t$.*

Theorem

Ein Termersetzungssystem (Σ, E) ist

*lokal konfluent
genau dann, wenn
jedes kritische Paar (t_1, t_2) konfluent ist
d.h. ein t existiert mit $t_1 \rightarrow_E t$, $t_2 \rightarrow_E t$.*

Lemma

Ein endliches Termersetzungssystem (Σ, E) besitzt bis auf Variantenbildung nur endlich viele kritische Paare, und diese lassen sich algorithmisch aus (Σ, E) erhalten.

$$\begin{array}{lcl} 1 & 0 + x & = x \\ 2 & (x + y) + z & = x + (y + z) \\ 3 & i(x) + x & = 0 \end{array}$$

$$\begin{array}{lll} 1 & 0 + x & = x \\ 2 & (x + y) + z & = x + (y + z) \\ 3 & i(x) + x & = 0 \end{array}$$

Ist E_G lokal konfluent?

$$\begin{array}{lll} 1 & 0 + x & = x \\ 2 & (x + y) + z & = x + (y + z) \\ 3 & i(x) + x & = 0 \end{array}$$

Ist E_G lokal konfluent?

Wir untersuchen die kritischen Paare.

Kritische Paare für E_G

1 in 2	$(0 + u) + z$	$(0 + (u + z), u + z)$
2 in 2	$((u + v) + w) + z$	$((u + v) + (w + z), (u + (v + w)) + z)$
3 in 2	$(i(u) + u) + z$	$(i(u) + (u + z), 0 + z)$

$$\begin{array}{ll} 1 \text{ in } 2 & (0 + u) + z \qquad (0 + (u + z), u + z) \\ 2 \text{ in } 2 & ((u + v) + w) + z \quad ((u + v) + (w + z), (u + (v + w)) + z) \\ 3 \text{ in } 2 & (i(u) + u) + z \qquad (i(u) + (u + z), 0 + z) \end{array}$$

Beide Seiten von 1) reduzieren zu $u + z$.

$$\begin{array}{ll} 1 \text{ in } 2 & (0 + u) + z \qquad (0 + (u + z), u + z) \\ 2 \text{ in } 2 & ((u + v) + w) + z \quad ((u + v) + (w + z), (u + (v + w)) + z) \\ 3 \text{ in } 2 & (i(u) + u) + z \qquad (i(u) + (u + z), 0 + z) \end{array}$$

Beide Seiten von 1) reduzieren zu $u + z$.

Beide Seiten von 2) reduzieren zu $((u + v) + w) + z$.

$$\begin{array}{ll} 1 \text{ in } 2 & (0 + u) + z \qquad (0 + (u + z), u + z) \\ 2 \text{ in } 2 & ((u + v) + w) + z \quad ((u + v) + (w + z), (u + (v + w)) + z) \\ 3 \text{ in } 2 & (i(u) + u) + z \qquad (i(u) + (u + z), 0 + z) \end{array}$$

Beide Seiten von 1) reduzieren zu $u + z$.

Beide Seiten von 2) reduzieren zu $((u + v) + w) + z$.

Reduktion von 3) führt zu dem Paar

$$i(u) + (u + z) \quad z$$

Kritische Paare für E_G

$$\begin{array}{ll}
 1 \text{ in } 2 & (0 + u) + z \quad (0 + (u + z), u + z) \\
 2 \text{ in } 2 & ((u + v) + w) + z \quad ((u + v) + (w + z), (u + (v + w)) + z) \\
 3 \text{ in } 2 & (i(u) + u) + z \quad (i(u) + (u + z), 0 + z)
 \end{array}$$

Beide Seiten von 1) reduzieren zu $u + z$.

Beide Seiten von 2) reduzieren zu $((u + v) + w) + z$.

Reduktion von 3) führt zu dem Paar

$$i(u) + (u + z) \quad z$$

Es gilt

$$E_G \models z \doteq i(u) + (u + z)$$

Kritische Paare für E_G

$$\begin{array}{ll}
 1 \text{ in } 2 & (0 + u) + z \quad (0 + (u + z), u + z) \\
 2 \text{ in } 2 & ((u + v) + w) + z \quad ((u + v) + (w + z), (u + (v + w)) + z) \\
 3 \text{ in } 2 & (i(u) + u) + z \quad (i(u) + (u + z), 0 + z)
 \end{array}$$

Beide Seiten von 1) reduzieren zu $u + z$.

Beide Seiten von 2) reduzieren zu $((u + v) + w) + z$.

Reduktion von 3) führt zu dem Paar

$$i(u) + (u + z) \quad z$$

Es gilt

$$E_G \models z \doteq i(u) + (u + z)$$

Setze $E_G^1 = E_G \cup \{z \doteq i(u) + (u + z)\}$.

Kritische Paare für E_G

$$\begin{array}{ll}
 1 \text{ in } 2 & (0 + u) + z \quad (0 + (u + z), u + z) \\
 2 \text{ in } 2 & ((u + v) + w) + z \quad ((u + v) + (w + z), (u + (v + w)) + z) \\
 3 \text{ in } 2 & (i(u) + u) + z \quad (i(u) + (u + z), 0 + z)
 \end{array}$$

Beide Seiten von 1) reduzieren zu $u + z$.

Beide Seiten von 2) reduzieren zu $((u + v) + w) + z$.

Reduktion von 3) führt zu dem Paar

$$i(u) + (u + z) \quad z$$

Es gilt

$$E_G \models z \doteq i(u) + (u + z)$$

Setze $E_G^1 = E_G \cup \{z \doteq i(u) + (u + z)\}$.

Ist E_G^1 lokal konfluent?

Kritische Paare für E_G^1

1 in 4	$i(0) + (0 + u)$	$(i(0) + u, u)$
2 in 4	$i(u + v) + ((u + v) + w)$	$(i(u + v) + (u + (v + w)), w)$
3 in 4	$i(i(u)) + (i(u) + u)$	$(i(i(u)) + 0, u)$
4 in 2	$(i(x) + (x + y)) + w$	$(i(x) + ((x + y) + w), y + w)$
4 in 4	$i(i(u)) + (i(u) + (u + v))$	$(i(i(u)) + v, u + v)$

Kritische Paare für E_G^1

1 in 4	$i(0) + (0 + u)$	$(i(0) + u, u)$
2 in 4	$i(u + v) + ((u + v) + w)$	$(i(u + v) + (u + (v + w)), w)$
3 in 4	$i(i(u)) + (i(u) + u)$	$(i(i(u)) + 0, u)$
4 in 2	$(i(x) + (x + y)) + w$	$(i(x) + ((x + y) + w), y + w)$
4 in 4	$i(i(u)) + (i(u) + (u + v))$	$(i(i(u)) + v, u + v)$

Reduktion der kritischen Paare ergibt:

$(i(0) + u, u)$	$(i(0) + u, u)$
$(i(u + v) + (u + (v + w)), w)$	$(i(u + v) + (u + (v + w)), w)$
$(i(i(u)) + 0, u)$	$(i(i(u)) + 0, u)$
$(i(x) + ((x + y) + w), y + w)$	$(y + w, y + w)$
$(i(i(u)) + v, u + v)$	$(i(i(u)) + v, u + v)$

Kritische Paare für E_G^1

1 in 4	$i(0) + (0 + u)$	$(i(0) + u, u)$
2 in 4	$i(u + v) + ((u + v) + w)$	$(i(u + v) + (u + (v + w)), w)$
3 in 4	$i(i(u)) + (i(u) + u)$	$(i(i(u)) + 0, u)$
4 in 2	$(i(x) + (x + y)) + w$	$(i(x) + ((x + y) + w), y + w)$
4 in 4	$i(i(u)) + (i(u) + (u + v))$	$(i(i(u)) + v, u + v)$

Reduktion der kritischen Paare ergibt:

$(i(0) + u, u)$	$(i(0) + u, u)$
$(i(u + v) + (u + (v + w)), w)$	$(i(u + v) + (u + (v + w)), w)$
$(i(i(u)) + 0, u)$	$(i(i(u)) + 0, u)$
$(i(x) + ((x + y) + w), y + w)$	$(y + w, y + w)$
$(i(i(u)) + v, u + v)$	$(i(i(u)) + v, u + v)$

Nur das vorletzte Paar ist also konfluent.

E_G^2

1	$0 + x$	$=$	x
2	$(x + y) + z$	$=$	$x + (y + z)$
3	$i(x) + x$	$=$	0
4	$i(x) + (x + y)$	$=$	y
5	$i(0) + x$	$=$	x
6	$i(x + y) + (x + (y + z))$	$=$	z
7	$i(i(x)) + y$	$=$	$x + y$

Neue Gleichungen in blau.

Kritische Paare für E_G^2

- 1 in 6 $(i(u) + (0 + (u + z)) , z)$
- 1 in 6 $(i(0 + y) + (y + z) , z)$
- 3 in 5 $(0 , 0)$
- 3 in 6 $(i(i(y + z) + y) + 0 , z)$
- 3 in 7 $(x + i(x) , 0)$
- 4 in 5 $(0 + v , v)$
- 4 in 6 $(i(i(u) + u) + v , v)$
- 4 in 7 $((x + (i(x) + v) , v)$
- 5 in 2 $(i(0) + (x + v) , x + v)$
- 5 in 4 $(i(i(0)) + x , x)$
- 5 in 6 $(i(i(0) + y) + (y + z) , z)$
- 6 in 2 $(i(x + y) + ((x + (y + z)) + w) , z + w)$
- 6 in 6 $(i(i(u + v) + u) + w , v + w)$
- 7 in 2 $(i(i(x)) + (y + z) , (x + y) + z)$
- 7 in 3 $(x + i(x) , 0)$
- 7 in 4 $(x + (i(x) + u) , u)$
- 7 in 6 $(v + w , v + w)$

Aus den nicht konfluenten kritischen Paare von E_G^2 ergeben sich die folgenden neuen Gleichungen:

$$i(i(y + z) + y) + 0 = z$$

$$x + i(x) = 0$$

$$x + (i(x) + v) = v$$

$$i(i(u + v) + u) + w = v + w$$

Im Knuth-Bendix Verfahren können auch Gleichungen wieder wegfallen.

Im Knuth-Bendix Verfahren können auch Gleichungen wieder wegfallen.

Unter den kritischen Paaren von E_G^3 kommt die Überlagerung

$$i(i(u + v) + u) + 0$$

von $i(i(y + z) + y) + 0 = z$ und $i(i(u + v) + u) + w = v + w$ vor,
die zu dem nicht konfluenten kritischen Paar führt: $(v + 0, v)$.

Im Knuth-Bendix Verfahren können auch Gleichungen wieder wegfallen.

Unter den kritischen Paaren von E_G^3 kommt die Überlagerung

$$i(i(u + v) + u) + 0$$

von $i(i(y + z) + y) + 0 = z$ und $i(i(u + v) + u) + w = v + w$ vor, die zu dem nicht konfluenten kritischen Paar führt: $(v + 0, v)$.

Nimmt man die neue Regel $(v + 0 = v)$ in E_G^4 dann sieht man, dass die Termersetzung $i(i(y + z) + y) + 0 = z$ überflüssig wird: sie kann aus $(v + 0 = v)$ und $i(i(u + v) + u) + w = v + w$ abgeleitet werden.

Endergebnis

Ein kanonisches Termersetzungssystem für die Gruppentheorie

E_{Group} :

$$0 + x \rightarrow x$$

$$x + 0 \rightarrow x$$

$$i(x) + x \rightarrow 0$$

$$x + i(x) \rightarrow 0$$

$$i(0) \rightarrow 0$$

$$(x + y) + z \rightarrow x + (y + z)$$

$$i(x) + (x + y) \rightarrow y$$

$$x + (i(x) + y) \rightarrow y$$

$$i(x + y) \rightarrow i(y) + i(x)$$

$$i(i(x)) \rightarrow x$$