Termersetzungssysteme
Vorlesung 4

Stephan Falke

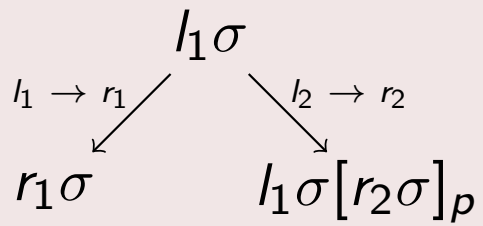
Verifikation trifft Algorithmik
Karlsruher Institut für Technologie (KIT)

28.06.2010

Kritische Paare

Definition

Seien $l_1 \to r_1$, $l_2 \to r_2$ mit $\mathcal{V}(l_1 \to r_1) \cap \mathcal{V}(l_2 \to r_2) = \emptyset$ gegeben
Sei $p \in \mathcal{P}os(l_1)$ so dass $l_1|_p \notin \mathcal{V}$ und sei σ ein allgemeinster Unifikator von $l_1|_p$ und l_2
Dann ist $\langle r_1\sigma, l_1\sigma[r_2\sigma]_p \rangle$ ein kritisches Paar:



$CP(\mathcal{R})$: kritische Paare zwischen allen Regeln aus $\mathcal{R}$
Kritische Paare einer Regel mit sich selbst (nach Umbenennung der Variablen) müssen auch betrachtet werden (ausser für $p = \Lambda$)!

Entscheidbarkeitsresultate

Satz

$\mathcal{R}$ is lokal konfluent gdw. alle kritischen Paare zusammenführbar sind

Folgerung

Falls $\mathcal{R}$ terminierend ist so ist $\mathcal{R}$ konfluent gdw. alle kritischen Paare zusammenführbar sind

Satz

Das folgende Problem ist entscheidbar:
Eingabe: *Ein terminierendes TES $\mathcal{R}$*
Frage: *Ist $\mathcal{R}$ (lokal) konfluent?*

Wortprobleme

Definition

Sei $\mathcal{E} = \{s_1^0 \approx s_1^1, \ldots, s_n^0 \approx s_n^1\}$ eine Menge von Axiomen.
Das Wortproblem von $\mathcal{E}$ ist das folgende Problem:
Eingabe: Eine Gleichung $s \approx t$
Frage: Folgt $s \approx t$ aus $\mathcal{E}$?

Ansatz zur Lösung des Wortproblems:

- Finde ein zu $\mathcal{E}$ "äquivalentes" TES $\mathcal{R}$ so dass $\mathcal{R}$ terminierend und konfluent ist
- $s \approx t$ folgt aus $\mathcal{E}$ gdw. $\mathrm{NF}_{\mathcal{R}}(s) = \mathrm{NF}_{\mathcal{R}}(t)$

1. Algorithmus

Algorithmus

Eingabe: $\mathcal{E} = \{s_1^0 \approx s_1^1, \ldots, s_n^0 \approx s_n^1\}$
Ausgabe: *Ein "äquivalentes", terminierendes und konfluentes TES* $\mathcal{R}$

for $(i_1, \ldots, i_n) \in \{0,1\}^n$ **do**
    $\mathcal{R} := \{s_1^{i_1} \to s_1^{1-i_1}, \ldots, s_n^{i_n} \to s_n^{1-i_n}\}$;
    if $\mathcal{R}$ *ist terminierend und konfluent* **then**
        return $\mathcal{R}$;
    end
end
fail

Beispiel

$$\begin{array}{lrcl} \mathcal{E}\colon & x + \mathcal{O} & \approx & x \\ & x + \mathsf{s}(y) & \approx & \mathsf{s}(x + y) \end{array}$$

Orientierung "von links nach rechts" ergibt

$$\begin{array}{lrcl} \mathcal{R}\colon & x + \mathcal{O} & \to & x \\ & x + \mathsf{s}(y) & \to & \mathsf{s}(x + y) \end{array}$$

terminierend

konfluent da keine kritischen Paare

$x + \mathsf{s}(\mathsf{s}(\mathcal{O})) \approx \mathsf{s}(x) + \mathsf{s}(\mathcal{O})$ folgt aus $\mathcal{E}$ da

$$\mathrm{NF}_{\mathcal{R}}(x + \mathsf{s}(\mathsf{s}(\mathcal{O}))) = \mathsf{s}(\mathsf{s}(x)) = \mathrm{NF}_{\mathcal{R}}(\mathsf{s}(x) + \mathsf{s}(\mathcal{O}))$$

$x + y \approx y + x$ folgt nicht aus $\mathcal{E}$ da $\mathrm{NF}_{\mathcal{R}}(x + y) \neq \mathrm{NF}_{\mathcal{R}}(y + x)$

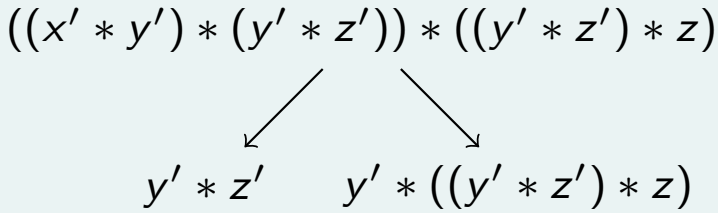
Beispiel (Zentrale Gruppoide)

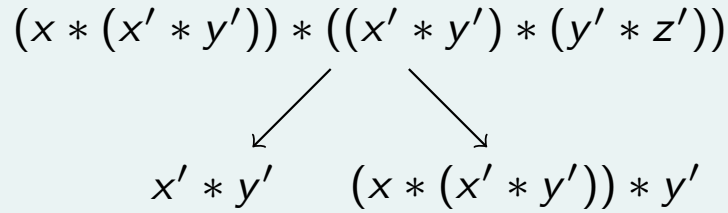
$$\mathcal{E}: \quad (x * y) * (y * z) \quad \approx \quad y$$

Orientierung kann nur von "von links nach rechts" erfolgen

$$\mathcal{R}: \quad (x * y) * (y * z) \quad \to \quad y$$

nicht konfluent da die kritischen Paare





nicht zusammenführbar sind

Der 1. Algorithmus schlägt fehl

Kritische Paare als Regeln

- Kritische Paare (betrachtet als Gleichungen) folgen aus den Axiomen
- Sie können daher orientiert und zu $\mathcal{R}$ hinzu gefügt werden

$$\begin{array}{lrcl} \mathcal{R}: & (x * y) * (y * z) & \to & y \\ & y' * ((y' * z') * z) & \to & y' * z' \\ & (x * (x' * y')) * y' & \to & x' * y' \end{array}$$

- Die ursprünglichen kritischen Paare sind nun zusammenführbar
- Die neuen Regeln erzeugen neue kritische Paare, d.h., der Prozess muss iteriert werden

Alle kritischen Paare sind zusammenführbar, d.h., $\mathcal{R}$ ist konfluent

2. Algorithmus

Algorithmus

Eingabe: $\mathcal{E} = \{s_1^0 \approx s_1^1, \ldots, s_n^0 \approx s_n^1\}$
Ausgabe: *Ein "äquivalentes", terminierendes und konfluentes TES* $\mathcal{R}$

$\mathcal{R}_0 :=$ *"eine terminierende Orientierung von* $\mathcal{E}$*"* **or fail**;
repeat
  $\mathcal{R}_{i+1} := \mathcal{R}_i$;
  for $\langle s_0, s_1 \rangle \in CP(\mathcal{R}_i)$ **do**
    $\widehat{s_0}, \widehat{s_1} :=$ *beliebige* $\mathcal{R}_i$*-Normalformen von* s_0, s_1;
    if $\widehat{s_0} = \widehat{s_1}$ **then**
      continue;
    end
    orientiere $\widehat{s_0} \approx \widehat{s_1}$ *so dass* $\mathcal{R}_{i+1} := \mathcal{R}_{i+1} \cup \{\widehat{s_i} \to \widehat{s_{1-i}}\}$ *terminierend ist* **or fail**;
  end
  $i := i + 1$;
until $\mathcal{R}_i = \mathcal{R}_{i+1}$;
return $\mathcal{R}_i$;

Diskussion

Mögliches Verhalten des Algorithmus:

- Erfolgreiche Berechnung mit Ausgabe $\mathcal{R}_i$

Satz

Wenn der 2. Algorithmus ein $\mathcal{R}_i$ zurück gibt dann ist $\mathcal{R}_i$ äquivalent zu $\mathcal{E}$, terminierend, und konfluent

- Abbruch nach endlicher Laufzeit wenn $\mathcal{R}_{i+1}$ nicht terminierend ist (oder dies nicht bewiesen werden kann)
- Unendlicher Lauf

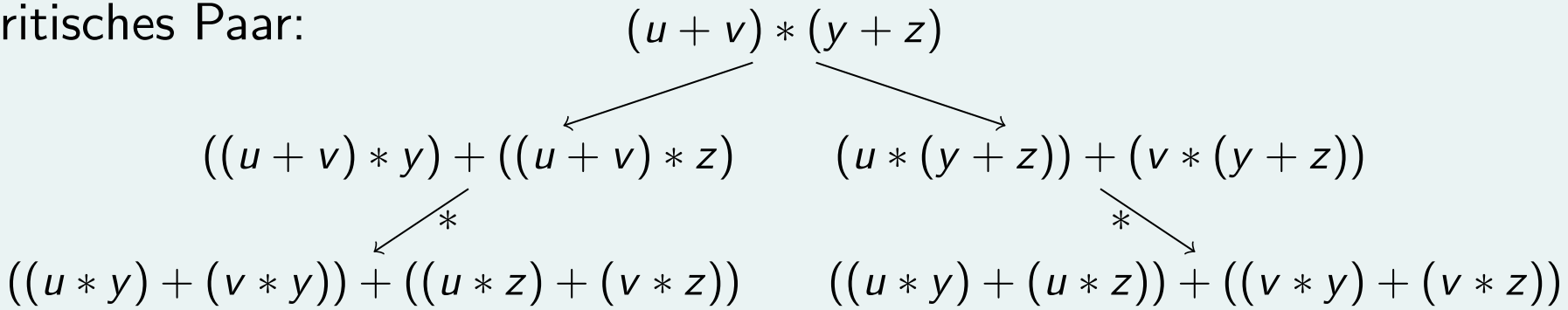
Beispiel (Abbruch nach endlicher Laufzeit)

$$\begin{array}{lrcl} \mathcal{E}\colon & x * (y + z) & \approx & (x * y) + (x * z) \\ & (u + v) * w & \approx & (u * w) + (v * w) \end{array}$$

Orientierung "von links nach rechts" liefert

$$\begin{array}{lrcl} \mathcal{R}_0\colon & x * (y + z) & \to & (x * y) + (x * z) \\ & (u + v) * w & \to & (u * w) + (v * w) \end{array}$$

Kritisches Paar:



Beide Orientierungen erzeugen ein nicht-terminierendes TES

Beispiel

Unendlicher Lauf

$$\begin{array}{lrcl} \mathcal{E}: & x + \mathcal{O} & \approx & x \\ & x + \mathsf{s}(y) & \approx & \mathsf{s}(x + y) \end{array}$$

"Ungünstige" Orientierung

$$\begin{array}{lrcl} \mathcal{R}_0: & x + \mathcal{O} & \to & x \\ & \mathsf{s}(x + y) & \to & x + \mathsf{s}(y) \end{array}$$

$\mathcal{R}_1$ fügt $x + \mathsf{s}(\mathcal{O}) \to \mathsf{s}(x)$ hinzu

$\mathcal{R}_2$ fügt $x + \mathsf{s}(\mathsf{s}(\mathcal{O})) \to \mathsf{s}(\mathsf{s}(x))$ hinzu

$\vdots$

$\mathcal{R}_n$ fügt $x + \mathsf{s}^n(\mathcal{O}) \to \mathsf{s}^n(x)$ hinzu

$\vdots$

Nachteile des 2. Algorithmus

- I.A. wird eine unnötig große Menge von Regeln berechnet
  - Das erzeugte TES enthält redundante Regeln
  - Erzeugte Regeln können nicht durch später erzeugte Regeln vereinfacht werden
- Der Algorithmus bricht ab sobald eine Regel erzeugt wird die die Terminierung zerstört
  - Diese Regel könnte redundant sein
  - Das Orientieren von normalisierten kritischen Paaren sollte zurück gestellt werden können
- Ein abstraktes Inferenzsystem erlaubt dies (und mehr)

Inferenzsystem 1/2

Das Inferenzsystem operiert auf Tripeln $(\mathcal{E}, \mathcal{R}, \mathcal{C})$:

- $\mathcal{E}$: Gleichungen
- $\mathcal{R}$: Ein TES
- $\mathcal{C}$: Ein TES dessen Terminierung nachgewiesen werden muss

Ziel: Transformiere $(\mathcal{E}, \emptyset, \emptyset)$ in $(\emptyset, \mathcal{R}, \mathcal{C})$

$$\text{Deduce} \quad \frac{(\mathcal{E}, \mathcal{R}, \mathcal{C})}{(\mathcal{E} \cup \{s \approx t\}, \mathcal{R}, \mathcal{C})} \quad \langle s, t \rangle \in CP(\mathcal{R})$$

$$\text{Delete} \quad \frac{(\mathcal{E} \uplus \{s \approx s\}, \mathcal{R}, \mathcal{C})}{(\mathcal{E}, \mathcal{R}, \mathcal{C})}$$

Inferenzsystem 2/2

Orient
$$\frac{(\mathcal{E} \uplus \{s \approx t\}, \mathcal{R}, \mathcal{C})}{(\mathcal{E}, \mathcal{R} \cup \{s \to t\}, \mathcal{C} \cup \{s \to t\})} \quad \mathcal{C} \cup \{s \to t\} \text{ terminiert}$$

Simplify
$$\frac{(\mathcal{E} \uplus \{s \stackrel{\cdot}{\approx} t\}, \mathcal{R}, \mathcal{C})}{(\mathcal{E} \cup \{u \stackrel{\cdot}{\approx} t\}, \mathcal{R}, \mathcal{C})} \quad s \to_{\mathcal{R}} u$$

Compose
$$\frac{(\mathcal{E}, \mathcal{R} \uplus \{s \to t\}, \mathcal{C})}{(\mathcal{E}, \mathcal{R} \cup \{s \to u\}, \mathcal{C})} \quad t \to_{\mathcal{R}} u$$

Collapse
$$\frac{(\mathcal{E}, \mathcal{R} \uplus \{s \to t\}, \mathcal{C})}{(\mathcal{E} \cup \{u \approx t\}, \mathcal{R}, \mathcal{C})} \quad s \to_{\mathcal{R}} u \text{ mit } l \to r \in \mathcal{R}$$
l kann nicht mit $s \to t$ reduziert werden

Korrektheit

Definition

Eine Ableitung $(\mathcal{E}_0, \emptyset, \emptyset) \vdash (\mathcal{E}_1, \mathcal{R}_1, \mathcal{C}_1) \cdots \vdash (\mathcal{E}_n, \mathcal{R}_n, \mathcal{C}_n)$ ist. . .

- . . . erfolgreich gdw. $\mathcal{E}_n = \emptyset$
- . . . fair gdw. $CP(\mathcal{R}) \subseteq \bigcup_{i=0}^{n} \mathcal{E}_i$

Satz

Wenn $(\mathcal{E}_0, \emptyset, \emptyset) \vdash (\mathcal{E}_1, \mathcal{R}_1, \mathcal{C}_1) \cdots \vdash (\mathcal{E}_n, \mathcal{R}_n, \mathcal{C}_n)$ *eine erfolgreiche faire Ableitung ist so ist* $\mathcal{R}_n$ *äquivalent zu* $\mathcal{E}_0$*, terminierend, und konfluent*

Beispiel

$$(\{h(x,y) \approx f(x),\ h(x,y) \approx f(y),\ g(x,y) \approx h(x,y),\ g(x,y) \approx a\}, \emptyset, \ldots)$$

$\vdash^{4}_{\text{Orient}}$ $(\emptyset, \{h(x,y) \to f(x),\ h(x,y) \to f(y),\ g(x,y) \to h(x,y),\ g(x,y) \to a\}, \ldots)$

$\vdash^{2}_{\text{Deduce}}$ $(\{f(x) \approx f(y),\ h(x,y) \approx a\},$
$\{h(x,y) \to f(x),\ h(x,y) \to f(y),\ g(x,y) \to h(x,y), g(x,y) \to a\}, \ldots)$

$\vdash_{\text{Simplify}}$ $(\{f(x) \approx f(y),\ f(x) \approx a\},$
$\{h(x,y) \to f(x),\ h(x,y) \to f(y),\ g(x,y) \to h(x,y), g(x,y) \to a\}, \ldots)$

$\vdash_{\text{Orient}}$ $(\{f(x) \approx f(y)\},$
$\{h(x,y) \to f(x),\ h(x,y) \to f(y),\ g(x,y) \to h(x,y), g(x,y) \to a,\ f(x) \to a\}, \ldots)$

$\vdash^{2}_{\text{Simplify}}$ $(\{a \approx a\},$
$\{h(x,y) \to f(x),\ h(x,y) \to f(y),\ g(x,y) \to h(x,y), g(x,y) \to a,\ f(x) \to a\}, \ldots)$

$\vdash^{*}_{\text{Compose}}$ $(\{a \approx a\}, \{h(x,y) \to a,\ g(x,y) \to a,\ f(x) \to a\}, \ldots)$

$\vdash_{\text{Delete}}$ $(\emptyset, \{h(x,y) \to a,\ g(x,y) \to a,\ f(x) \to a\}, \ldots)$

Beispiel

Aus den Gruppenaxiomen

$$\begin{aligned} x * (y * z) &\approx (x * y) * z \\ x * \mathsf{e} &\approx x \\ x * \mathsf{i}(x) &\approx \mathsf{e} \end{aligned}$$

wird das TES

$$\begin{aligned} x * (y * z) &\to (x * y) * z \\ x * \mathsf{e} &\to x \\ x * \mathsf{i}(x) &\to \mathsf{e} \\ (x * y) * \mathsf{i}(y) &\to x \\ \mathsf{i}(\mathsf{e}) &\to \mathsf{e} \\ \mathsf{e} * x &\to x \\ \mathsf{i}(\mathsf{i}(x)) &\to x \\ \mathsf{i}(x) * x &\to \mathsf{e} \\ (x * \mathsf{i}(y)) * y &\to x \\ \mathsf{i}(x * y) &\to \mathsf{i}(y) * \mathsf{i}(x) \end{aligned}$$