Termersetzungssysteme
Vorlesung 3

Stephan Falke

Verifikation trifft Algorithmik
Karlsruher Institut für Technologie (KIT)

14.06.2010

Reduktionsordnungen

Definition

Eine fundierte transitive Relation $\succ$ auf $\mathcal{T}(\Sigma, \mathcal{V})$ ist eine Reduktionsordnung gdw.

1. $\succ$ ist stabil, d.h., für alle $s_1 \succ s_2$ und alle Substitutionen σ gilt $s_1\sigma \succ s_2\sigma$
2. $\succ$ ist monoton, d.h., für alle $s_1 \succ s_2$ und alle $f \in \Sigma$ mit Stelligkeit n gilt

$$f(t_1, \ldots, t_{i-1}, s_1, t_{i+1}, \ldots, t_n) \succ f(t_1, \ldots, t_{i-1}, s_2, t_{i+1}, \ldots, t_n)$$

für alle $1 \leq i \leq n$ und alle $t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n$

Satz

Ein TES $\mathcal{R}$ ist terminierend gdw. es eine Reduktionsordnung $\succ$ mit $l \succ r$ für alle $l \to r \in \mathcal{R}$ gibt

Church-Rosser und Konfluenz

Ein TRS $\mathcal{R}$ ist…

- … Church-Rosser gdw. $x \leftrightarrow_{\mathcal{R}}^{*} y \;\Rightarrow\; x \downarrow_{\mathcal{R}} y$

$$\begin{tikzcd} x \arrow[rr, leftrightarrow, "*"] \arrow[dr, dashed, "*"'] & & y \arrow[dl, dashed, "*"] \\ & z & \end{tikzcd}$$

- … konfluent gdw. $y_1 \leftarrow_{\mathcal{R}}^{*} x \rightarrow_{\mathcal{R}}^{*} y_2 \;\Rightarrow\; y_1 \downarrow_{\mathcal{R}} y_2$

$$\begin{tikzcd} & x \arrow[dl, "*"'] \arrow[dr, "*"] & \\ y_1 \arrow[dr, dashed, "*"'] & & y_2 \arrow[dl, dashed, "*"] \\ & z & \end{tikzcd}$$

Äquivalenz und Unentscheidbarkeit

Satz

$\mathcal{R}$ ist Church-Rosser gdw. $\mathcal{R}$ konfluent ist

Satz

Das folgende Problem ist i.A. unentscheidbar:
Eingabe: *Ein TES $\mathcal{R}$*
Frage: *Ist $\mathcal{R}$ konfluent?*

$\Longrightarrow$ Korrekte aber unvollständige Verfahren können trotzdem oft zeigen dass ein TES $\mathcal{R}$ konfluent ist

Lokale Konfluenz

Ein TRS $\mathcal{R}$ ist lokal konfluent gdw. $y_1 \leftarrow_{\mathcal{R}} x \rightarrow_{\mathcal{R}} y_2 \;\Rightarrow\; y_1 \downarrow_{\mathcal{R}} y_2$

$$
\begin{tikzcd}
 & x \arrow[dl] \arrow[dr] & \\
y_1 \arrow[dr, dashed, "*"'] & & y_2 \arrow[dl, dashed, "*"] \\
 & z &
\end{tikzcd}
$$

Satz

Das folgende Problem ist i.A. unentscheidbar:
Eingabe: *Ein TES $\mathcal{R}$*
Frage: *Ist $\mathcal{R}$ lokal konfluent?*

Zusammenhang

Lemma (Newman)

Falls $\mathcal{R}$ terminierend und lokal konfluent ist so ist $\mathcal{R}$ auch konfluent

Ziel der heutigen Vorlesung:

Satz

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

Folgerung

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

Lokale Divergenzen 1/6

Untersuche alle lokalen Divergenzen der Form

$$\begin{array}{ccc} & s & \\ {\scriptstyle l_1 \to r_1} \swarrow & & \searrow {\scriptstyle l_2 \to r_2} \\ t_1 & & t_2 \end{array}$$

auf Zusammenführbarkeit

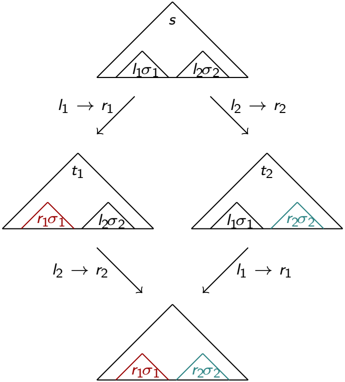
Es gibt $l_i \to r_i \in \mathcal{R}$, Positionen $p_i \in \mathcal{P}os(s)$ und Substitutionen σ_i so dass

$$s|_{p_i} = l_i\sigma_i$$
$$t_i = s[r_i\sigma_i]_{p_i}$$

für $i = 1, 2$

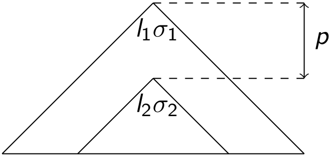
Lokale Divergenzen 2/6

Fall 1: p_1 und p_2 sind unabhängig



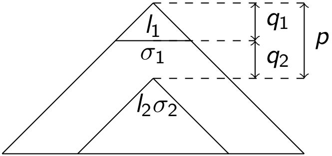
Lokale Divergenzen 3/6

Fall 2: p_1 ist ein Präfix von p_2, d.h., $p_2 = p_1.p$ (p kann leer sein)
O.B.d.A. kann $p_1 = \Lambda$ angenommen werden



Lokale Divergenzen 4/6

Fall 2.1: $l_2\sigma_2$ ist “innerhalb” von σ_1
D.h. $p = q_1.q_2$ so dass $l_1|_{q_1} = x \in \mathcal{V}$



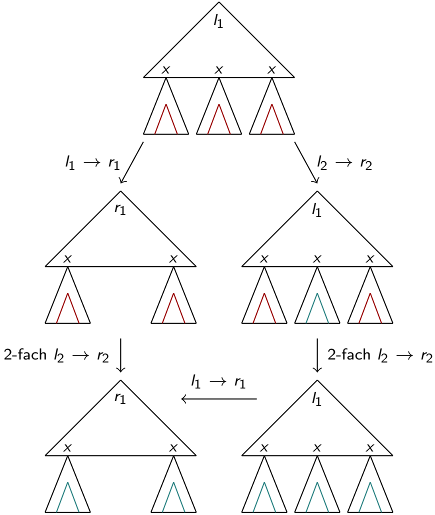
Falls x m-fach in l_1 und n-fach in r_1 auftritt so können t_1 und t_2 zusammengeführt werden indem zunächst die Regel $l_2 \to r_2$

n-fach auf t_1
$(m-1)$-fach auf t_2

und dann die Regel $l_1 \to r_1$ angewendet wird

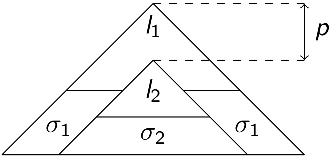
Lokale Divergenzen 5/6

Illustration mit $m = 3$ und $n = 2$ $l_2\sigma_2$ $r_2\sigma_2$



Lokale Divergenzen 6/6

Fall 2.2: l_1 und l_2 sind überlappend
D.h. $p \in \mathcal{P}os(l_1)$ so dass $l_1|_p \notin \mathcal{V}$ und $l_1|_p\sigma_1 = l_2\sigma_2$



Zusammenführbarkeit dieser kritischen Überlappung muss explizit untersucht werden

Kritische Paare 1/2

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:

$$\begin{tikzcd}
 & l_1\sigma \arrow[dl, "l_1 \to r_1"'] \arrow[dr, "l_2 \to r_2"] & \\
r_1\sigma & & l_1\sigma[r_2\sigma]_p
\end{tikzcd}$$

$CP(\mathcal{R})$: 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 $p = \Lambda$)!

Kritische Paare 2/2

$$\begin{array}{llcl}
(1) & \mathsf{f}(\mathsf{f}(x, y), z) & \to & \mathsf{f}(x, \mathsf{f}(y, z)) \\
(2) & \mathsf{f}(\mathsf{i}(x_1), x_1) & \to & \mathsf{e}
\end{array}$$

(1) und (2), $p = 1$: $\sigma = \{x \mapsto \mathsf{i}(x_1), y \mapsto x_1\}$

$$\begin{tikzcd}
& \mathsf{f}(\mathsf{f}(\mathsf{i}(x_1), x_1), z) \arrow[dl] \arrow[dr] & \\
\mathsf{f}(\mathsf{i}(x_1), \mathsf{f}(x_1, z)) & & \mathsf{f}(\mathsf{e}, z)
\end{tikzcd}$$

(1) und (1), $p = 1$: $\sigma = \{x \mapsto \mathsf{f}(x', y'), y \mapsto z'\}$

$$\begin{tikzcd}
& \mathsf{f}(\mathsf{f}(\mathsf{f}(x', y'), z'), z) \arrow[dl] \arrow[dr] & \\
\mathsf{f}(\mathsf{f}(x', y'), \mathsf{f}(z', z)) & & \mathsf{f}(\mathsf{f}(x', \mathsf{f}(y', z')), z)
\end{tikzcd}$$

In den übrigen Fällen ist Unifikation nicht möglich

Kritisches Paar Lemma und Satz

Lemma

Falls $s \rightarrow_{\mathcal{R}} t_1$ *und* $s \rightarrow_{\mathcal{R}} t_2$ *dann* $t_1 \downarrow_{\mathcal{R}} t_2$ *oder* $t_i = s[u_i]_p$ *so dass* $\langle u_1, u_2 \rangle$ *oder* $\langle u_2, u_1 \rangle$ *Instanz eines kritischen Paars ist*

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*

Entscheidbarkeit

Satz

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

Beweis:

- $CP(\mathcal{R})$ ist endlich und kann effizient berechnet werden
- Da $\mathcal{R}$ terminierend ist können Normalformen $\widehat{u}$ und $\widehat{v}$ für alle kritischen Paare $\langle u, v \rangle$ berechnet werden
- Falls $\widehat{u} = \widehat{v}$ für alle kritischen Paare dann ist $\mathcal{R}$ lokal konfluent (warum?)
- Falls $\widehat{u} \neq \widehat{v}$ für ein kritisches Paar dann $\widehat{u} \leftarrow_{\mathcal{R}}^{*} u \leftarrow s \rightarrow v \rightarrow_{\mathcal{R}}^{*} \widehat{v}$ und $\mathcal{R}$ ist nicht lokal konfluent (warum?) $\square$

Beispiel

$$\begin{array}{llcl}
(1) & \mathsf{add}(x, \mathcal{O}) & \to & x \\
(2) & \mathsf{add}(\mathcal{O}, y) & \to & y \\
(3) & \mathsf{add}(x, \mathsf{s}(y)) & \to & \mathsf{s}(\mathsf{add}(x, y)) \\
(4) & \mathsf{add}(\mathsf{s}(x), y) & \to & \mathsf{s}(\mathsf{add}(x, y))
\end{array}$$

(1) und (2):

$$\begin{tikzcd}
 & \mathsf{add}(\mathcal{O}, \mathcal{O}) \arrow[dl, "\mathsf{add}(x, \mathcal{O}) \to x"'] \arrow[dr, "\mathsf{add}(\mathcal{O}, y) \to y"] & \\
\mathcal{O} \arrow[rr, phantom, "="] & & \mathcal{O}
\end{tikzcd}$$

(1) und (4) (analog: (2) und (3)):

$$\begin{tikzcd}
 & \mathsf{add}(\mathsf{s}(x), \mathcal{O}) \arrow[dl, "\mathsf{add}(x, \mathcal{O}) \to x"'] \arrow[dr, "\mathsf{add}(\mathsf{s}(x), y) \to \mathsf{s}(\mathsf{add}(x, y))"] & \\
\mathsf{s}(x) \arrow[drr, phantom, "="] & & \mathsf{s}(\mathsf{add}(x, \mathcal{O})) \arrow[d, "\mathsf{add}(x, \mathcal{O}) \to x"] \\
 & & \mathsf{s}(x)
\end{tikzcd}$$

(3) und (4):

$$\begin{tikzcd}
 & \mathsf{add}(\mathsf{s}(x), \mathsf{s}(y)) \arrow[dl, "\mathsf{add}(\mathsf{s}(x), y) \to \mathsf{s}(\mathsf{add}(x, y))"'] \arrow[dr, "\mathsf{add}(x, \mathsf{s}(y)) \to \mathsf{s}(\mathsf{add}(x, y))"] & \\
\mathsf{s}(\mathsf{add}(x, \mathsf{s}(y))) \arrow[dr, "\mathsf{add}(x, \mathsf{s}(y)) \to \mathsf{s}(\mathsf{add}(x, y))"'] & & \mathsf{s}(\mathsf{add}(\mathsf{s}(x), y)) \arrow[dl, "\mathsf{add}(\mathsf{s}(x), y) \to \mathsf{s}(\mathsf{add}(x, y))"] \\
 & \mathsf{s}(\mathsf{s}(\mathsf{add}(x, y))) &
\end{tikzcd}$$

$\Rightarrow \mathcal{R}$ ist lokal konfluent (und konfluent da terminierend)

Konfluenz für nicht-terminierende TESs

- Für nicht-terminierende TESs ist sogar lokale Konfluenz i.A. unentscheidbar
- Unter bestimmten syntaktischen Einschränkungen an das TES ist Konfluenz allerdings automatisch garantiert

Definition

Ein TES ist orthogonal gdw. es keine kritischen Paare hat und alle linken Seiten linear sind (d.h., keine Variable mehrfach vorkommt)

Satz

Jedes orthogonale TES ist konfluent

Kombinatorische Logik

$$\begin{aligned} \mathsf{S}\ x\ y\ z &\to x\ z\ (y\ z) \\ \mathsf{K}\ x\ y &\to x \\ \mathsf{I}\ x &\to x \end{aligned}$$

nicht terminierend: $\mathsf{S\ I\ I\ (S\ I\ I)} \to \mathsf{I\ (S\ I\ I)\ (I\ (S\ I\ I))}$
$\to \mathsf{S\ I\ I\ (I\ (S\ I\ I))}$
$\to \mathsf{S\ I\ I\ (S\ I\ I)}$

konfluent da orthogonal

Notwendigkeit der Links-Linearität

$$\begin{aligned} \mathsf{f}(x,x) &\to \mathsf{a} \\ \mathsf{f}(x,\mathsf{g}(x)) &\to \mathsf{b} \\ \mathsf{c} &\to \mathsf{g}(\mathsf{c}) \end{aligned}$$

nicht terminierend

keine kritischen Paare

nicht orthogonal da nicht links-linear

nicht konfluent: a und b sind Normalformen und

$$\begin{tikzcd} & \mathsf{f}(\mathsf{c},\mathsf{c}) \arrow[dl] \arrow[dr] & \\ \mathsf{a} & & \mathsf{f}(\mathsf{c},\mathsf{g}(\mathsf{c})) \arrow[d] \\ & & \mathsf{b} \end{tikzcd}$$