Termersetzungssysteme
Vorlesung 2

Stephan Falke

Verifikation trifft Algorithmik
Karlsruher Institut für Technologie (KIT)

03.05.2010

Termersetzungssysteme

- Eine Ersetzungsregel hat die Form $l \to r$ mit $l, r \in \mathcal{T}(\Sigma, \mathcal{V})$ so dass
  - $l \notin \mathcal{V}$
  - $\mathcal{V}(r) \subseteq \mathcal{V}(l)$
- Ein Termersetzungssystem (TES) ist eine Menge von Ersetzungsregeln
- Ersetzungsrelation des TES $\mathcal{R}$:

$$s \to_{\mathcal{R}} t$$

gdw.

es gibt $l \to r \in \mathcal{R}$, $p \in \mathcal{P}os(s)$, σ so dass $s|_p = l\sigma$ und $t = s[r\sigma]_p$

- Das TES $\mathcal{R}$ ist terminierend gdw. $\to_{\mathcal{R}}$ fundiert ist, d.h., gdw. keine unendlichen Ketten $t_0 \to_{\mathcal{R}} t_1 \to_{\mathcal{R}} t_2 \to_{\mathcal{R}} \ldots$ existieren

Unentscheidbarkeit

Satz

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

Satz

Das folgende Problem ist i.A. unentscheidbar:
Eingabe: *Ein TES $\mathcal{R}$ und ein Term t*
Frage: *Sind alle Reduktionen von t mit $\mathcal{R}$ terminierend?*

Beweis: Simulation von Turing-Maschinen durch TESe. □

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

Motivation 1

- $\mathcal{R}$ ist terminierend falls es eine fundierte Relation $\succ$ gibt so dass $s \succ t$ für alle s, t mit $s \to_{\mathcal{R}} t$
- I.A. gibt es unendlich viele Terme s, t mit $s \to_{\mathcal{R}} t$
- Reicht es, $l \succ r$ für alle $l \to r \in \mathcal{R}$ zu verlangen?

$\mathcal{R} = \{\text{endless}(x) \to \text{endless}(\text{s}(x))\}$ ist nicht terminierend

Für die fundierte Relation $\succ = \{ (\text{endless}(x), \text{endless}(\text{s}(x)) \}$ gilt:

$$\text{endless}(x) \succ \text{endless}(\text{s}(x))$$

- Die Instanziierung der Variablen muss berücksichtigt werden: $l \succ r \Rightarrow l\sigma \succ r\sigma$ für alle Substitutionen σ (Stabilität)

Motivation 2

- Reicht dies?

$\mathcal{R} = \{\text{infty}(x) \to \text{s}(\text{infty}(x))\}$ ist nicht terminierend

Fundierte und stabile Relation $\succ = \{ (l,\ r) \mid l = \text{infty}(\ldots), r = \text{s}(\ldots)\}$:

$$\text{infty}(x) \succ \text{s}(\text{infty}(x))$$

- Die Kontexte müssen berücksichtigt werden:
  $l\sigma \succ r\sigma \Rightarrow s[l\sigma]_p \succ s[r\sigma]_p$ für alle $p \in \mathcal{P}os(s)$ (Monotonie)

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 $t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n$

Anwendung

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

Beweis:

"$\Leftarrow$" Da $\succ$ fundiert ist reicht es zu zeigen dass $s \succ t$ für alle $s \to_{\mathcal{R}} t$. Falls $s \to_{\mathcal{R}} t$ dann $s|_p = l\sigma$ und $t = s[r\sigma]_p$ für $l \to r \in \mathcal{R}$, $p \in \mathcal{P}os(s)$ und ein σ. Aus $l \succ r$ folgt $l\sigma \succ r\sigma$ da $\succ$ stabil ist. Aus $l\sigma \succ r\sigma$ folgt $s = s[l\sigma]_p \succ s[r\sigma]_p = t$.

"$\Rightarrow$" Betrachte die Relation $\to^+_{\mathcal{R}}$. Dann ist $\to^+_{\mathcal{R}}$ offensichtlich fundiert da $\mathcal{R}$ terminierend ist. $\to^+_{\mathcal{R}}$ ist trivialerweise stabil und monoton. □

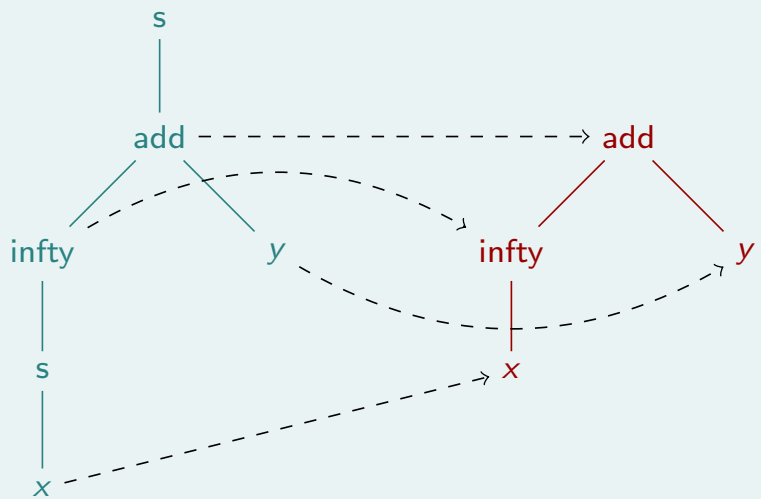
Einbettungsordnung

Definition

Die Einbettungsordnung $\succ_{\text{emb}}$ ist definiert durch $s \succ_{\text{emb}} t$ gdw.

1. $s = f(s_1, \ldots, s_n)$ und $s_i \succeq_{\text{emb}} t$ für ein $1 \leq i \leq n$, oder
2. $s = f(s_1, \ldots, s_n)$, $t = f(t_1, \ldots, t_n)$ und es existiert ein i so dass $s_i \succ_{\text{emb}} t_i$ und $s_j \succeq_{\text{emb}} t_j$ für alle $j \neq i$

$\mathsf{s}(\mathsf{add}(\mathsf{infty}(\mathsf{s}(x)), y)) \succ_{\text{emb}} \mathsf{add}(\mathsf{infty}(x), y)$



$\succ_{\text{emb}}$ ist Reduktionsordnung

Definition

Die Einbettungsordnung $\succ_{\text{emb}}$ ist definiert durch $s \succ_{\text{emb}} t$ gdw.

1. $s = f(s_1, \ldots, s_n)$ und $s_i \succeq_{\text{emb}} t$ für ein $1 \leq i \leq n$, oder
2. $s = f(s_1, \ldots, s_n)$, $t = f(t_1, \ldots, t_n)$ und es existiert ein i so dass $s_i \succ_{\text{emb}} t_i$ und $s_j \succeq_{\text{emb}} t_j$ für alle $j \neq i$

Satz

$\succ_{\text{emb}}$ ist eine Reduktionsordnung

Beweis:

fundiert:	Strukturelle Induktion über s in $s \succ_{\text{emb}} t$ zeigt $\lvert s\rvert > \lvert t\rvert$
transitiv:	Strukturelle Induktion über s in $s \succ_{\text{emb}} t \succ_{\text{emb}} r$
stabil:	Strukturelle Induktion über s in $s \succ_{\text{emb}} t$
monoton:	Folgt direkt aus 2

□

Lexikographische Pfadordnung

Definition

Eine Präzedenz $>$ ist eine strikte Ordnung auf Σ

Definition

Für eine Präzedenz $>$ ist die lexikographische Pfadordnung $\succ_{\text{lpo}}$ definiert durch $s \succ_{\text{lpo}} t$ gdw.

1. $t \in \mathcal{V}(s)$ und $s \neq t$, oder
2. $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$ und
   - (a) $s_i \succeq_{\text{lpo}} t$ für ein $1 \leq i \leq m$, oder
   - (b) $f > g$ und $s > t_j$ für alle $1 \leq j \leq n$, oder
   - (c) $f = g$, $s \succ_{\text{lpo}} t_j$ für alle $1 \leq j \leq n$, und es existiert ein i so dass $s_1 = t_1, \ldots, s_{i-1} = t_{i-1}$ und $s_i \succ_{\text{lpo}} t_i$

Definition

Für eine Präzedenz $>$ ist die lexikographische Pfadordnung $\succ_{\text{lpo}}$ definiert durch $s \succ_{\text{lpo}} t$ gdw.

1. $t \in \mathcal{V}(s)$ und $s \neq t$, oder
2. $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$ und
   - (a) $s_i \succeq_{\text{lpo}} t$ für ein $1 \leq i \leq m$, oder
   - (b) $f > g$ und $s > t_j$ für alle $1 \leq j \leq n$, oder
   - (c) $f = g$, $s \succ_{\text{lpo}} t_j$ für alle $1 \leq j \leq n$, und es existiert ein i so dass $s_1 = t_1, \ldots, s_{i-1} = t_{i-1}$ und $s_i \succ_{\text{lpo}} t_i$

Beispiel

Es gelte ack $>$ s

$$\begin{array}{rcl} \text{ack}(\mathcal{O}, y) & \succ_{\text{lpo}} & \text{s}(y) \\ \text{ack}(\text{s}(x), \mathcal{O}) & \succ_{\text{lpo}} & \text{ack}(x, \text{s}(\mathcal{O})) \\ \text{ack}(\text{s}(x), \text{s}(y)) & \succ_{\text{lpo}} & \text{ack}(x, \text{ack}(\text{s}(x), y)) \end{array}$$

Eigenschaften von $\succ_{\mathrm{lpo}}$

Satz

$\succ_{\mathrm{lpo}}$ *ist eine Reduktionsordnung*

Satz

1. *Für eine gegebene Präzedenz kann in polynomieller Zeit entschieden werden ob* $s \succ_{\mathrm{lpo}} t$ *gilt*
2. *Die Frage ob es eine Präzedenz gibt so dass* $l \succ_{\mathrm{lpo}} r$ *für alle* $l \to r \in \mathcal{R}$ *ist* NP*-vollständig*

Multimengenvergleiche

- Eine Multimenge ist eine "Menge" in der die Anzahl der Vorkommen eines Elements relevant ist
- Multimengenvergleiche: Gegeben Multimengen M, N und eine Ordnung $>$ auf deren Elementen,

$$M >^{\text{mul}} N \quad \text{gdw.} \quad M \neq N \text{ und } \forall n \in N - M.\ \exists m \in M - N.\ m > n$$

$$M = \{5, 3, 1, 1\} >^{\text{mul}} \{4, 3, 3, 1\} = N$$

$$N - M = \{4, 3\}, M - N = \{5, 1\} \text{ und } 5 > 4, 5 > 3$$

Multimengen-Pfadordnung

Definition

Für eine Präzedenz $>$ ist die Multimengen-Pfadordnung $\succ_{\text{mpo}}$ definiert durch $s \succ_{\text{mpo}} t$ gdw.

1. $t \in \mathcal{V}(s)$ und $s \neq t$, oder
2. $s = f(s_1, \ldots, s_m)$, $t = g(t_1, \ldots, t_n)$ und
   - (a) $s_i \succeq_{\text{mpo}} t$ für ein $1 \leq i \leq m$, oder
   - (b) $f > g$ und $s > t_j$ für alle $1 \leq j \leq n$, oder
   - (c) $f = g$ und $\{s_1, \ldots, s_m\} \succ_{\text{mpo}}^{\text{mul}} \{t_1, \ldots, t_n\}$

Es gelte mul $>$ add $>$ s

$$
\begin{array}{rcl}
\text{add}(\mathcal{O}, y) & \succ_{\text{mpo}} & y \\
\text{add}(\text{s}(x), y) & \succ_{\text{mpo}} & \text{s}(\text{add}(x, y)) \\
\text{mul}(\mathcal{O}, y) & \succ_{\text{mpo}} & \mathcal{O} \\
\text{mul}(\text{s}(x), y) & \succ_{\text{mpo}} & \text{add}(y, \text{mul}(y, x))
\end{array}
$$

Eigenschaften von $\succ_{\mathrm{mpo}}$

Satz

$\succ_{\mathrm{mpo}}$ *ist eine Reduktionsordnung*

Satz

1. *Für eine gegebene Präzedenz kann in polynomieller Zeit entschieden werden ob* $s \succ_{\mathrm{mpo}} t$ *gilt*
2. *Die Frage ob es eine Präzedenz gibt so dass* $l \succ_{\mathrm{mpo}} r$ *für alle* $l \to r \in \mathcal{R}$ *ist* NP*-vollständig*

Polynomordnungen: Idee

- Terme werden auf Polynome mit Koeffizienten aus $\mathbb{N}$ abgebildet
- $s \succ_{\mathcal{P}ol} t$ gdw. $\mathcal{P}ol(s\sigma) - \mathcal{P}ol(t\sigma) > 0$ für alle Instanziierungen der Variablen durch Grundterme (d.h., Terme ohne Variablen)
- Hinreichende Bedingung: $\mathcal{P}ol(s) - \mathcal{P}ol(t) > 0$ für alle Instanziierungen der Variablen durch natürliche Zahlen
- Es ist i. A. unentscheidbar ob $\mathcal{P}ol(s) - \mathcal{P}ol(t) > 0$ für alle Instanziierungen der Variablen (Hilberts 10tes Problem)
- Hinreichendes Kriterium: absolute positiveness
  - Sei $\mathcal{P}ol(s) - \mathcal{P}ol(t) = \sum_{\alpha=(\alpha_1,\ldots,\alpha_n)} a_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ (beachte: $a_\alpha \in \mathbb{Z}$)
  - $\mathcal{P}ol(s) - \mathcal{P}ol(t) > 0$ gilt für alle Instanziierungen der Variablen falls $a_{(0,\ldots,0)} > 0$ und $a_\alpha \geq 0$ für alle übrigen α

Polynominterpretationen

- Eine Polynominterpretation weist jedem $f \in \Sigma$ mit Stelligkeit n ein Polynom $\mathcal{P}ol(f) \in \mathbb{N}[X_1, \ldots, X_n]$ zu

$$\mathcal{P}ol(\mathcal{O}) = 0 \quad \mathcal{P}ol(\mathsf{s}) = X_1 + 1 \quad \mathcal{P}ol(\mathsf{add}) = 2 \cdot X_1 + X_2 + 1$$

- Dies weist auch jedem Term ein Polynom zu:
  - $\mathcal{P}ol(x) = x$
  - $\mathcal{P}ol(f(t_1, \ldots, t_n)) = \mathcal{P}ol(f)(\mathcal{P}ol(t_1), \ldots, \mathcal{P}ol(t_n))$

$$\mathcal{P}ol(\mathsf{add}(\mathsf{s}(x), y)) = (2 \cdot X_1 + X_2 + 1)(x + 1, y) = 2 \cdot x + y + 3$$

Polynomordnungen

Definition

Für eine Polynominterpretation $\mathcal{P}ol$ ist die Polynomordnung $\succ_{\mathcal{P}ol}$ definiert durch $s \succ_{\mathcal{P}ol} t$ gdw. $\mathcal{P}ol(s) - \mathcal{P}ol(t) > 0$ für alle Instanziierungen der Variablen durch natürliche Zahlen

Beispiel

$\mathcal{P}ol(\mathcal{O}) = 0 \quad \mathcal{P}ol(\mathsf{s}) = X_1 + 1 \quad \mathcal{P}ol(\mathsf{add}) = 2 \cdot X_1 + X_2 + 1$

$$\begin{aligned} \mathsf{add}(\mathcal{O}, y) &\succ_{\mathcal{P}ol} y && \text{da } (y+1) - y = 1 > 0 \\ \mathsf{add}(\mathsf{s}(x), y) &\succ_{\mathcal{P}ol} \mathsf{s}(\mathsf{add}(x, y)) && \text{da } (2x + y + 3) - (2x + y + 2) = 1 > 0 \end{aligned}$$

Monotone Polynominterpretationen

Definition

Ein Polynom p ist monoton in X_i gdw.

$$p(x_1, \ldots, x_i + 1, \ldots, x_n) - p(x_1, \ldots, x_i, \ldots, x_n) > 0$$

für alle Instanziierungen der Variablen durch natürliche Zahlen
Eine Polynominterpretation $\mathcal{P}ol$ ist monoton gdw. $\mathcal{P}ol(f)$ für alle $f \in \Sigma$ monoton in allen X_i ist

$\mathcal{P}ol(\text{add}) = 2 \cdot X_1 + X_2 + 1$ ist monoton in X_1 und X_2

$$(2x_1 + x_2 + 3) - (2x_1 + x_2 + 1) = 2 > 0$$

$$(2x_1 + x_2 + 2) - (2x_1 + x_2 + 1) = 1 > 0$$

Polynomordnungen als Reduktionsordnungen

Satz

Für eine monotone Polynominterpretation $\mathcal{P}ol$ ist $\succ_{\mathcal{P}ol}$ eine Reduktionsordnung

Beweis:

fundiert:	$>$ auf $\mathbb{N}$ ist fundiert
transitiv:	$>$ auf $\mathbb{N}$ ist transitiv
stabil:	Definition von $\succ_{\mathcal{P}ol}$ benutzt alle Instanziierungen
monoton:	Die Polynome sind monoton

□