Termersetzungssysteme
Vorlesung 1

Stephan Falke

Verifikation trifft Algorithmik
Karlsruher Institut für Technologie (KIT)

19.04.2010

Organisation

Vorlesung: Montag 9:45–11:15 Seminarraum 131

19.04.	03.05.	17.05.	31.05.	14.06.	28.06.

Hausaufgaben: Bearbeitung freiwillig

Literatur:

- F. Baader/T. Nipkow: *Term Rewriting and All That*. Cambridge University Press, 1998
- N. Dershowitz/D. Plaisted: *Rewriting*. Handbook of Automated Reasoning, Volume 1, Seiten 535–610
- E. Ohlebusch: *Advanced Topics in Term Rewriting*. Springer-Verlag, 2002

Termersetzung...

- ... ist die Theorie der schrittweisen Transformation von Objekten
- ...erlaubt effizientes Rechnen und Beweisen mit Gleichungen
- ...ist ein Turing-vollständiges Berechnungsmodel
- ...ist die theoretische Grundlage funktionaler Programmiersprachen

Beispiel (Addition natürlicher Zahlen)

OCaml-Programm:

```
type nat = Zero | S of nat

let rec add x y = match x with
  | Zero -> y
  | S x' -> S (add x' y)
```

Termersetzungssystem $\mathcal{R}$:

$$\Sigma = \{\mathcal{O}, \mathsf{s}, \mathsf{add}\}$$

$$\begin{aligned} \mathsf{add}(\mathcal{O}, y) &\to y \\ \mathsf{add}(\mathsf{s}(x'), y) &\to \mathsf{s}(\mathsf{add}(x', y)) \end{aligned}$$

$$\begin{aligned} \mathsf{add}(\mathsf{add}(\mathsf{s}(\mathcal{O}), \mathsf{s}(\mathsf{s}(\mathcal{O}))), \mathsf{s}(\mathcal{O})) &\to_{\mathcal{R}} \mathsf{add}(\mathsf{s}(\mathsf{add}(\mathcal{O}, \mathsf{s}(\mathsf{s}(\mathcal{O})))), \mathsf{s}(\mathcal{O})) \\ &\to_{\mathcal{R}} \mathsf{add}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathcal{O}))), \mathsf{s}(\mathcal{O})) \\ &\to_{\mathcal{R}} \mathsf{s}(\mathsf{add}(\mathsf{s}(\mathsf{s}(\mathcal{O})), \mathsf{s}(\mathcal{O}))) \\ &\to_{\mathcal{R}} \mathsf{s}(\mathsf{s}(\mathsf{add}(\mathsf{s}(\mathcal{O}), \mathsf{s}(\mathcal{O})))) \\ &\to_{\mathcal{R}} \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{add}(\mathcal{O}, \mathsf{s}(\mathcal{O}))))) \\ &\to_{\mathcal{R}} \mathsf{s}(\mathsf{s}(\mathsf{s}(\mathsf{s}(\mathcal{O})))) \end{aligned}$$

Beispiel (Gruppentheorie 1)

Axiome:

$$\begin{array}{lrcl} (G1) & \mathsf{e} \cdot x & \approx & x \\ (G2) & \mathsf{i}(x) \cdot x & \approx & \mathsf{e} \\ (G3) & (x \cdot y) \cdot z & \approx & x \cdot (y \cdot z) \end{array}$$

$x \cdot \mathsf{i}(x) \approx \mathsf{e}$ folgt aus den Axiomen:

$$\begin{array}{lcl} x \cdot \mathsf{i}(x) & \overset{G1}{\approx} & \mathsf{e} \cdot (x \cdot \mathsf{i}(x)) \\ & \overset{G2}{\approx} & (\mathsf{i}(x \cdot \mathsf{i}(x)) \cdot (x \cdot \mathsf{i}(x))) \cdot (x \cdot \mathsf{i}(x)) \\ & \overset{G3}{\approx} & \mathsf{i}(x \cdot \mathsf{i}(x)) \cdot ((x \cdot \mathsf{i}(x)) \cdot (x \cdot \mathsf{i}(x))) \\ & \overset{G3}{\approx} & \mathsf{i}(x \cdot \mathsf{i}(x)) \cdot (((x \cdot \mathsf{i}(x)) \cdot x) \cdot \mathsf{i}(x)) \\ & \overset{G3}{\approx} & \mathsf{i}(x \cdot \mathsf{i}(x)) \cdot ((x \cdot (\mathsf{i}(x) \cdot x)) \cdot \mathsf{i}(x)) \\ & \overset{G3}{\approx} & \mathsf{i}(x \cdot \mathsf{i}(x)) \cdot (x \cdot ((\mathsf{i}(x) \cdot x) \cdot \mathsf{i}(x))) \\ & \overset{G2}{\approx} & \mathsf{i}(x \cdot \mathsf{i}(x)) \cdot (x \cdot (\mathsf{e} \cdot \mathsf{i}(x))) \\ & \overset{G1}{\approx} & \mathsf{i}(x \cdot \mathsf{i}(x)) \cdot (x \cdot \mathsf{i}(x)) \\ & \overset{G2}{\approx} & \mathsf{e} \end{array}$$

Beispiel (Gruppentheorie 2)

- Idee: Wende Axiome nur in eine Richtung an und vergleiche Normalformen

$$\begin{array}{rcl} \mathsf{e} \cdot x & \to & x \\ \mathsf{i}(x) \cdot x & \to & \mathsf{e} \\ (x \cdot y) \cdot z & \to & x \cdot (y \cdot z) \end{array}$$

- Unvollständig: $x \cdot \mathsf{i}(x)$ und e sind Normalformen
- Lösung: Füge weitere Regeln hinzu

$$\begin{array}{rcl} x \cdot \mathsf{e} & \to & x \\ x \cdot \mathsf{i}(x) & \to & \mathsf{e} \\ \mathsf{i}(\mathsf{i}(x)) & \to & x \\ \mathsf{i}(\mathsf{e}) & \to & \mathsf{e} \\ \mathsf{i}(x \cdot y) & \to & \mathsf{i}(y) \cdot \mathsf{i}(x) \\ \mathsf{i}(x) \cdot (x \cdot y) & \to & y \\ x \cdot (\mathsf{i}(x) \cdot y) & \to & y \end{array}$$

- Vollständig: $s \approx t$ gilt in allen Gruppen gdw. $\mathrm{NF}(s) = \mathrm{NF}(t)$
- Aber: Wie findet man die weiteren Regeln automatisch?

Vorschau

Zentrale Probleme:

- Terminierung: Existenz von Normalformen
  - "Klassische" Methoden: Pfadordnungen und Polynomordnungen
  - "Moderne" Methoden: Dependency Pairs
- Konfluenz: Eindeutigkeit von Normalformen
- Vervollständigung: Automatische Bestimmung eines terminierenden und konfluenten Termersetzungssystems aus einer Menge von Axiomen

Heute:

- (Abstrakte) Reduktionssysteme
- Terme und Termersetzung

Reduktionssysteme

- Ein Reduktionssystem ist ein Paar $(A, \to)$ mit $\to \subseteq A \times A$
- Abgeleitete Relationen:

$\to^0$	$=$	$\{(x,x) \mid x \in A\}$	Identität
$\to^{i+1}$	$=$	$\to^i \circ \to$	$(i+1)$-fache Komposition
$\to^+$	$=$	$\bigcup_{i>0} \to^i$	transitiver Abschluß
$\to^*$	$=$	$\to^+ \cup \to^0$	reflexiv-transitiver Abschluß
$\leftarrow$	$=$	$\{(y,x) \mid x \to y\}$	inverse Relation
$\leftrightarrow$	$=$	$\to \cup \leftarrow$	symmetrischer Abschluß
$\leftrightarrow^+$			transitiv-symmetrischer Abschluß
$\leftrightarrow^*$			reflexiv-transitiv-symmetrischer Abschluß

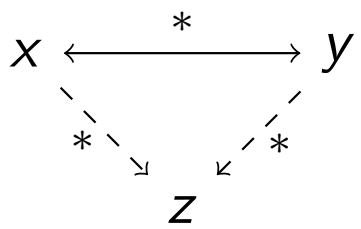
Eigenschaften von Reduktionssystemen 1

Terminologie:

- x ist reduzierbar gdw. $x \longrightarrow y$ für ein y
- y ist eine Normalform von x gdw. $x \longrightarrow^* y$ und y ist nicht reduzierbar
- x und y sind zusammenführbar, $x \downarrow y$, gdw. $x \longrightarrow^* z \longleftarrow^* y$ für ein z
- x und y sind konvertierbar gdw. $x \leftrightarrow^* y$

Die Relation $\longrightarrow$ ist...

- ...terminierend gdw. es keine unendliche Kette $a_0 \longrightarrow a_1 \longrightarrow \ldots$ gibt
- ...Church-Rosser gdw. $x \leftrightarrow^* y \;\Rightarrow\; x \downarrow y$



Satz

Sei $\to$ terminierend und Church-Rosser

1. *Zu jedem x existiert eine eindeutige Normalform $\mathrm{NF}(x)$ so dass $x \to^* \mathrm{NF}(x)$*
2. *$x \leftrightarrow^* y$ gdw. $\mathrm{NF}(x) = \mathrm{NF}(y)$*

Beweis:

1. Die Existenz von Normalformen folgt direkt aus der Terminierung. Für die Eindeutigkeit sei $x_1 \leftarrow^* x \to^* x_2$ so dass x_1 und x_2 Normalformen sind. Da $\to$ Church-Rosser ist folgt $x_1 \downarrow x_2$ und daher $x_1 = x_2$ da x_1 und x_2 Normalformen sind.
2. Beachte dass $\mathrm{NF}(x)$ und $\mathrm{NF}(y)$ eindeutig sind.

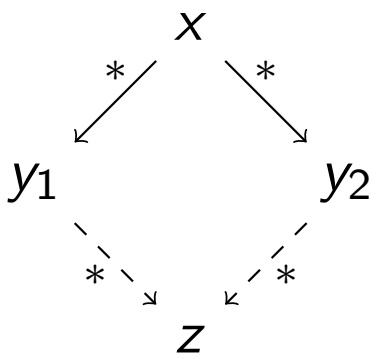
   "$\Rightarrow$" $x \leftrightarrow^* y$ impliziert $\mathrm{NF}(x) \leftrightarrow^* \mathrm{NF}(y)$ und daher $\mathrm{NF}(x) \downarrow \mathrm{NF}(y)$ da $\to$ Church-Rosser ist. Wie oben folgt dann $\mathrm{NF}(x) = \mathrm{NF}(y)$.

   "$\Leftarrow$" Wenn $\mathrm{NF}(x) = \mathrm{NF}(y)$ dann $x \to^* \mathrm{NF}(x) = \mathrm{NF}(y) \leftarrow^* y$ und daher trivialerweise $x \leftrightarrow^* y$. □

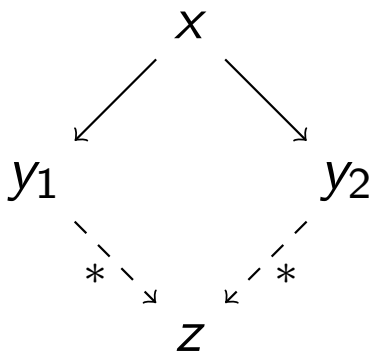
Eigenschaften von Reduktionssystemen 2

Die Relation $\longrightarrow$ ist...

- ...konfluent gdw. $y_1 \longleftarrow^* x \longrightarrow^* y_2 \;\Rightarrow\; y_1 \downarrow y_2$



- ...lokal konfluent gdw. $y_1 \longleftarrow x \longrightarrow y_2 \;\Rightarrow\; y_1 \downarrow y_2$



Zusammenhänge 1

Satz

$\longrightarrow$ ist Church-Rosser gdw. $\longrightarrow$ ist konfluent

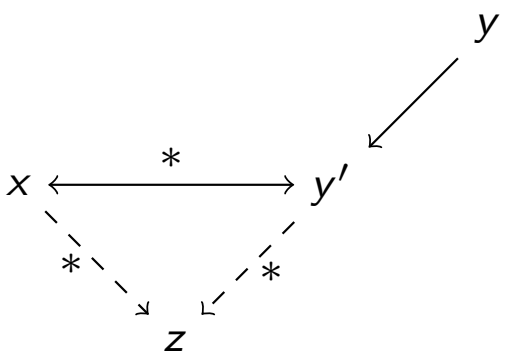
Beweis:

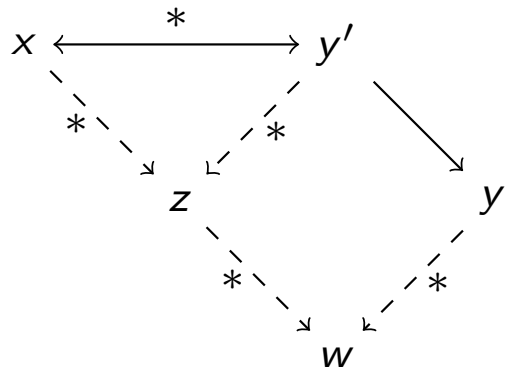
"$\Rightarrow$" Sei $y_1 \longleftarrow^* x \longrightarrow^* y_2$. Dann $y_1 \longleftrightarrow^* y_2$ und daher $y_1 \downarrow y_2$ da $\longrightarrow$ Church-Rosser ist.

"$\Leftarrow$" Sei $x \longleftrightarrow^* y$. Dann wird $x \downarrow y$ per Induktion über die Länge von $x \longleftrightarrow^* y$ gezeigt.

Falls $x = y$ so ist $x \downarrow y$ trivial.

Falls $x \longleftrightarrow^* y' \longleftrightarrow y$ dann folgt $x \downarrow y'$ aus der Induktionshypothese, d.h., $x \longrightarrow^* z \longleftarrow^* y'$ für ein z. Unterscheide zwei Fälle:





Im zweiten Fall existiert w da $\longrightarrow$ konfluent ist. □

Zusammenhänge 2

Lemma (Newman)

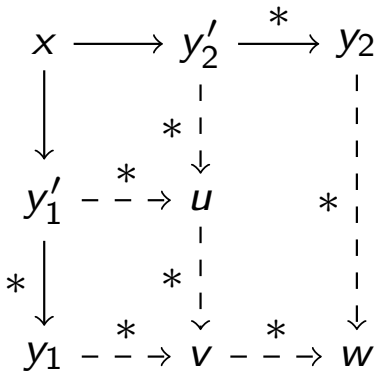
Falls $\longrightarrow$ terminierend und lokal konfluent ist so ist $\longrightarrow$ auch konfluent

Beweis:

Noethersche Induktion bzgl. $\longrightarrow$ um die "lokalisierte" Version des Lemmas zu zeigen. Führe eine Fallunterscheidung in $y_1 \longleftarrow^* x \longrightarrow^* y_2$ durch.

Falls $y_1 = x$ oder $y_2 = x$ dann ist $y_1 \downarrow y_2$ trivial.

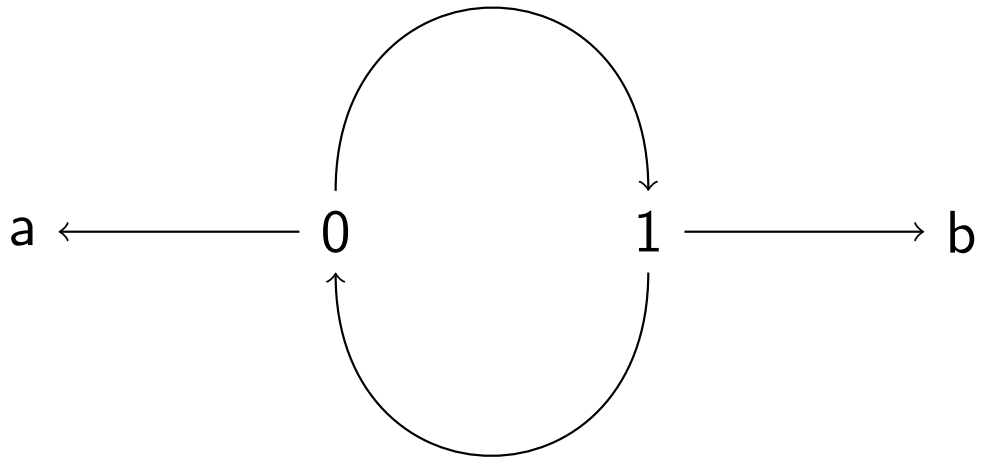
Andernfalls $x \longrightarrow y_1' \longrightarrow^* y_1$ und $x \longrightarrow y_2' \longrightarrow y_2$ und $y_1 \downarrow y_2$ folgt aus lokaler Konfluenz und der Induktionshypothese:



□

Zusammenhänge 3

Terminierung ist für das Lemma von Newman notwendig:



Lokal konfluent aber nicht konfluent (da nicht terminierend)

Terme

- Eine Signatur Σ ist eine Menge von Funktionssymbolen
- Jedes Funktionssymbol $f \in \sigma$ hat eine Stelligkeit $\mathrm{ar}(f)$

$$\Sigma = \{\mathcal{O}, \mathrm{s}, \mathrm{add}\}$$
$$\mathrm{ar}(\mathcal{O}) = 0 \text{ (eine Konstante)}, \mathrm{ar}(\mathrm{s}) = 1, \mathrm{ar}(\mathrm{add}) = 2$$

- $\mathcal{V}$ ist eine Menge von Variablen so dass $\Sigma \cap \mathcal{V} = \emptyset$
- $\mathcal{T}(\Sigma, \mathcal{V})$ ist die Menge von Termen über Σ und $\mathcal{V}$:
  - $\mathcal{V} \subseteq \mathcal{T}(\Sigma, \mathcal{V})$
  - für $f \in \Sigma$ mit $\mathrm{ar}(f) = n$ und $t_1, \ldots, t_n \in \mathcal{T}(\Sigma, \mathcal{V})$ ist $f(t_1, \ldots, t_n) \in \mathcal{T}(\Sigma, \mathcal{V})$

$$x, y, z, \mathcal{O}, \mathrm{s}(\mathcal{O}), \mathrm{s}(\mathrm{s}(x)), \mathrm{add}(\mathrm{s}(x), \mathrm{add}(y, \mathrm{s}(\mathcal{O}))), \ldots$$

Positionen, Teilterme

- Die Menge der Positionen eines Terms ist definiert als
  - $\mathcal{P}os(x) := \{\Lambda\}$
  - $\mathcal{P}os(f(t_1, \ldots, t_n)) := \{\Lambda\} \cup \bigcup_{i=1}^{n} \{i.p \mid p \in \mathcal{P}os(t_i)\}$

$\mathcal{P}os(\mathrm{add}(\mathrm{s}(x), \mathrm{add}(\mathcal{O}, y))) = \{\Lambda,\ 1,\ 1.1,\ 2,\ 2.1,\ 2.2\}$

- Die Teilterm an einer Position eines Terms ist definiert als
  - $s|_\Lambda := s$
  - $f(t_1, \ldots, t_n)|_{i.p} := t_i|_p$

$\mathrm{add}(\mathrm{s}(x), \mathrm{add}(\mathcal{O}, y))|_2 = \mathrm{add}(\mathcal{O}, y) \qquad \mathrm{add}(\mathrm{s}(x), \mathrm{add}(\mathcal{O}, y))|_{2.2} = y$

Ersetzungen, Substitutionen

- Die Ersetzung eines Teilterms durch einen Term ist definiert als
  - $s[t]_\Lambda := t$
  - $f(s_1, \ldots, s_n)[t]_{i.p} := f(s_1, \ldots, s_i[t]_p, \ldots, s_n)$

$$\mathsf{add}(\mathsf{s}(x), \mathsf{add}(\mathcal{O}, y))[y]_2 = \mathsf{add}(\mathsf{s}(x), y)$$

- Eine Substitution ist eine Funktion $\sigma : \mathcal{V} \to \mathcal{T}(\Sigma, \mathcal{V})$
- σ wird auf die natürliche Weise zu einer Funktion von $\mathcal{T}(\Sigma, \mathcal{V})$ nach $\mathcal{T}(\Sigma, \mathcal{V})$ erweitert

$$\mathsf{add}(\mathsf{s}(x), \mathsf{add}(\mathcal{O}, y))\{x \mapsto \mathcal{O}, y \mapsto \mathsf{s}(\mathcal{O})\} = \mathsf{add}(\mathsf{s}(\mathcal{O}), \mathsf{add}(\mathcal{O}, \mathsf{s}(\mathcal{O})))$$

Termersetzungssysteme

- Eine Ersetzungsregel hat die Form $l \to r$ 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 $t = s[r\sigma]_p$

- Ein geeignetes σ kann einfach berechnet werden (Matching)

Syntaktische Unifikation

- Gegeben $s_1 =^? t_1, \ldots, s_n =^? t_n$, finde σ so dass $s_i\sigma = t_i\sigma$ für alle i
- Entscheidbar, allgemeinste Unifikatoren könne mit Hilfe der folgenden Inferenzregeln bestimmt werden:

$$\text{Delete}\ \frac{\{t =^? t\} \cup S}{S}$$

$$\text{Decompose}\ \frac{\{f(t_1, \ldots, t_n) =^? f(u_1, \ldots, u_n)\} \cup S}{\{t_1 =^? u_1, \ldots, t_n =^? u_n\} \cup S}$$

$$\text{Orient}\ \frac{\{t =^? x\} \cup S}{\{x =^? t\} \cup S} \quad \text{falls } t \notin \mathcal{V}$$

$$\text{Eliminate}\ \frac{\{x =^? t\} \cup S}{\{x =^? t\} \cup S\{x \mapsto t\}} \quad \text{falls } x \in \mathcal{V}(S) - \mathcal{V}(t)$$

$$\text{Clash}\ \frac{\{f(t_1, \ldots, t_n) =^? g(u_1, \ldots, u_m)\} \cup S}{\bot} \quad \text{falls } f \neq g$$

$$\text{Occurs}\ \frac{\{x =^? t\} \cup S}{\bot} \quad \text{falls } x \in \mathcal{V}(t) \text{ und } x \neq t$$

Beispiel

$$\text{Eliminate}\ \frac{x =^? \mathrm{f}(\mathrm{a}),\ \mathrm{g}(x,x) =^? \mathrm{g}(x,y)}{x =^? \mathrm{f}(\mathrm{a}),\ \mathrm{g}(\mathrm{f}(\mathrm{a}),\mathrm{f}(\mathrm{a})) =^? \mathrm{g}(\mathrm{f}(\mathrm{a}),y)}$$

$$\text{Decompose}\ \frac{x =^? \mathrm{f}(\mathrm{a}),\ \mathrm{g}(\mathrm{f}(\mathrm{a}),\mathrm{f}(\mathrm{a})) =^? \mathrm{g}(\mathrm{f}(\mathrm{a}),y)}{x =^? \mathrm{f}(\mathrm{a}),\ \mathrm{f}(\mathrm{a}) =^? \mathrm{f}(\mathrm{a}),\ \mathrm{f}(\mathrm{a}) =^? y}$$

$$\text{Delete}\ \frac{x =^? \mathrm{f}(\mathrm{a}),\ \mathrm{f}(\mathrm{a}) =^? \mathrm{f}(\mathrm{a}),\ \mathrm{f}(\mathrm{a}) =^? y}{x =^? \mathrm{f}(\mathrm{a}),\ \mathrm{f}(\mathrm{a}) =^? y}$$

$$\text{Orient}\ \frac{x =^? \mathrm{f}(\mathrm{a}),\ \mathrm{f}(\mathrm{a}) =^? y}{x =^? \mathrm{f}(\mathrm{a}),\ y =^? \mathrm{f}(\mathrm{a})}$$

Allgemeinster Unifikator: $\sigma = \{x \mapsto \mathrm{f}(\mathrm{a}),\ y \mapsto \mathrm{f}(\mathrm{a})\}$