Proof Terms for Rewriting

Christina Kohl

supervisor: Aart Middeldorp

Computational Logic
Department of Computer Science
University of Innsbruck

January 10, 2018

Outline

- Motivation
- Proof Terms
  - Basic Operations
  - Overlaps
- Implementation
- Future Work

Outline

- Motivation
- Proof Terms
- Implementation
- Future Work

Motivation

- multisteps as first-order terms
- useful for manipulating and analyzing steps
- used by VvO and RdV to investigate equivalences of reductions
- used by AM and JN to formalize proof of development closure

Goal

- implement operations on proof terms
- provide interactive web interface

Outline

- Motivation
- Proof Terms
  - Basic Operations
  - Overlaps
- Implementation
- Future Work

Reminder

left-linear TRS: left-hand side of every rule does not contain multiple occurrences of the same variable

Reminder

multistep relation $\multimap\!\!\!\to$ is inductively defined

- $x \multimap\!\!\!\to x$ for all variables x
- $f(s_1, \ldots, s_n) \multimap\!\!\!\to f(t_1, \ldots, t_n)$ if $s_i \multimap\!\!\!\to t_i$ for all $1 \leqslant i \leqslant n$
- $\ell\sigma \multimap\!\!\!\to r\tau$ if $\ell \to r \in \mathcal{R}$ and $x\sigma \multimap\!\!\!\to x\tau$ for all variables x

Proof Terms

- rule symbol is associated with each rewrite rule $\ell \to r$ of a (left-linear) TRS R
- proof terms are terms built from function symbols, variables and rule symbols

Notation

- function symbols (of arity greater than 0): $\mathsf{f}, \mathsf{g}, \mathsf{h}$
- constants: $\mathsf{a}, \mathsf{b}, \mathsf{c}$
- variables: x, y, z
- rule symbols: $\alpha, \beta, \gamma, \ldots$

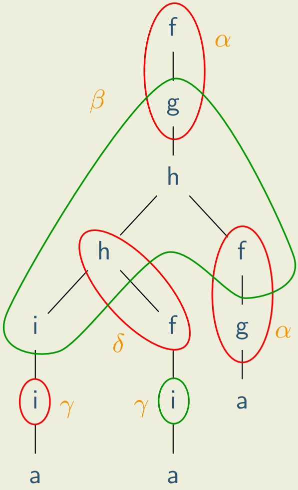
Example

$$\mathsf{f}(\mathsf{g}(x)) \xrightarrow{\alpha} \mathsf{g}(\mathsf{h}(x, \mathsf{i}(\mathsf{a})))$$
$$\mathsf{g}(\mathsf{h}(\mathsf{h}(\mathsf{i}(x), y), \mathsf{f}(z))) \xrightarrow{\beta} \mathsf{h}(\mathsf{h}(y, y), \mathsf{f}(z))$$
$$\mathsf{i}(x) \xrightarrow{\gamma} x$$
$$\mathsf{h}(x, \mathsf{f}(y)) \xrightarrow{\delta} \mathsf{h}(\mathsf{i}(\mathsf{f}(y)), \mathsf{f}(y))$$
$$\mathsf{g}(\mathsf{h}(x, y)) \xrightarrow{\varepsilon} \mathsf{h}(x, y)$$

$$s = \mathsf{f}(\mathsf{g}(\mathsf{h}(\mathsf{h}(\mathsf{i}(\mathsf{i}(\mathsf{a})), \mathsf{f}(\mathsf{i}(\mathsf{a}))), \mathsf{f}(\mathsf{g}(\mathsf{a})))))$$

$$A = \alpha(\mathsf{h}(\delta(\mathsf{i}(\gamma(\mathsf{a})), \mathsf{i}(\mathsf{a})), \alpha(\mathsf{a})))$$

$$B = \mathsf{f}(\beta(\mathsf{i}(\mathsf{a}), \mathsf{f}(\gamma(\mathsf{a})), \mathsf{g}(\mathsf{a})))$$



Outline

Definitions

rule symbol α associated with $\ell \to r$

- $\mathsf{lhs}(\alpha)$ denotes ℓ
- $\mathsf{rhs}(\alpha)$ denotes r
- $\mathsf{var}(\alpha)$ denotes list $(x_1, \ldots, x_n)$ of variables appearing in ℓ in some fixed order
- arity of α is length of $\mathsf{var}(\alpha)$
- $\langle t_1, \ldots, t_n \rangle_\alpha$ denotes substitution $\{x_i \mapsto t_i \mid 1 \leqslant i \leqslant n\}$

Definitions

- source src(A) and target tgt(A) of proof term A

$$
\begin{aligned}
\mathsf{src}(x) &= \mathsf{tgt}(x) = x \\
\mathsf{src}(f(A_1,\ldots,A_n)) &= f(\mathsf{src}(A_1),\ldots,\mathsf{src}(A_n)) \\
\mathsf{src}(\alpha(A_1,\ldots,A_n)) &= \mathsf{lhs}(\alpha)\langle \mathsf{src}(A_1),\ldots,\mathsf{src}(A_n)\rangle_\alpha \\
\mathsf{tgt}(f(A_1,\ldots,A_n)) &= f(\mathsf{tgt}(A_1),\ldots,\mathsf{tgt}(A_n)) \\
\mathsf{tgt}(\alpha(A_1,\ldots,A_n)) &= \mathsf{rhs}(\alpha)\langle \mathsf{tgt}(A_1),\ldots,\mathsf{tgt}(A_n)\rangle_\alpha
\end{aligned}
$$

- proof terms A and B are co-initial if $\mathsf{src}(A) = \mathsf{src}(B)$

Example

Tool

Definition (Orthogonality)

for proof terms A and B define orthogonality predicate $A \perp B$

$$
\begin{aligned}
&& x \perp x \\
f(A_1,\ldots,A_n) \perp f(B_1,\ldots,B_n) &\iff& A_i \perp B_i \text{ for all } 1 \leqslant i \leqslant n \\
\alpha(A_1,\ldots,A_n) \perp \mathsf{lhs}(\alpha)\langle B_1,\ldots,B_n\rangle_\alpha &\iff& A_i \perp B_i \text{ for all } 1 \leqslant i \leqslant n \\
\mathsf{lhs}(\alpha)\langle A_1,\ldots,A_n\rangle_\alpha \perp \alpha(B_1,\ldots,B_n) &\iff& A_i \perp B_i \text{ for all } 1 \leqslant i \leqslant n
\end{aligned}
$$

Example

Tool

Definition (Join)

for proof terms A and B define join operation $A \sqcup B$

$$
\begin{aligned}
x \sqcup x &= x \\
f(A_1, \ldots, A_n) \sqcup f(B_1, \ldots, B_n) &= f(A_1 \sqcup B_1, \ldots, A_n \sqcup B_n) \\
\alpha(A_1, \ldots, A_n) \sqcup \alpha(B_1, \ldots, B_n) &= \alpha(A_1 \sqcup B_1, \ldots, A_n \sqcup B_n) \\
\alpha(A_1, \ldots, A_n) \sqcup \mathsf{lhs}(\alpha)\langle B_1, \ldots, B_n\rangle_\alpha &= \alpha(A_1 \sqcup B_1, \ldots, A_n \sqcup B_n) \\
\mathsf{lhs}(\alpha)\langle A_1, \ldots, A_n\rangle_\alpha \sqcup \alpha(B_1, \ldots, B_n) &= \alpha(A_1 \sqcup B_1, \ldots, A_n \sqcup B_n)
\end{aligned}
$$

Example

Tool

Definition (Residual)

for proof terms A and B define residual operation A/B

$$
\begin{aligned}
x/x &= x \\
f(A_1,\ldots,A_n)/f(B_1,\ldots,B_n) &= f(A_1/B_1,\ldots,A_n/B_n) \\
\alpha(A_1,\ldots,A_n)/\alpha(B_1,\ldots,B_n) &= \mathrm{rhs}(\alpha)\langle A_1/B_1,\ldots,A_n/B_n\rangle_\alpha \\
\alpha(A_1,\ldots,A_n)/\mathrm{lhs}(\alpha)\langle B_1,\ldots,B_n\rangle_\alpha &= \alpha(A_1/B_1,\ldots,A_n/B_n) \\
\mathrm{lhs}(\alpha)\langle A_1,\ldots,A_n\rangle_\alpha/\alpha(B_1,\ldots,B_n) &= \mathrm{rhs}(\alpha)\langle A_1/B_1,\ldots,A_n/B_n\rangle_\alpha
\end{aligned}
$$

Example

Tool

Definition (Deletion)

for proof terms A and B define deletion operation $A - B$

$$
\begin{aligned}
x - x &= x \\
f(A_1, \ldots, A_n) - f(B_1, \ldots, B_n) &= f(A_1 - B_1, \ldots, A_n - B_n) \\
\alpha(A_1, \ldots, A_n) - \alpha(B_1, \ldots, B_n) &= \mathsf{lhs}(\alpha)\langle A_1 - B_1, \ldots, A_n - B_n \rangle_\alpha \\
\alpha(A_1, \ldots, A_n) - \mathsf{lhs}(\alpha)\langle B_1, \ldots, B_n \rangle_\alpha &= \alpha(A_1 - B_1, \ldots, A_n - B_n)
\end{aligned}
$$

Example

Tool

Outline

- Motivation
- Proof Terms
  - Basic Operations
  - Overlaps
- Implementation
- Future Work

Definitions

- labeled left-hand side of a rule α:

$$\mathsf{lhs}^\sharp(\alpha) = \varphi(\mathsf{lhs}(\alpha), \alpha, 0)$$

with

$$\varphi(t, \alpha, i) = \begin{cases} t & \text{if } t \in \mathcal{V} \\ f_{\alpha^i}(\varphi(t_1, \alpha, i+1), \dots, \varphi(t_n, \alpha, i+1)) & \text{if } t = f(t_1, \dots, t_n) \end{cases}$$

labels function symbols in $\mathsf{lhs}(\alpha)$ with α and distance from root.

- labeled source of a proof term A:

$$\mathsf{src}^\sharp(A) = \begin{cases} A & \text{if } A \in \mathcal{V} \\ f(\mathsf{src}^\sharp(A_1), \dots, \mathsf{src}^\sharp(A_n)) & \text{if } A = f(A_1, \dots, A_n) \\ \mathsf{lhs}^\sharp(\alpha)\langle \mathsf{src}^\sharp(A_1), \dots, \mathsf{src}^\sharp(A_n)\rangle_\alpha & \text{if } A = \alpha(A_1, \dots, A_n) \end{cases}$$

Example

Tool

Definition (Merge)

for two co-initial proof terms A and B merge(A, B) computes single labeled term in which all function symbols corresponding to redex patterns in A and B are marked

merge$(A, B) = \text{merge}'(\text{src}^\sharp(A), \text{src}^\sharp(B))$ with $\text{merge}'(s, t) = s$ for $s, t \in \mathcal{V}$ and

$$\text{merge}'(s, t) = f_{ab}(\text{merge}'(s_1, t_1), \ldots, \text{merge}'(s_n, t_n))$$

if $s = f_a(s_1, \ldots, s_n)$ and $t = f_b(t_1, \ldots, t_n)$
(unlabeled function symbol f is identified with f_-)

Example

Tool

Measure Overlap

measure amount of overlap between co-initial proof terms A and B

$$\blacktriangle(A, B) = \text{measure}(\text{merge}(A, B))$$

with $\text{measure}(u) = 0$ if $u \in \mathcal{V}$ and

$$\text{measure}(f_{ab}(u_1, \ldots, u_n)) = \begin{cases} 1 + \sum_{i=1}^{n} \text{measure}(u_i) & \text{if } a \neq - \text{ and } b \neq - \\ \sum_{i=1}^{n} \text{measure}(u_i) & \text{otherwise} \end{cases}$$

Example

Tool

Overlaps

- projection functions

$$\ell_1(f_{ab}) = a \qquad\qquad \ell_2(f_{ab}) = b$$

- overlaps(A, B) collects all pairs of overlapping redexes in co-initial proof terms

$$\left\{ (p, \alpha, q, \beta) \;\middle|\; \begin{array}{l} p, q \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(u),\ \ell_1(u(p)) = \alpha^0,\ \ell_2(u(q)) = \beta^0, \text{ and either} \\ p \leqslant q \text{ and } \ell_1(u(q)) = \alpha^{|q \backslash p|} \text{ or } q < p \text{ and } \ell_2(u(p)) = \beta^{|p \backslash q|} \end{array} \right\}$$

with $u = \mathrm{merge}(A, B)$

Example

Tool

Outline

- Motivation
- Proof Terms
- Implementation
- Future Work

Implementation

Scala

vaadin }>

Vaadin

- automates communication between browser and server
- code is written in Java (or Scala) and executed on the server's JVM
- UI is rendered as HTML5 in the browser
- event driven
- CSS themes
- deployed as Java servlet

Outline

Future Work

- extend to arbitrary rewrite sequences (composition of proof terms)
- extend to general rewrite systems (not left-linear)
- add export−to−latex functionality to tool
- add ability to show images to the tool