universität innsbruck

26S lecture 6

Term Rewriting

Philipp Dablander and **Aart Middeldorp**

Outline

Theorem

validity problem for finite ground ESs is decidable — congruence closure

Definitions

- rewrite order is proper order $>$ on terms which is
  - closed under contexts $s > t \implies C[s] > C[t]$ for all contexts C
  - closed under substitutions $s > t \implies s\sigma > t\sigma$ for all substitutions σ
- TRS $\mathcal{R}$ and rewrite order $>$ are compatible if $\ell > r$ for all rules $\ell \to r$ in $\mathcal{R}$
- reduction order is well–founded rewrite order

Theorem

TRS $\mathcal{R}$ is terminating $\iff$ $\mathcal{R} \subseteq >$ for some reduction order $>$

Definitions

- well–founded monotone $\mathcal{F}$–algebra $(\mathcal{A}, >)$ consists of non–empty algebra $\mathcal{A} = (A, \{f_{\mathcal{A}}\}_{f \in \mathcal{F}})$ with well–founded order $>$ on A such that every $f_{\mathcal{A}}$ is strictly monotone in all coordinates:

$$f_{\mathcal{A}}(a_1, \ldots, a_i, \ldots, a_n) > f_{\mathcal{A}}(a_1, \ldots, b, \ldots, a_n)$$

  for all $a_1, \ldots, a_n, b \in A$ and $i \in \{1, \ldots, n\}$ with $a_i > b$
- relation $>_{\mathcal{A}}$ on terms: $s >_{\mathcal{A}} t$ if $[\alpha]_{\mathcal{A}}(s) > [\alpha]_{\mathcal{A}}(t)$ for all assignments α

Lemma

$>_{\mathcal{A}}$ is reduction order for every well–founded monotone algebra $(\mathcal{A}, >)$

Theorem

TRS $\mathcal{R}$ is terminating $\iff$ $\mathcal{R} \subseteq >_{\mathcal{A}}$ for well–founded monotone algebra $(\mathcal{A}, >)$

Definition

TRS $\mathcal{R}$ is polynomially terminating (over $\mathbb{N}$) if $\mathcal{R} \subseteq >_{\mathcal{A}}$ for some well–founded monotone algebra $(\mathcal{A}, >)$ such that

- carrier of $\mathcal{A}$ is $\mathbb{N}$
- $>$ is standard order on $\mathbb{N}$
- $f_{\mathcal{A}} \in \mathbb{Z}[x_1, \ldots, x_n]$ for every n-ary f

Lemma

$\mathcal{R}$ is polynomially terminating over $\mathbb{N}$ $\iff$
$\mathcal{R}$ is polynomially terminating over $\{n \in \mathbb{N} \mid n \geqslant N\}$ for some $N \geqslant 0$

Outline

Definition (Lexicographic Path Order)

- precedence is proper order $>$ on $\mathcal{F}$
- binary relation $>_{\mathsf{lpo}}$ on terms over $\mathcal{F}$: $s >_{\mathsf{lpo}} t$ if $s = f(s_1, \ldots, s_n)$ and either

  ① $t = f(t_1, \ldots, t_n)$ and for some $1 \leqslant i \leqslant n$

  a $s_j = t_j$ for all $1 \leqslant j < i$

  b $s_i >_{\mathsf{lpo}} t_i$

  c $s >_{\mathsf{lpo}} t_j$ for all $i < j \leqslant n$

  ② $t = g(t_1, \ldots, t_m)$ and $f > g$ and $s >_{\mathsf{lpo}} t_j$ for all $1 \leqslant j \leqslant m$

  ③ $s_i >_{\mathsf{lpo}} t$ or $s_i = t$ for some $1 \leqslant i \leqslant n$

Theorem

$>_{\mathsf{lpo}}$ is reduction order if precedence $>$ is well–founded

Examples

1. $$0 + y \to y \qquad 0 \times y \to 0$$
   $$\mathsf{s}(x) + y \to \mathsf{s}(x + y) \qquad \mathsf{s}(x) \times y \to (x \times y) + y$$
   $$\times > + > \mathsf{s}$$

2. $$\mathsf{ack}(0, y) \to \mathsf{s}(y)$$
   $$\mathsf{ack}(\mathsf{s}(x), 0) \to \mathsf{ack}(x, \mathsf{s}(0))$$
   $$\mathsf{ack}(\mathsf{s}(x), \mathsf{s}(y)) \to \mathsf{ack}(x, \mathsf{ack}(\mathsf{s}(x), y))$$
   $$\mathsf{ack} > \mathsf{s}$$

3. $$\mathsf{e} \cdot x \to x \qquad x \cdot \mathsf{e} \to x$$
   $$x^- \cdot x \to \mathsf{e} \qquad x \cdot x^- \to \mathsf{e}$$
   $$(x \cdot y) \cdot z \to x \cdot (y \cdot z) \qquad x^{--} \to x$$
   $$\mathsf{e}^- \to \mathsf{e} \qquad (x \cdot y)^- \to y^- \cdot x^-$$
   $$x^- \cdot (x \cdot y) \to y \qquad x \cdot (x^- \cdot y) \to y$$
   $$^- > \cdot > \mathsf{e}$$

Example

$$\dfrac{\mathsf{ack} > \mathsf{s} \qquad \dfrac{}{\mathsf{ack}(0,y) >_{\mathsf{lpo}} y}\,\textcircled{3}}{\mathsf{ack}(0,y) >_{\mathsf{lpo}} \mathsf{s}(y)}\,\textcircled{2}$$

$$\dfrac{\textcircled{3}\,\dfrac{}{\mathsf{s}(x) >_{\mathsf{lpo}} x} \qquad \dfrac{\mathsf{ack} > \mathsf{s} \qquad \dfrac{}{\mathsf{ack}(\mathsf{s}(x),0) >_{\mathsf{lpo}} 0}\,\textcircled{3}}{\mathsf{ack}(\mathsf{s}(x),0) >_{\mathsf{lpo}} \mathsf{s}(0)}\,\textcircled{2}}{\mathsf{ack}(\mathsf{s}(x),0) >_{\mathsf{lpo}} \mathsf{ack}(x,\mathsf{s}(0))}\,\textcircled{1}$$

$$\dfrac{\textcircled{3}\,\dfrac{}{\mathsf{s}(x) >_{\mathsf{lpo}} x} \qquad \dfrac{\mathsf{s}(x) = \mathsf{s}(x) \qquad \dfrac{}{\mathsf{s}(y) >_{\mathsf{lpo}} y}\,\textcircled{3}}{\mathsf{ack}(\mathsf{s}(x),\mathsf{s}(y)) >_{\mathsf{lpo}} \mathsf{ack}(\mathsf{s}(x),y)}\,\textcircled{1}}{\mathsf{ack}(\mathsf{s}(x),\mathsf{s}(y)) >_{\mathsf{lpo}} \mathsf{ack}(x,\mathsf{ack}(\mathsf{s}(x),y))}\,\textcircled{1}$$

Theorem

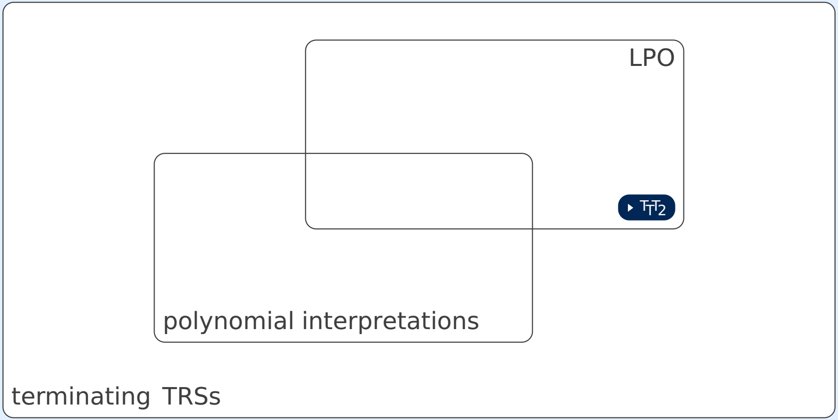
- if $> \subseteq \sqsupset$ then $>_{\mathsf{lpo}} \subseteq \sqsupset_{\mathsf{lpo}}$ (incrementality)
- if $>$ is total then $>_{\mathsf{lpo}}$ is total on ground terms
- following two problems are decidable:

1. instance: finite TRS $\mathcal{R}$, precedence $>$
   question: $\mathcal{R} \subseteq >_{\mathsf{lpo}}$?

2. instance: finite TRS $\mathcal{R}$
   question: $\exists$ precedence $>$ such that $\mathcal{R} \subseteq >_{\mathsf{lpo}}$?

Remark

LPO and polynomial interpretations are incomparable



Outline

Definition (Composition of Substitutions)

composition of substitutions σ and τ: $\sigma\tau = \{x \mapsto \sigma(x)\tau \mid x \in \mathcal{V}\}$

Example

$\sigma = \{x \mapsto \mathsf{s}(y),\ y \mapsto x + \mathsf{s}(0)\}$ $\quad \tau = \{x \mapsto \mathsf{s}(0),\ z \mapsto \mathsf{s}(\mathsf{s}(y))\}$

- $\sigma\tau = \{x \mapsto \mathsf{s}(y),\ y \mapsto \mathsf{s}(0) + \mathsf{s}(0),\ z \mapsto \mathsf{s}(\mathsf{s}(y))\}$
- $\tau\sigma = \{x \mapsto \mathsf{s}(0),\ y \mapsto x + \mathsf{s}(0),\ z \mapsto \mathsf{s}(\mathsf{s}(x + \mathsf{s}(0)))\}$

Lemma (Associativity)

$(\rho\sigma)\tau = \rho(\sigma\tau)$ for all substitutions ρ, σ, τ

Definitions (Subsumption)

- $\lessdot$ subsumption

  $s \lessdot t \iff s\sigma = t$ for some substitution σ "s subsumes t" "t is instance of s"

- $\lessdot$ proper subsumption

  $s \lessdot t \iff s \lessdot t \wedge t \not\lessdot s$

Example

$x + y \lessdot \mathsf{s}(y) + \mathsf{s}(0)$ $\mathsf{s}(x) + y \not\lessdot x + \mathsf{s}(0)$ $\mathsf{s}(x) + y \lessdot \mathsf{s}(x) + x$

Theorem

$\gtrdot$ is well–founded order on terms

Definitions (Renaming)

- $\doteq$ literal similarity

  $s \doteq t \iff s \lessdot t \wedge t \lessdot s$
- variable substitution is substitution from $\mathcal{V}$ to $\mathcal{V}$
- renaming is bijective variable substitution
- terms s and t are variants if $s = t\sigma$ for some renaming σ

Lemma

terms s and t are variants $\iff$ $s \doteq t$

Example

$\mathsf{s}(x) + \mathsf{s}(y + 0) \doteq \mathsf{s}(y) + \mathsf{s}(z + 0)$

$\mathsf{s}(x) + \mathsf{s}(y + 0) \not\doteq \mathsf{s}(x) + \mathsf{s}(x + 0)$

Definition (Unification Problem)

instance: terms s, t

question: $\exists \underbrace{\text{substitution } \sigma}_{\text{unifier}}$ such that $s\sigma = t\sigma$?

Definition

substitution σ is at least as general as τ ($\sigma \lesssim \tau$) if $\sigma\rho = \tau$ for some substitution ρ

Theorem

$\gtrdot$ is well–founded order on substitutions

Definition (Most General Unifier)

most general unifier (mgu) is at least as general as any other unifier

Definition (Unification Rules)

d decomposition

$$\frac{\{f(s_1, \dots, s_n) \approx f(t_1, \dots, t_n)\} \uplus E}{\{s_1 \approx t_1, \dots, s_n \approx t_n\} \cup E}$$

t removal of trivial equations $(x \in \mathcal{V})$

$$\frac{\{x \approx x\} \uplus E}{E}$$

v variable elimination $(x \in \mathcal{V})$

$$\frac{\{x \approx t\} \uplus E}{E\sigma} \quad \text{and} \quad \frac{\{t \approx x\} \uplus E}{E\sigma}$$

if $\underbrace{x \notin \mathcal{V}\mathrm{ar}(t)}_{\text{occurs check}}$ and $\sigma = \{x \mapsto t\}$

Example

$$\{x + (0 + s(y)) \approx s(z) + (0 + x)\}$$

$$\Downarrow \mathsf{d}$$

$$\{x \approx s(z),\ 0 + s(y) \approx 0 + x\}$$

$$\Downarrow \mathsf{v} \quad x \mapsto s(z)$$

$$\{0 + s(y) \approx 0 + s(z)\}$$

$$\Downarrow \mathsf{d}$$

$$\{0 \approx 0,\ s(y) \approx s(z)\}$$

$$\Downarrow \mathsf{d}$$

$$\{s(y) \approx s(z)\}$$

$$\Downarrow \mathsf{d}$$

$$\{y \approx z\}$$

$$\Downarrow \mathsf{v} \quad y \mapsto z$$

$$\varnothing$$

mgu $\{x \mapsto s(z)\}\{y \mapsto z\} = \{x \mapsto s(z),\ y \mapsto z\}$

Theorem

- there are no infinite derivations

$$\{s \approx t\} \Longrightarrow_{\sigma_1} E_1 \Longrightarrow_{\sigma_2} E_2 \Longrightarrow_{\sigma_3} \cdots$$

- if s and t are unifiable then for every maximal derivation

$$\{s \approx t\} \Longrightarrow_{\sigma_1} E_1 \Longrightarrow_{\sigma_2} E_2 \Longrightarrow_{\sigma_3} \cdots \Longrightarrow_{\sigma_n} E_n$$

  - $E_n = \varnothing$
  - $\sigma_1\sigma_2\sigma_3\cdots\sigma_n$ is mgu of s and t

Optional Failure Rules

$$\frac{\{f(s_1,\ldots,s_n) \approx g(t_1,\ldots,t_m)\} \uplus E}{\bot} \qquad \frac{\{x \approx t\} \uplus E}{\bot} \qquad \frac{\{t \approx x\} \uplus E}{\bot}$$

if $x \in \mathcal{V}\mathrm{ar}(t)$ and $x \neq t$

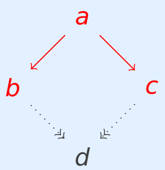
Outline

Newman's Lemma

SN & WCR $\Longrightarrow$ CR

Definition (WCR)

$\forall\, a, b, c$



local peak

$\exists\, d$

Question

how to prove WCR ?

Example

rewrite rules

$$\mathsf{f}(\mathsf{a},\mathsf{g}(x)) \to \mathsf{f}(x,x) \qquad\qquad \mathsf{g}(\mathsf{b}) \to \mathsf{c}$$

three local peaks

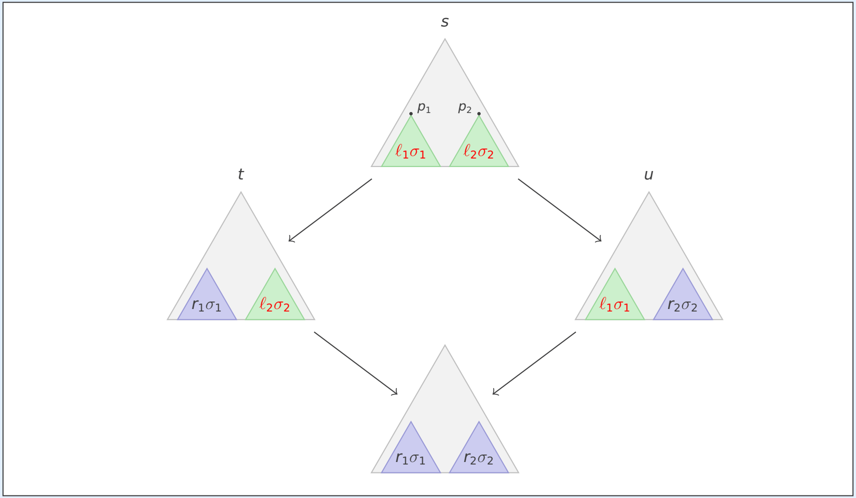
$$\mathsf{f}(\mathsf{g}(\mathsf{b}),\mathsf{g}(\mathsf{b})) \qquad\qquad \mathsf{f}(\mathsf{a},\mathsf{g}(\mathsf{g}(\mathsf{b}))) \qquad\qquad \mathsf{f}(\mathsf{a},\mathsf{g}(\mathsf{b}))$$

$$1 \swarrow \quad \searrow 2 \qquad\qquad 2\,1 \swarrow \quad \searrow \epsilon \qquad\qquad 2 \swarrow \quad \searrow \epsilon$$

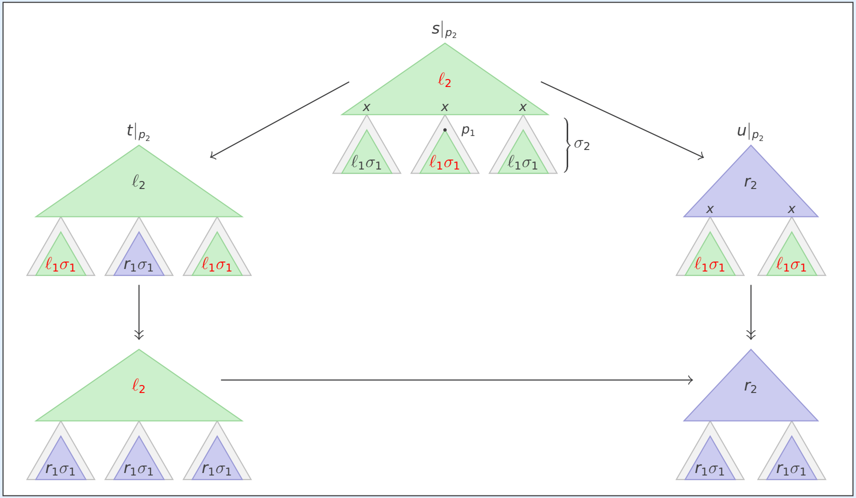
$$\mathsf{f}(\mathsf{c},\mathsf{g}(\mathsf{b})) \quad \mathsf{f}(\mathsf{g}(\mathsf{b}),\mathsf{c}) \qquad \mathsf{f}(\mathsf{a},\mathsf{g}(\mathsf{c})) \quad \mathsf{f}(\mathsf{g}(\mathsf{b}),\mathsf{g}(\mathsf{b})) \qquad \mathsf{f}(\mathsf{a},\mathsf{c}) \quad \mathsf{f}(\mathsf{b},\mathsf{b})$$

parallel redexes	variable overlap	overlapping redexes
non−critical	non−critical	critical

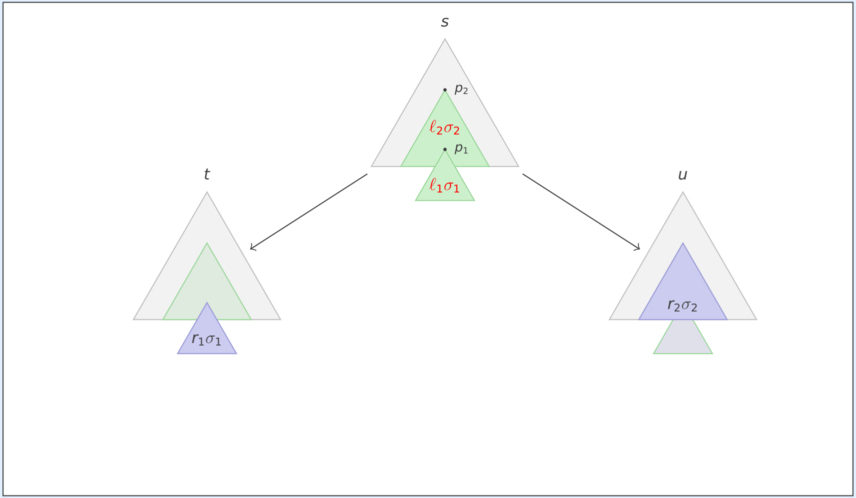
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 1: parallel redexes



local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 2: variable overlap



local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 3: overlapping redexes



Definitions (Critical Pair)

- overlap of TRS $\mathcal{R}$ is triple $\langle \ell_1 \to r_1, p, \ell_2 \to r_2 \rangle$ such that
  1. $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are variants of rewrite rules in $\mathcal{R}$ without common variables
  2. $p \in \mathcal{P}os_{\mathcal{F}}(\ell_2)$
  3. ℓ_1 and $\ell_2|_p$ are unifiable with most general unifier σ
  4. if $p = \epsilon$ then $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not variants
- $\ell_2\sigma[r_1\sigma]_p \leftarrow \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma \to r_2\sigma$ critical peak
- $\ell_2\sigma[r_1\sigma]_p \approx r_2\sigma$ critical pair
- critical pair $s \approx t$ is joinable if $s \downarrow t$

Critical Pair Lemma

TRS is locally confluent $\iff$ all critical pairs are joinable

Example

$$\mathsf{e} \cdot x \to x \qquad x^- \cdot x \to \mathsf{e} \qquad (x \cdot y) \cdot z \to x \cdot (y \cdot z)$$

overlaps

1. $\langle \mathsf{e} \cdot u \to u, 1, (x \cdot y) \cdot z \to x \cdot (y \cdot z) \rangle$
2. $\langle u^- \cdot u \to \mathsf{e}, 1, (x \cdot y) \cdot z \to x \cdot (y \cdot z) \rangle$
3. $\langle (u \cdot v) \cdot w \to u \cdot (v \cdot w), 1, (x \cdot y) \cdot z \to x \cdot (y \cdot z) \rangle$

critical peaks

1. $u \cdot z \xleftarrow{1} (\mathsf{e} \cdot u) \cdot z \to \mathsf{e} \cdot (u \cdot z)$
2. $\mathsf{e} \cdot z \xleftarrow{1} (u^- \cdot u) \cdot z \to u^- \cdot (u \cdot z)$
3. $(u \cdot (v \cdot w)) \cdot z \xleftarrow{1} ((u \cdot v) \cdot w) \cdot z \to (u \cdot v) \cdot (w \cdot z)$

Theorem (Knuth & Bendix 1970)

terminating TRS is confluent $\iff$ all critical pairs are joinable

Outline

Homework Exercises for April 27

1. Exercise 2.44. 1
2. Prove the termination of the TRS of Exercise 3.5. 1
3. Exercise 4.28. 2
4. Exercise 5.3. 2
5. Exercise 5.7. 1

Outline

Lecture Notes

- Section 4.3 (except Lemma 4.3.8 — Corollary 4.3.10)
- Section 2.4 (Definition 2.4.6 — Example 2.4.17)
- Section 2.5
- Section 5.1 (until Corollary 5.1.12)

Important Concepts

- critical pair
- critical pair lemma
- critical peak
- incrementality
- lexicographic path order (LPO)
- literal similarity
- mgu
- overlap
- precedence
- renaming
- subsumption
- unification algorithm
- unifier
- variant