universität innsbruck

26S lecture 7

# Term Rewriting

Philipp Dablander and **Aart Middeldorp**

## Outline





**Definition**

- precedence is proper order $>$ on $\mathcal{F}$
- binary relation $>_{\mathsf{lpo}}$ on terms over $\mathcal{F}$: $s >_{\mathsf{lpo}} t$ if $s = f(s_1, \dots, s_n)$ and either
  - ① $t = f(t_1, \dots, t_n)$ 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 $t = g(t_1, \dots, t_m)$ 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



**Theorem**

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

  instance: finite TRS $\mathcal{R}$

  question: $\exists$ precedence $>$ such that $\mathcal{R} \subseteq >_{\mathsf{lpo}}$ ?

**Definitions**

- $s \leq t \iff s\sigma = t$ for some substitution $\sigma$
- $s < t \iff s \leq t \wedge t \not\leq s$
- $s \doteq t \iff s \leq t \wedge t \leq s$
- substitution $\sigma$ is at least as general as $\tau$ ($\sigma \leq \tau$) if $\sigma\rho = \tau$ for some substitution $\rho$

**Lemma**

$>$ is well–founded order on terms and substitutions

**Definitions**

- 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 $\sigma$
- terms $s$ and $t$ are unifiable if $s\sigma = t\sigma$ for some substitution $\sigma$
- most general unifier (mgu) is at least as general as any other unifier

**Lemma**

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



**Theorem**

unification problem

instance: terms $s$, $t$

question: are $s$ and $t$ unifiable ?

is decidable (and unification algorithm produces most general unifier)

**Definitions**

- overlap 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 without common variables
  2. $p \in \mathcal{P}os_{\mathcal{F}}(\ell_2)$
  3. $\ell_1$ and $\ell_2|_p$ are unifiable with most general unifier $\sigma$
  4. if $p = \epsilon$ then $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not variants
- $\ell_2\sigma[r_1\sigma]_p \xleftarrow{p} \ell_2\sigma \xrightarrow{\epsilon} r_2\sigma$ critical peak $\quad \ell_2\sigma[r_1\sigma]_p \approx r_2\sigma$ 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

**Corollary**

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



# Outline

## Example

TRS $\mathcal{R}$

$$x + 0 \xrightarrow{1} x \qquad x + s(y) \xrightarrow{3} s(x + y) \qquad p(s(x)) \xrightarrow{5} x$$

$$x - 0 \xrightarrow{2} x \qquad x - s(y) \xrightarrow{4} p(x - y) \qquad s(p(x)) \xrightarrow{6} x$$

$$s(x + p(y)) \xrightarrow{7} x + y \qquad p(x - p(y)) \xrightarrow{8} x - y$$

- SN ? (e.g.) LPO with precedence $+ > s$ and $- > p$
- WCR ? 4 critical pairs

$$\overline{x + s(p(y))}: \quad x + y \xleftarrow{6} x + s(p(y)) \xrightarrow{3} s(x + p(y)), \qquad x + y \xleftarrow{7} s(x + p(y))$$

$$\overline{x - s(p(y))}: \quad x - y \xleftarrow{6} x - s(p(y)) \xrightarrow{4} p(x - p(y)), \qquad x - y \xleftarrow{8} p(x - p(y))$$

$$\overline{p(s(p(x)))}: \quad p(x) \xleftarrow{6} p(s(p(x))) \xrightarrow{5} p(x), \qquad p(x) = p(x)$$

$$\overline{s(p(s(x)))}: \quad s(x) \xleftarrow{5} s(p(s(x))) \xrightarrow{6} s(x), \qquad s(x) = s(x)$$

- new rewrite rules preserve termination and do not change $\leftrightarrow^*$



## Example (cont'd)

- new critical pairs

$$\overline{p(s(x + p(y)))}: \quad p(x + y) \xleftarrow{7} p(s(x + p(y))) \xrightarrow{5} x + p(y), \qquad p(x + y) \xleftarrow{9} x + p(y)$$

$$\overline{s(x + p(s(y)))}: \quad s(x + y) \xleftarrow{5} s(x + p(s(y))) \xrightarrow{7} x + s(y), \qquad s(x + y) \xleftarrow{3} x + s(y)$$

$$\overline{s(p(x - p(y)))}: \quad s(x - y) \xleftarrow{8} s(p(x - p(y))) \xrightarrow{6} x - p(y), \qquad s(x - y) \xleftarrow{10} x - p(y)$$

$$\overline{p(x - p(s(y)))}: \quad p(x - y) \xleftarrow{5} p(x - p(s(y))) \xrightarrow{8} x - s(y), \qquad p(x - y) \xleftarrow{4} x - s(y)$$

- new rewrite rules

$$x + p(y) \xrightarrow{9} p(x + y) \qquad x - p(y) \xrightarrow{10} s(x - y)$$

preserve termination (extend LPO precedence with $+ > p$ and $- > s$)



## Example (cont'd)

- new critical pairs

$$\overline{x + s(y + p(z))}: \quad x + (y + z) \xleftarrow{7} x + s(y + p(z)) \xrightarrow{3} s(x + (y + p(z))) \xrightarrow{9} s(x + p(y + z)) \xrightarrow{7} x + (y + z)$$

$$\overline{x - s(y + p(z))}: \quad x - (y + z) \xleftarrow{7} x - s(y + p(z)) \xrightarrow{4} p(x - (y + p(z))) \xrightarrow{9} p(x - p(y + z)) \xrightarrow{8} x - (y + z)$$

$$\overline{x + p(s(y))}: \quad x + y \xleftarrow{5} x + p(s(y)) \xrightarrow{9} p(x + s(y)) \xrightarrow{3} p(s(x + y)) \xrightarrow{5} x + y$$

$$\overline{s(x + p(y - p(z)))}: \quad s(x + (y - z)) \xleftarrow{8} s(x + p(y - p(z))) \xrightarrow{7} x + (y - p(z)) \xrightarrow{10} x + s(y - z) \xrightarrow{3} s(x + (y - z))$$

$$\overline{p(x - p(y - p(z)))}: \quad p(x - (y - z)) \xleftarrow{8} p(x - p(y - p(z))) \xrightarrow{8} x - (y - p(z)) \xrightarrow{10} x - s(y - z) \xrightarrow{4} p(x - (y - z))$$

$$\overline{x - p(s(y))}: \quad x - y \xleftarrow{5} x - p(s(y)) \xrightarrow{10} s(x - s(y)) \xrightarrow{4} s(p(x - y)) \xrightarrow{6} x - y$$



## Example (cont'd)

- new critical pairs

$$\overline{x + p(y - p(z))}: \quad x + (y - z) \xleftarrow{8} x + p(y - p(z)) \xrightarrow{9} p(x + (y - p(z))) \xrightarrow{10} p(x + s(y - z)) \xrightarrow{3} p(s(x + (y - z))) \xrightarrow{5} x + (y - z)$$

$$\overline{x - p(y - p(z))}: \quad x - (y - z) \xleftarrow{8} x - p(y - p(z)) \xrightarrow{10} s(x - (y - p(z))) \xrightarrow{10} s(x - s(y - z)) \xrightarrow{4} s(p(x - (y - z))) \xrightarrow{6} x - (y - z)$$

$$\overline{s(x + p(y))}: \quad s(p(x + y)) \xleftarrow{9} s(x + p(y)) \xrightarrow{7} x + y, \qquad s(p(x + y)) \xrightarrow{6} x + y$$

$$\overline{p(x - p(y))}: \quad p(s(x - y)) \xleftarrow{10} p(x - p(y)) \xrightarrow{8} x - y, \qquad p(s(x - y)) \xrightarrow{5} x - y$$

## Example (cont'd)

TRS $\mathcal{R} = \{1, 2, 3, 4, 5, 6\}$ TRS $\mathcal{S} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$$x + 0 \xrightarrow{1} x \qquad x + \mathsf{s}(y) \xrightarrow{3} \mathsf{s}(x + y) \qquad \mathsf{p}(\mathsf{s}(x)) \xrightarrow{5} x$$
$$x - 0 \xrightarrow{2} x \qquad x - \mathsf{s}(y) \xrightarrow{4} \mathsf{p}(x - y) \qquad \mathsf{s}(\mathsf{p}(x)) \xrightarrow{6} x$$
$$\mathsf{s}(x + \mathsf{p}(y)) \xrightarrow{7} x + y \qquad \mathsf{p}(x - \mathsf{p}(y)) \xrightarrow{8} x - y$$
$$x + \mathsf{p}(y) \xrightarrow{9} \mathsf{p}(x + y) \qquad x - \mathsf{p}(y) \xrightarrow{10} \mathsf{s}(x - y)$$

- $\mathcal{S}$ is SN LPO with precedence $+ > \mathsf{s}, \mathsf{p}$ and $- > \mathsf{s}, \mathsf{p}$
- $\mathcal{S}$ is WCR all critical pairs of $\mathcal{S}$ are joinable
- $\leftrightarrow^*_{\mathcal{S}} = \leftrightarrow^*_{\mathcal{R}}$



## Outline

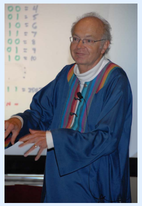




## Knuth–Bendix Completion Procedure

input: ES $\mathcal{E}$ and reduction order $>$

output: complete TRS $\mathcal{R}$ such that $\leftrightarrow^*_{\mathcal{E}} = \leftrightarrow^*_{\mathcal{R}}$



$\mathcal{R} := \varnothing \quad C := \mathcal{E}$

**while** $C \neq \varnothing$ **do**

  select $s \approx t \in C$

  $C := C \setminus \{s \approx t\}$

  compute $\mathcal{R}$–normal forms $s'$ and $t'$ of $s$ and $t$

  **if** $s' \neq t'$ **then**

    **if** $s' > t'$ **then** $\mathcal{S} := \{s' \to t'\}$

    **else if** $t' > s'$ **then** $\mathcal{S} := \{t' \to s'\}$

    **else** failure

    $C := C \cup \mathrm{CP}(\mathcal{R}, \mathcal{S}) \cup \mathrm{CP}(\mathcal{S}, \mathcal{R}) \cup \mathrm{CP}(\mathcal{S})$

    $\mathcal{R} := \mathcal{R} \cup \mathcal{S}$



## Notation

$\mathrm{CP}(\mathcal{R}, \mathcal{S})$ consists of critical pairs originating from overlaps $\langle \alpha, p, \beta \rangle$ with $\alpha \in \mathcal{R}$ and $\beta \in \mathcal{S}$

## Invariants

① $\mathcal{R} \subseteq >$

② $\leftrightarrow^*_{\mathcal{E}} = \leftrightarrow^*_{\mathcal{R} \cup \mathcal{C}}$

③ equations in $\mathrm{CP}(\mathcal{R}) \setminus C$ are joinable in $\mathcal{R}$

## Three Possibilities

Knuth–Bendix completion procedure may

① terminate without failure $\Longrightarrow$ $\mathcal{R}$ is complete and $\leftrightarrow^*_{\mathcal{E}} = \leftrightarrow^*_{\mathcal{R}}$

② terminate with failure

③ not terminate (divergence)

## Three Possibilities

Knuth–Bendix completion procedure may

② terminate with failure

## Example

- rewrite rules

$$\mathsf{f}(x,y) \to \mathsf{g}(x) \qquad \mathsf{f}(x,y) \to \mathsf{h}(y)$$

- two critical pairs

$$\mathsf{g}(x) \approx \mathsf{h}(y) \qquad \mathsf{h}(y) \approx \mathsf{g}(x)$$

- no orientation possible $\implies$ failure



## Three Possibilities

Knuth–Bendix completion procedure may

③ not terminate (divergence)

## Example

- rewrite rules

$$\mathsf{f}(\mathsf{g}(x)) \to \mathsf{g}(\mathsf{h}(x)) \qquad \mathsf{g}(\mathsf{h}(\mathsf{a})) \to \mathsf{f}(\mathsf{b}) \qquad \mathsf{g}(\mathsf{h}(\mathsf{h}(\mathsf{h}(\mathsf{a})))) \to \mathsf{f}(\mathsf{f}(\mathsf{f}(\mathsf{b})))$$
$$\mathsf{g}(\mathsf{a}) \to \mathsf{b} \qquad \mathsf{g}(\mathsf{h}(\mathsf{h}(\mathsf{a}))) \to \mathsf{f}(\mathsf{f}(\mathsf{b})) \qquad \cdots$$

- LPO with precedence $\mathsf{a} > \mathsf{f} > \mathsf{g} > \mathsf{h} > \mathsf{b}$
- critical pairs

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



## Example

- rewrite rules

$$\mathsf{f}(\mathsf{g}(x)) \leftarrow \mathsf{g}(\mathsf{h}(x))$$
$$\mathsf{g}(\mathsf{a}) \to \mathsf{b}$$

- LPO with precedence $\mathsf{g} > \mathsf{f} > \mathsf{b}$
- no critical pairs



## Outline

**Critical Pair Lemma**

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

**Corollary**

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

**Remark**

not all critical pairs need to be considered for inferring confluence

**Definition (Prime Critical Pair)**

- critical pair $t \approx u$ derived from critical peak $t\ {}_p\!\leftarrow s \rightarrow_\epsilon u$ is prime if all proper subterms of $s|_p$ are in normal form
- $\mathrm{PCP}(\mathcal{R})$ denotes set of all prime critical pairs of TRS $\mathcal{R}$



**Example**

TRS

$$\begin{aligned} \mathsf{e} \cdot x &\to x & x \cdot \mathsf{e} &\to x \\ x^- \cdot x &\to \mathsf{e} & x \cdot x^- &\to \mathsf{e} \\ (x \cdot y) \cdot z &\to x \cdot (y \cdot z) & x^{--} &\to x \\ \mathsf{e}^- &\to \mathsf{e} & (x \cdot y)^- &\to y^- \cdot x^- \\ x^- \cdot (x \cdot y) &\to y & x \cdot (x^- \cdot y) &\to y \end{aligned}$$

some critical peaks

1. $y \cdot \mathsf{e} \xleftarrow[2]{} y \cdot (y^- \cdot y^{--}) \xrightarrow[\epsilon]{} y^{--}$ non−prime
2. $\mathsf{e} \cdot \mathsf{e} \xleftarrow[1]{} \mathsf{e}^- \cdot \mathsf{e} \xrightarrow[\epsilon]{} \mathsf{e}$ prime
3. $\mathsf{e}^- \xleftarrow[\epsilon]{} \mathsf{e}^- \cdot \mathsf{e} \xrightarrow[\epsilon]{} \mathsf{e}$ non−prime

**Theorem**

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



## Outline





**Remark**

most problems for finite left−linear right−ground TRSs are decidable

**Theorem**

first−order theory of rewriting is decidable for left−linear right−ground TRSs

**First−Order Theory of Rewriting**

- first−order logic over language $\mathcal{L}$ without function symbols
- $\mathcal{L}$ contains following binary predicate symbols:

  $\to \quad \to^* \quad = \quad \to^+ \quad \downarrow \quad \leftrightarrow \quad \leftrightarrow^* \quad \to^! \quad \nrightarrow\!\!\!\!\!\rightarrow \quad \to_\epsilon \quad \to_{>\epsilon}$

- models of $\mathcal{L}$ are finite TRSs $(\mathcal{F}, \mathcal{R})$ such that
  - $\mathcal{R}$ is left−linear and right−ground
  - $\mathcal{T}(\mathcal{F}) \neq \varnothing$

## First–Order Theory of Rewriting (cont'd)

- set of ground terms serves as domain for variables in formulas over $\mathcal{L}$
- interpretation of predicate symbols in $(\mathcal{F}, \mathcal{R})$ are binary relations over $\mathcal{T}(\mathcal{F})$

| | | | |
|---|---|---|---|
| $\to$ | one–step rewriting $\to_{\mathcal{R}}$ | $\leftrightarrow^*$ | conversion |
| $\to^*$ | relation $\to^*_{\mathcal{R}}$ | $\twoheadrightarrow\!\!\!\!\!+$ | parallel rewriting |
| $=$ | identity relation | $\to_\epsilon$ | one–step rewriting at root |
| $\to^!$ | $s \to^*_{\mathcal{R}} t$ and $t \in \mathsf{NF}(\mathcal{R})$ | $\to_{>\epsilon}$ | one–step rewriting below root |

### Examples

- $\forall t\ \forall u\ \forall v\ \left(t \to^* u \wedge t \to^* v \implies \exists w\ (u \to^* w \wedge v \to^* w)\right)$
- $\forall u\ \forall v\ (t \to^! u \wedge t \to^! v \implies u = v)$
- $\exists s\ \exists t\ \left(s \,\#\!\!\to t \wedge \neg(s \to t) \wedge \neg(s = t)\right)$



## Additional Predicate

- $\mathcal{L}$ is extended with unary predicate symbol $\mathsf{INF}_\circ$

$$\mathsf{INF}_\circ(t) \iff \{u \mid t \circ u\} \text{ is infinite}$$

for every boolean combination $\circ$ of binary predicate symbols in $\mathcal{L}$

### Examples

- $\neg\exists t\ \left(\mathsf{INF}_{\to^*}(t) \vee t \to^+ t\right)$ expresses termination
- $\exists t\ \mathsf{INF}_{\neq}(t)$

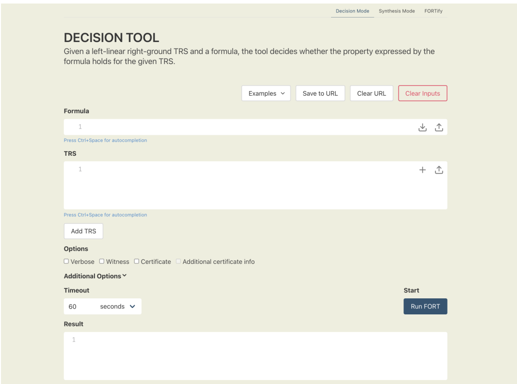
### Remark

- properties are restricted to ground terms
- so $\forall t\ \forall u\ \forall v\ (t \to^* u \wedge t \to^* v \implies u \downarrow v)$ stands for ground–confluence



## Remark

decision procedure for first–order theory of rewriting for left–linear right–ground TRSs is based on tree automata techniques and implemented in FORT






## Outline

## Homework Exercises for May 4

① Exercise 5.5. ②

② Exercise 5.6. ②

③ Exercise 5.14. ③



# Outline





## Lecture Notes

- Section 5.1 (from Definition 5.1.13)
- Section 5.2

## Additional Literature

- F. Rapp and A. Middeldorp, Automating the First–Order Theory of Left–Linear Right–Ground Term Rewrite Systems, Proc. 1st FSCD, LIPIcs 52, pp. 36:1–36:12, 2016
- A. Middeldorp, A. Lochmann and F. Mitterwallner, First–Order Theory of Rewriting for Linear Variable–Separated Rewrite Systems: Automation, Formalization, Certification, Journal of Automated Reasoning 67, article 14, 76 pages, 2023

## Important Concepts

- completion
- divergence
- first–order theory of rewriting
- prime critical pair