universität innsbruck

Term Rewriting

Philipp Dablander and **Aart Middeldorp**

Outline

1. **Summary of Lecture 6**
2. **Completion**
3. **Primality**
4. **First–Order Theory of Rewriting**
5. **Exercises**
6. **Further Reading**

Definition

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

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

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

Lemma

$\gg$ 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 σ
- terms s and t are unifiable if $s\sigma = t\sigma$ for some substitution σ
- 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. $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$
  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
- $\ell_2\sigma[r_1\sigma]_p \xleftarrow{p} \ell_2\sigma \xrightarrow{\epsilon} r_2\sigma$ 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 $\mathcal{R}$

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

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

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

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

$$\overline{x + \underline{\mathsf{s}(\mathsf{p}(y))}} \quad \swarrow^{6} \quad \searrow^{3} \qquad x + y \xleftarrow[7]{} \mathsf{s}(x + \mathsf{p}(y))$$

$$\overline{x - \underline{\mathsf{s}(\mathsf{p}(y))}} \quad \swarrow^{6} \quad \searrow^{4} \qquad x - y \xleftarrow[8]{} \mathsf{p}(x - \mathsf{p}(y))$$

$$\overline{\mathsf{p}(\underline{\mathsf{s}(\mathsf{p}(x))})} \quad \swarrow^{6} \quad \searrow^{5} \qquad \mathsf{p}(x) = \mathsf{p}(x)$$

$$\overline{\mathsf{s}(\underline{\mathsf{p}(\mathsf{s}(x))})} \quad \swarrow^{5} \quad \searrow^{6} \qquad \mathsf{s}(x) = \mathsf{s}(x)$$

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

Example (cont'd)

- new critical pairs

$$\overline{\mathsf{p}(\underline{\mathsf{s}(x+\mathsf{p}(y))})} \qquad {}_{7}\swarrow \quad \searrow_{5} \qquad \mathsf{p}(x+y) \underset{9}{\longleftarrow} x+\mathsf{p}(y)$$

$$\overline{\mathsf{s}(x+\underline{\mathsf{p}(\mathsf{s}(y))})} \qquad {}_{5}\swarrow \quad \searrow_{7} \qquad \mathsf{s}(x+y) \underset{3}{\longleftarrow} x+\mathsf{s}(y)$$

$$\overline{\mathsf{s}(\underline{\mathsf{p}(x-\mathsf{p}(y))})} \qquad {}_{8}\swarrow \quad \searrow_{6} \qquad \mathsf{s}(x-y) \underset{10}{\longleftarrow} x-\mathsf{p}(y)$$

$$\overline{\mathsf{p}(x-\underline{\mathsf{p}(\mathsf{s}(y))})} \qquad {}_{5}\swarrow \quad \searrow_{8} \qquad \mathsf{p}(x-y) \underset{4}{\longleftarrow} x-\mathsf{s}(y)$$

- new rewrite rules

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

preserve termination (extend LPO precedence with $+ > \mathsf{p}$ and $- > \mathsf{s}$)

Example (cont'd)

- new critical pairs

$$x + (y + z) \;{}_{7}\!\swarrow\; \overline{x + \underline{s(y + p(z))}} \;\searrow_{3}\; s(x + (y + p(z)))$$
$$x + (y + z) \;{}_{7}\!\nwarrow\; s(x + p(y + z)) \;\swarrow_{9}\; s(x + (y + p(z)))$$

$$x - (y + z) \;{}_{7}\!\swarrow\; \overline{x - \underline{s(y + p(z))}} \;\searrow_{4}\; p(x - (y + p(z)))$$
$$x - (y + z) \;{}_{8}\!\nwarrow\; p(x - p(y + z)) \;\swarrow_{9}\; p(x - (y + p(z)))$$

$$x + y \;{}_{5}\!\swarrow\; \overline{x + \underline{p(s(y))}} \;\searrow_{9}\; p(x + s(y))$$
$$x + y \;{}_{5}\!\nwarrow\; p(s(x + y)) \;\swarrow_{3}\; p(x + s(y))$$

$$s(x + (y - z)) \;{}_{8}\!\swarrow\; \overline{s(x + \underline{p(y - p(z))})} \;\searrow_{7}\; x + (y - p(z))$$
$$s(x + (y - z)) \;{}_{3}\!\nwarrow\; x + s(y - z) \;\swarrow_{10}\; x + (y - p(z))$$

$$p(x - (y - z)) \;{}_{8}\!\swarrow\; \overline{p(x - \underline{p(y - p(z))})} \;\searrow_{8}\; x - (y - p(z))$$
$$p(x - (y - z)) \;{}_{4}\!\nwarrow\; x - s(y - z) \;\swarrow_{10}\; x - (y - p(z))$$

$$x - y \;{}_{5}\!\swarrow\; \overline{x - \underline{p(s(y))}} \;\searrow_{10}\; s(x - s(y))$$
$$x - y \;{}_{6}\!\nwarrow\; s(p(x - y)) \;\swarrow_{4}\; s(x - s(y))$$

Example (cont'd)

- new critical pairs

$$\begin{array}{ccc} & \overline{x + \underline{\mathsf{p}(y - \mathsf{p}(z))}} & \\ {}^{8}\swarrow & & \searrow^{9} \\ x + (y - z) & & \mathsf{p}(x + (y - \mathsf{p}(z))) \\ 5 \uparrow & & \downarrow 10 \\ \mathsf{p}(\mathsf{s}(x + (y - z))) & \xleftarrow[3]{} & \mathsf{p}(x + \mathsf{s}(y - z)) \end{array}$$

$$\begin{array}{ccc} & \overline{x - \underline{\mathsf{p}(y - \mathsf{p}(z))}} & \\ {}^{8}\swarrow & & \searrow^{10} \\ x - (y - z) & & \mathsf{s}(x - (y - \mathsf{p}(z))) \\ 6 \uparrow & & \downarrow 10 \\ \mathsf{s}(\mathsf{p}(x - (y - z))) & \xleftarrow[4]{} & \mathsf{s}(x - \mathsf{s}(y - z)) \end{array}$$

$$\begin{array}{ccc} & \overline{\mathsf{s}(\underline{x + \mathsf{p}(y)})} & \\ {}^{9}\swarrow & & \searrow^{7} \\ \mathsf{s}(\mathsf{p}(x + y)) & \xrightarrow[6]{} & x + y \end{array}$$

$$\begin{array}{ccc} & \overline{\mathsf{p}(\underline{x - \mathsf{p}(y)})} & \\ {}^{10}\swarrow & & \searrow^{8} \\ \mathsf{p}(\mathsf{s}(x - y)) & \xrightarrow[5]{} & x - y \end{array}$$

Example (cont'd)

TRS $\mathcal{R} = \{1, 2, 3, 4, 5, 6\}$

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

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

- $\mathcal{S}$ 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

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

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

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

Three Possibilities

Knuth–Bendix completion procedure may

① terminate without failure $\implies$ $\mathcal{R}$ 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 $\Longrightarrow$ 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

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

- 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
- 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:

$$\to \qquad \to^* \qquad = \qquad \to^+ \qquad \downarrow \qquad \leftrightarrow \qquad \leftrightarrow^* \qquad \to^! \qquad \twoheadrightarrow\!\!\!\!\!\!\shortmid\shortmid \qquad \to_\epsilon \qquad \to_{>\epsilon}$$

- 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 $\to_{\mathcal{R}}^*$	$\mathrel{+\!\!\!\!\!\!\to}$	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

- $\forall t\ \forall u\ \forall v\ \left(t \to^* u \wedge t \to^* v \implies \exists w\ (u \to^* w \wedge v \to^* w)\right)$
- $\forall u\ \forall v\ (t \to^! u \wedge t \to^! v \implies u = v)$
- $\exists s\ \exists t\ \left(s \mathrel{+\!\!\!\!\!\!\to} t \wedge \neg(s \to t) \wedge \neg(s = t)\right)$

Additional Predicate

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

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

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

Examples

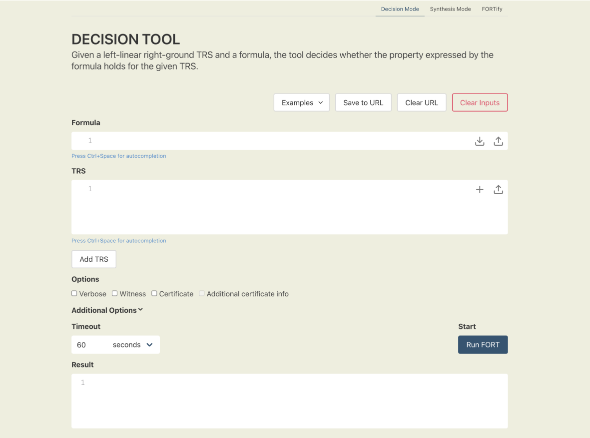
- $\neg\exists t\ \big(\mathsf{INF}_{\to^*}(t) \vee t \to^+ t\big)$ expresses termination
- $\exists t\ \mathsf{INF}_{\neq}(t)$

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