Introduction to Term Rewriting

lecture 5

Aart Middeldorp and Femke van Raamsdonk

Institute of Computer Science
University of Innsbruck

Department of Computer Science
VU Amsterdam

Sunday

introduction, examples, abstract rewriting, equational reasoning, term rewriting

Monday

termination, completion

Tuesday

completion, termination

Wednesday

confluence, modularity, strategies

Thursday

exam, advanced topics

Outline

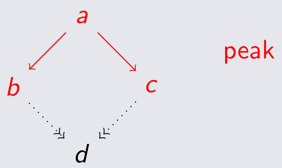
- Critical Pairs
- Unification
- Completion

Newman's Lemma

SN & WCR $\quad\Rightarrow\quad$ CR

Definition (WCR)

$\forall a, b, c$



$\exists d$

Question

how to prove WCR ?

Example

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

three peaks

$$\mathsf{f}(\underline{\mathsf{g}(\mathsf{b})}, \overline{\mathsf{g}(\mathsf{b})}) \quad \xleftarrow{1} \text{ and } \xrightarrow{2} \quad \mathsf{f}(\mathsf{c},\mathsf{g}(\mathsf{b})) \qquad \mathsf{f}(\mathsf{g}(\mathsf{b}),\mathsf{c})$$

parallel redexes

non-critical

$$\overline{\mathsf{f}(\mathsf{a}, \mathsf{g}(\underline{\mathsf{g}(\mathsf{b})}))} \quad \xleftarrow{21} \text{ and } \xrightarrow{\epsilon} \quad \mathsf{f}(\mathsf{a},\mathsf{g}(\mathsf{c})) \qquad \mathsf{f}(\mathsf{g}(\mathsf{b}),\mathsf{g}(\mathsf{b}))$$

variable overlap

non-critical

$$\overline{\mathsf{f}(\mathsf{a}, \underline{\mathsf{g}(\mathsf{b})})} \quad \xleftarrow{2} \text{ and } \xrightarrow{\epsilon} \quad \mathsf{f}(\mathsf{a},\mathsf{c}) \qquad \mathsf{f}(\mathsf{b},\mathsf{b})$$

overlapping redexes

critical

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 rewrite rules 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
- $\ell_2\sigma[r_1\sigma]_p \quad \leftarrow\rtimes\rightarrow \quad r_2\sigma$ critical pair
- critical pair $s \leftarrow\rtimes\rightarrow t$ is convergent if $s \downarrow t$

Critical Pair Lemma (Huet 1980)

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

Example

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

overlaps

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

critical pairs

- $u \cdot z \leftarrow \rtimes \to \mathrm{e} \cdot (u \cdot z)$ convergent
- $\mathrm{e} \cdot z \leftarrow \rtimes \to u^- \cdot (u \cdot z)$ not convergent
- $(u \cdot (v \cdot w)) \cdot z \leftarrow \rtimes \to (u \cdot v) \cdot (w \cdot z)$ convergent

Theorem (Knuth & Bendix 1970)

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

Outline

- Critical Pairs
- Unification
- Completion

Definition

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

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

Definitions

- $\lesssim$ subsumption

  $s \lesssim t \iff \exists\sigma : s\sigma = t$ "s subsumes t" "t is instance of s"

- $\lessdot$ proper subsumption

  $s \lessdot t \iff s \lesssim t \ \wedge\ \neg(t \lesssim s)$

Example

$x + y \lesssim s(y) + s(0)$ $s(x) + y \not\lesssim x + s(0)$ $s(x) + y \lesssim s(x) + x$

Lemma

$\gtrdot$ *is well-founded order on terms*

Definitions

- $\doteq$ literal similarity

  $s \doteq t \iff s \lesssim t \;\wedge\; t \lesssim s$

- 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

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

Definition (Unification Problem)

instance: terms s, t

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

Definition

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

Lemma

$>$ *is well-founded order on substitutions*

Definition

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

Definition (Unification Rules)

d decomposition

$$\frac{E_1,\ f(s_1,\ldots,s_n) \approx f(t_1,\ldots,t_n),\ E_2}{E_1,\ s_1 \approx t_1,\ \ldots,\ s_n \approx t_n,\ E_2}$$

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

$$\frac{E_1,\ x \approx x,\ E_2}{E_1,\ E_2}$$

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

$$\frac{E_1,\ x \approx t,\ E_2}{(E_1,\ E_2)\sigma} \quad \text{and} \quad \frac{E_1,\ t \approx x,\ E_2}{(E_1,\ E_2)\sigma}$$

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

Example

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

$$\mathsf{d} \Downarrow$$

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

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

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

$$y \approx z$$

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

$$\square$$

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

Theorem

- *there are no infinite derivations*

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

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

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

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

Optional Failure Rules

$$\frac{E_1,\ f(s_1,\ldots,s_n) \approx g(t_1,\ldots,t_m),\ E_2}{\bot} \qquad \frac{E_1,\ x \approx t,\ E_2}{\bot} \quad \frac{E_1,\ t \approx x,\ E_2}{\bot}$$

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

Outline

- Critical Pairs
- Unification
- Completion
  - Example
  - Procedure

Example

TRS $\mathcal{R}$

$$
\begin{array}{rrcl@{\qquad}rrcl}
① & x + 0 & \to & x & ② & x - 0 & \to & x \\
③ & x + \mathsf{s}(y) & \to & \mathsf{s}(x + y) & ④ & x - \mathsf{s}(y) & \to & \mathsf{p}(x - y) \\
⑤ & \mathsf{p}(\mathsf{s}(x)) & \to & x & ⑥ & \mathsf{s}(\mathsf{p}(x)) & \to & x \\
⑦ & \mathsf{s}(x + \mathsf{p}(y)) & \to & x + y & ⑧ & \mathsf{p}(x - \mathsf{p}(y)) & \to & x - y
\end{array}
$$

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

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

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

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

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

Example (cont'd)

- added rewrite rules

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

  preserve termination and do not change $\overset{*}{\longleftrightarrow}$

- new critical pairs

$\overline{\mathsf{p}(\underline{\mathsf{s}(x + \mathsf{p}(y))})}$: $\xrightarrow{⑦}$ $\mathsf{p}(x + y)$ and $\xrightarrow{⑤}$ $x + \mathsf{p}(y)$; $\mathsf{p}(x + y) \xleftarrow{⑨} x + \mathsf{p}(y)$

$\overline{\mathsf{s}(x + \underline{\mathsf{p}(\mathsf{s}(y))})}$: $\xrightarrow{⑤}$ $\mathsf{s}(x + y)$ and $\xrightarrow{⑦}$ $x + \mathsf{s}(y)$; $\mathsf{s}(x + y) \xleftarrow{②} x + \mathsf{s}(y)$

$\overline{\mathsf{s}(\underline{\mathsf{p}(x - \mathsf{p}(y))})}$: $\xrightarrow{⑧}$ $\mathsf{s}(x - y)$ and $\xrightarrow{⑥}$ $x - \mathsf{p}(y)$; $\mathsf{s}(x - y) \xleftarrow{⑩} x - \mathsf{p}(y)$

$\overline{\mathsf{p}(x - \underline{\mathsf{p}(\mathsf{s}(y))})}$: $\xrightarrow{⑤}$ $\mathsf{p}(x - y)$ and $\xrightarrow{⑧}$ $x - \mathsf{s}(y)$; $\mathsf{p}(x - y) \xleftarrow{④} x - \mathsf{s}(y)$

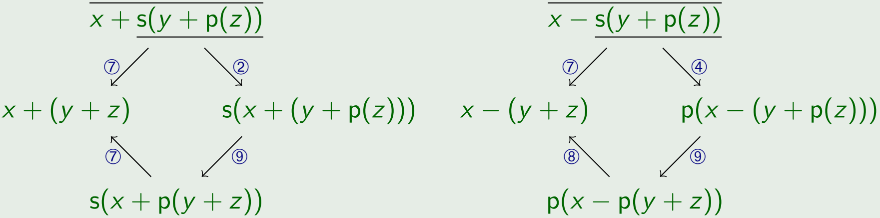
Example (cont'd)

- added rewrite rules

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

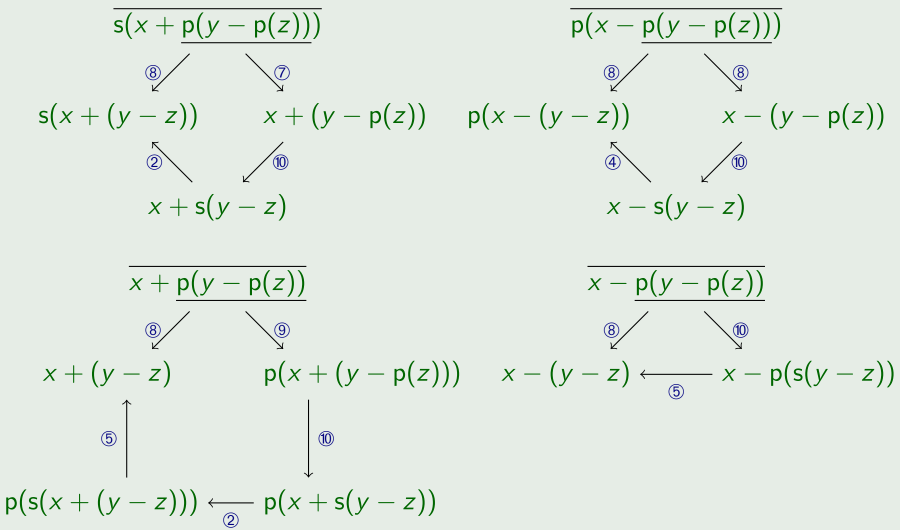
  preserve termination (extend LPO precedence with $+ > \mathsf{p}$ and $- > \mathsf{s}$)

- new critical pairs



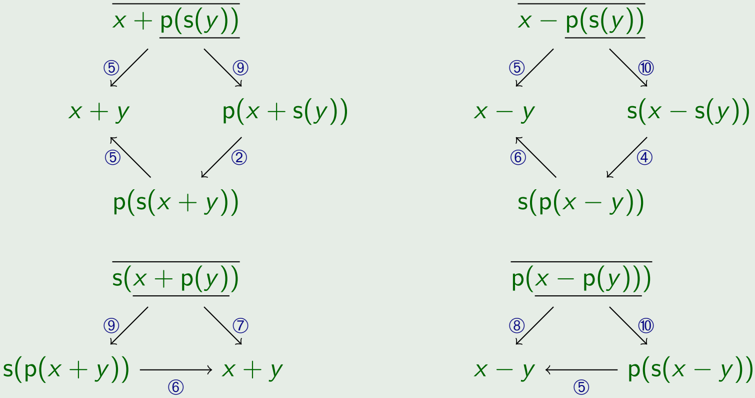
Example (cont'd)

- new critical pairs



Example (cont'd)

- new critical pairs



Example (cont'd)

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

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

- $\mathcal{S}$ 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 convergent
- $\overset{*}{\underset{\mathcal{S}}{\longleftrightarrow}} = \overset{*}{\underset{\mathcal{R}}{\longleftrightarrow}}$

Outline

- Critical Pairs
- Unification
- Completion
  - Example
  - Procedure

Knuth–Bendix Completion Procedure (Simple Version)

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

output complete TRS $\mathcal{R}$ such that $\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}} = \overset{*}{\underset{\mathcal{R}}{\longleftrightarrow}}$

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

while $C \neq \varnothing$ do

  choose $s \approx t \in C \qquad C := C \setminus \{s \approx t\}$

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

  if $s' \neq t'$ then

    if $s' > t'$ then

      $\alpha := s' \qquad \beta := t'$

    else if $t' > s'$ then

      $\alpha := t' \qquad \beta := s'$

    else

      failure

    $\mathcal{R} := \mathcal{R} \cup \{\alpha \to \beta\}$

    $C := C \cup \{e \in \mathrm{CP}(\mathcal{R}) \mid \alpha \to \beta$ was used to generate $e\}$

Invariants

1. $\mathcal{R} \subseteq >$
2. $\xleftrightarrow[\mathcal{E}]{*} = \xleftrightarrow[\mathcal{R}]{*} \cup \xleftrightarrow[C]{*}$
3. equations in $\mathsf{CP}(\mathcal{R}) \setminus C$ are convergent with respect to $\mathcal{R}$

Three Possibilities

Knuth-Bendix completion procedure may

1. terminate without failure $\implies$ $\mathcal{R}$ is complete and $\xleftrightarrow[\mathcal{E}]{*} = \xleftrightarrow[\mathcal{R}]{*}$
2. terminate with failure
3. not terminate (divergence)

Three Possibilities

Knuth-Bendix completion procedure may

2. terminate with failure

Example

- rewrite rules

$$f(x, y) \rightarrow g(x) \qquad f(x, y) \rightarrow h(y)$$

- two critical pairs

$$g(x) \leftarrow \rtimes \rightarrow h(y) \qquad h(y) \leftarrow \rtimes \rightarrow g(x)$$

- no orientation possible $\Longrightarrow$ failure

Three Possibilities

Knuth-Bendix completion procedure may

3. not terminate (divergence)

Example

- rewrite rules

$$f(g(x)) \to g(h(x)) \qquad g(a) \to b$$

$$g(h(a)) \to f(b)$$
$$g(h(h(a))) \to f(f(b))$$
$$g(h(h(h(a)))) \to f(f(f(b)))$$
$$\cdots$$

- LPO with precedence $a > f > g > h > b$
- critical pairs

$$f(b) \leftarrow \rtimes \rightarrow g(h(a))$$
$$f(f(b)) \leftarrow \rtimes \rightarrow g(h(h(a)))$$
$$f(f(f(b))) \leftarrow \rtimes \rightarrow g(h(h(h(a))))$$

Simple Word Problems in Universal Algebras
Donald E. Knuth and Peter Bendix
in: Computational Problems in Abstract Algebra, Pergamon Press, pp. 263 – 297, 1970