universität innsbruck

26S lecture 6

Term Rewriting

Philipp Dablander and **Aart Middeldorp**

Outline

1. **Summary of Lecture 5**
2. **Lexicographic Path Order**
3. **Unification**
4. **Critical Pairs**
5. **Exercises**
6. **Further Reading**

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 $\mathbb{N}$
- $f_{\mathcal{A}} \in \mathbb{Z}[x_1, \dots, x_n]$ 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

1. Summary of Lecture 5
2. **Lexicographic Path Order**
3. Unification
4. Critical Pairs
5. Exercises
6. Further Reading

Definition (Lexicographic Path Order)

- precedence is proper order $>$ on $\mathcal{F}$

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

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 $s = f(s_1, \dots, s_n)$ 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 $i < j \leqslant n$

Definition (Lexicographic Path Order)

- precedence is proper order $>$ on $\mathcal{F}$
- binary relation $>_{\text{lpo}}$ on terms over $\mathcal{F}$: $s >_{\text{lpo}} t$ 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 $s_i >_{\text{lpo}} t_i$

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

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

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 $1 \leqslant i \leqslant n$

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 $s = f(s_1, \dots, s_n)$ 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 $1 \leqslant i \leqslant n$

Example

- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} (x \times y) + y$?

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 $1 \leqslant i \leqslant n$

Example

- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} (x \times y) + y$?

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 $s = f(s_1, \dots, s_n)$ 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 $1 \leqslant i \leqslant n$

Example

- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} (x \times y) + y$? $\times > +$

Definition (Lexicographic Path Order)

- precedence is proper order $>$ on $\mathcal{F}$
- binary relation $>_{\text{lpo}}$ on terms over $\mathcal{F}$: $s >_{\text{lpo}} t$ 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 $s_i >_{\text{lpo}} t_i$

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

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

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

Example

- $\mathsf{s}(x) \times y >_{\text{lpo}} (x \times y) + y$ $\quad \times > +$
- $\mathsf{s}(x) \times y >_{\text{lpo}} x \times y$? $\quad \mathsf{s}(x) \times y >_{\text{lpo}} y$?

Definition (Lexicographic Path Order)

- precedence is proper order $>$ on $\mathcal{F}$
- binary relation $>_{\text{lpo}}$ on terms over $\mathcal{F}$: $s >_{\text{lpo}} t$ 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 $s_i >_{\text{lpo}} t_i$

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

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

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

Example

- $\mathsf{s}(x) \times y >_{\text{lpo}} (x \times y) + y$ $\qquad \times > +$
- $\mathsf{s}(x) \times y >_{\text{lpo}} x \times y$? $\qquad \mathsf{s}(x) \times y >_{\text{lpo}} y$?

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 $s = f(s_1, \dots, s_n)$ 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 $1 \leqslant i \leqslant n$

Example

- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} (x \times y) + y$ $\quad \times > +$
- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} x \times y$? $\quad \mathsf{s}(x) \times y >_{\mathsf{lpo}} y$? $\quad \mathsf{s}(x) >_{\mathsf{lpo}} x$?

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 $1 \leqslant i \leqslant n$

Example

- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} (x \times y) + y$ $\quad \times > +$
- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} x \times y$ $\quad \mathsf{s}(x) \times y >_{\mathsf{lpo}} y$? $\quad \mathsf{s}(x) >_{\mathsf{lpo}} x$?

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 $s = f(s_1, \dots, s_n)$ 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 $1 \leqslant i \leqslant n$

Example

- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} (x \times y) + y$ $\quad \times > +$
- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} x \times y$ $\quad \mathsf{s}(x) \times y >_{\mathsf{lpo}} y$? $\quad \mathsf{s}(x) >_{\mathsf{lpo}} x$?

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 $s = f(s_1, \dots, s_n)$ 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 $1 \leqslant i \leqslant n$

Example

- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} (x \times y) + y$ $\times > +$
- $\mathsf{s}(x) \times y >_{\mathsf{lpo}} x \times y$ $\mathsf{s}(x) \times y >_{\mathsf{lpo}} y$ $\mathsf{s}(x) >_{\mathsf{lpo}} x$?

Definition (Lexicographic Path Order)

- precedence is proper order $>$ on $\mathcal{F}$
- binary relation $>_{\text{lpo}}$ on terms over $\mathcal{F}$: $s >_{\text{lpo}} t$ 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 $s_i >_{\text{lpo}} t_i$

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

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

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

Example

- $\mathsf{s}(x) \times y >_{\text{lpo}} (x \times y) + y$ $\quad\quad \times > +$
- $\mathsf{s}(x) \times y >_{\text{lpo}} x \times y$ $\quad \mathsf{s}(x) \times y >_{\text{lpo}} y$ $\quad \mathsf{s}(x) >_{\text{lpo}} x$

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 $$\begin{aligned} 0 + y &\to y & 0 \times y &\to 0 \\ \mathsf{s}(x) + y &\to \mathsf{s}(x + y) & \mathsf{s}(x) \times y &\to (x \times y) + y \end{aligned}$$

Examples

① $0 + y \to y \qquad 0 \times y \to 0 \qquad\qquad \times > + > \mathsf{s}$

$\mathsf{s}(x) + y \to \mathsf{s}(x + y) \qquad \mathsf{s}(x) \times y \to (x \times y) + y$

Examples

① $$\begin{aligned} 0 + y &\to y & 0 \times y &\to 0 \\ \mathsf{s}(x) + y &\to \mathsf{s}(x + y) & \mathsf{s}(x) \times y &\to (x \times y) + y \end{aligned}$$

$\times > + > \mathsf{s}$

② $$\begin{aligned} \mathsf{ack}(0, y) &\to \mathsf{s}(y) \\ \mathsf{ack}(\mathsf{s}(x), 0) &\to \mathsf{ack}(x, \mathsf{s}(0)) \\ \mathsf{ack}(\mathsf{s}(x), \mathsf{s}(y)) &\to \mathsf{ack}(x, \mathsf{ack}(\mathsf{s}(x), y)) \end{aligned}$$

Examples

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

2. $$\begin{aligned} \mathsf{ack}(0, y) &\to \mathsf{s}(y) \\ \mathsf{ack}(\mathsf{s}(x), 0) &\to \mathsf{ack}(x, \mathsf{s}(0)) \\ \mathsf{ack}(\mathsf{s}(x), \mathsf{s}(y)) &\to \mathsf{ack}(x, \mathsf{ack}(\mathsf{s}(x), y)) \end{aligned} \qquad \mathsf{ack} > \mathsf{s}$$

Examples

①

$$\begin{aligned} 0 + y &\to y & 0 \times y &\to 0 \\ \mathsf{s}(x) + y &\to \mathsf{s}(x + y) & \mathsf{s}(x) \times y &\to (x \times y) + y \end{aligned}$$

$$\times > + > \mathsf{s}$$

②

$$\begin{aligned} \mathsf{ack}(0, y) &\to \mathsf{s}(y) \\ \mathsf{ack}(\mathsf{s}(x), 0) &\to \mathsf{ack}(x, \mathsf{s}(0)) \\ \mathsf{ack}(\mathsf{s}(x), \mathsf{s}(y)) &\to \mathsf{ack}(x, \mathsf{ack}(\mathsf{s}(x), y)) \end{aligned}$$

$$\mathsf{ack} > \mathsf{s}$$

③

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

Examples

① $$\begin{aligned} 0 + y &\to y & 0 \times y &\to 0 \\ \mathsf{s}(x) + y &\to \mathsf{s}(x + y) & \mathsf{s}(x) \times y &\to (x \times y) + y \end{aligned} \qquad \times > + > \mathsf{s}$$

② $$\begin{aligned} \mathsf{ack}(0, y) &\to \mathsf{s}(y) \\ \mathsf{ack}(\mathsf{s}(x), 0) &\to \mathsf{ack}(x, \mathsf{s}(0)) \\ \mathsf{ack}(\mathsf{s}(x), \mathsf{s}(y)) &\to \mathsf{ack}(x, \mathsf{ack}(\mathsf{s}(x), y)) \end{aligned} \qquad \mathsf{ack} > \mathsf{s}$$

③ $$\begin{aligned} \mathsf{e} \cdot x &\to x & x \cdot \mathsf{e} &\to x \\ x^- \cdot x &\to \mathsf{e} & x \cdot x^- &\to \mathsf{e} \\ (x \cdot y) \cdot z &\to x \cdot (y \cdot z) & x^{--} &\to x \\ \mathsf{e}^- &\to \mathsf{e} & (x \cdot y)^- &\to y^- \cdot x^- \\ x^- \cdot (x \cdot y) &\to y & x \cdot (x^- \cdot y) &\to y \end{aligned} \qquad {}^- > \cdot > \mathsf{e}$$

Examples

①

$$\begin{aligned} 0 + y &\to y & 0 \times y &\to 0 \\ \mathsf{s}(x) + y &\to \mathsf{s}(x + y) & \mathsf{s}(x) \times y &\to (x \times y) + y \end{aligned}$$

$$\times > + > \mathsf{s}$$

②

$$\begin{aligned} \mathsf{ack}(0, y) &\to \mathsf{s}(y) \\ \mathsf{ack}(\mathsf{s}(x), 0) &\to \mathsf{ack}(x, \mathsf{s}(0)) \\ \mathsf{ack}(\mathsf{s}(x), \mathsf{s}(y)) &\to \mathsf{ack}(x, \mathsf{ack}(\mathsf{s}(x), y)) \end{aligned}$$

$$\mathsf{ack} > \mathsf{s}$$

③

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

$${}^- > \cdot > \mathsf{e}$$

Example

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

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

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

Theorem

- if $> \subseteq \sqsupset$ then $>_{\mathsf{lpo}} \subseteq \sqsupset_{\mathsf{lpo}}$ (incrementality)

Theorem

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

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:

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

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:

❶ instance: finite TRS $\mathcal{R}$, precedence $>$

question: $\mathcal{R} \subseteq >_{\mathsf{lpo}}$?

❷ instance: finite TRS $\mathcal{R}$

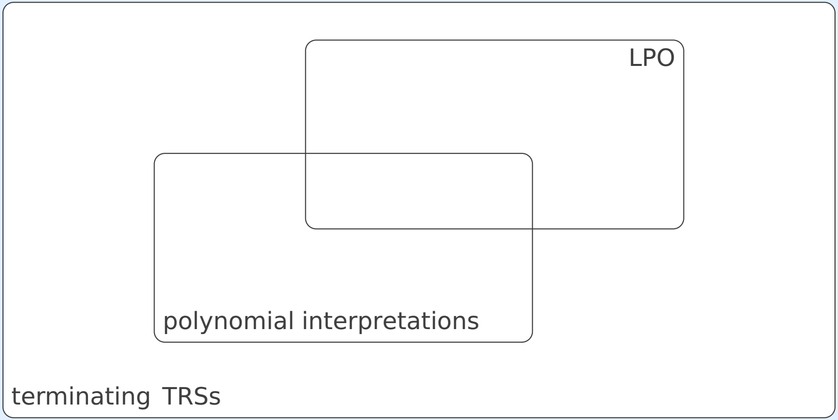
question: $\exists$ precedence $>$ such that $\mathcal{R} \subseteq >_{\mathsf{lpo}}$?

Remark

LPO and polynomial interpretations are incomparable

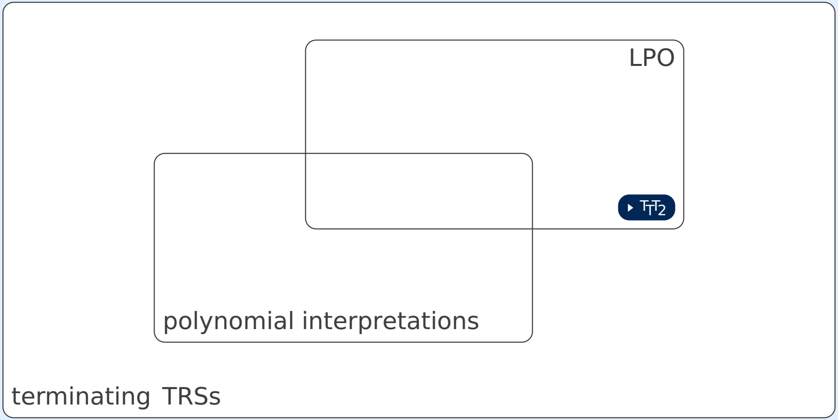
Remark

LPO and polynomial interpretations are incomparable



Remark

LPO and polynomial interpretations are incomparable



LPO

▸ TTT2

polynomial interpretations

terminating TRSs

Outline

1. **Summary of Lecture 5**
2. **Lexicographic Path Order**
3. **Unification**
4. **Critical Pairs**
5. **Exercises**
6. **Further Reading**

Definition (Composition of Substitutions)

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

Definition (Composition of Substitutions)

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

Example

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

Definition (Composition of Substitutions)

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

Example

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

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

Definition (Composition of Substitutions)

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

Example

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

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

Definition (Composition of Substitutions)

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

Example

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

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

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

Definitions (Subsumption)

- $\lessdot$ subsumption

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

Definitions (Subsumption)

- $\lessdot$ subsumption

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

- $\lessdot$ proper subsumption

  $s \lessdot t \quad \Longleftrightarrow \quad s \lessdot t \wedge t \not\lessdot s$

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

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

Definitions (Subsumption)

- $\mathrel{\underline{\lessdot}}$ subsumption

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

- $\lessdot$ proper subsumption

  $s \lessdot t \iff s \mathrel{\underline{\lessdot}} t \wedge t \not\mathrel{\underline{\lessdot}} s$

Example

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

Definitions (Subsumption)

- $\lessdot$ subsumption

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

- $<\!\!\cdot$ proper subsumption

  $s <\!\!\cdot\ t \iff s \lessdot t \wedge t \not\lessdot s$

Example

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

Definitions (Subsumption)

- $\mathrel{\dot{\leqslant}}$ subsumption

  $s \mathrel{\dot{\leqslant}} t \iff s\sigma = t$ for some substitution σ "s subsumes t" "t is instance of s"

- $\lessdot$ proper subsumption

  $s \lessdot t \iff s \mathrel{\dot{\leqslant}} t \wedge t \mathrel{\not\dot{\leqslant}} s$

Example

$x + y \mathrel{\dot{\leqslant}} \mathsf{s}(y) + \mathsf{s}(0)$ $\mathsf{s}(x) + y \mathrel{\not\dot{\leqslant}} x + \mathsf{s}(0)$ $\mathsf{s}(x) + y \mathrel{\dot{\leqslant}} \mathsf{s}(x) + x$

Theorem

$\gtrdot$ is well–founded order on terms

Definitions (Renaming)

- $\doteq$ literal similarity

  $s \doteq t \iff s \mathrel{\dot{\leq}} t \wedge t \mathrel{\dot{\leq}} s$

Definitions (Renaming)

- $\doteq$ literal similarity

  $s \doteq t \iff s \mathrel{\underline{\lessdot}} t \wedge t \mathrel{\underline{\lessdot}} s$

- variable substitution is substitution from $\mathcal{V}$ to $\mathcal{V}$

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

Definitions (Renaming)

- $\doteq$ literal similarity

  $s \doteq t \iff s \mathrel{\dot{\leq}} t \wedge t \mathrel{\dot{\leq}} s$

- 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

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 $\iff$ $s \doteq t$

Definitions (Renaming)

- $\doteq$ literal similarity

  $s \doteq t \iff s \mathrel{\underline{\lessdot}} t \wedge t \mathrel{\underline{\lessdot}} s$
- 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

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

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 (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

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 (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 ($\sigma \leqslant \tau$) 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

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

Definition (Unification Rules)

d decomposition

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

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

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

Definition (Unification Rules)

d decomposition

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

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

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

Example

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

Example

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

$$\mathsf{d} \Downarrow$$

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

Example

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

$$\mathsf{d} \Downarrow$$

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

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

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

Example

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

$$\mathsf{d} \Downarrow$$

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

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

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

$$\mathsf{d} \Downarrow$$

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

Example

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

$$\mathsf{d} \Downarrow$$

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

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

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

Example

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

$$\mathsf{d} \Downarrow$$

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

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

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

Example

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

$$\mathsf{d} \Downarrow$$

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

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

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

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

$$\varnothing$$

Example

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

$$\mathsf{d} \Downarrow$$

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

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

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

$$\mathsf{d} \Downarrow$$

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

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

$$\varnothing$$

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

Theorem

- there are no infinite derivations

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

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

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

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

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

  - $E_n = \varnothing$

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

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

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

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

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

Outline

1. **Summary of Lecture 5**
2. **Lexicographic Path Order**
3. **Unification**
4. **Critical Pairs**
5. **Exercises**
6. **Further Reading**

Newman's Lemma

$\mathrm{SN}\ \&\ \mathrm{WCR} \quad \Longrightarrow \quad \mathrm{CR}$

Newman’s Lemma

SN & WCR $\Longrightarrow$ CR

Definition (WCR)

$$\begin{tikzcd}
\forall\, a, b, c & & a \arrow[dl] \arrow[dr] & \\
& b \arrow[dr, dotted, two heads] & & c \arrow[dl, dotted, two heads] \\
\exists\, d & & d &
\end{tikzcd}$$

Newman's Lemma

$\mathrm{SN} \;\&\; \mathrm{WCR} \quad \Longrightarrow \quad \mathrm{CR}$

Definition (WCR)

$$\begin{tikzcd}
\forall\, a, b, c & & a \arrow[dl] \arrow[dr] & \\
& b \arrow[dr, dotted, two heads] & & c \arrow[dl, dotted, two heads] \\
\exists\, d & & d &
\end{tikzcd}$$

local peak

Newman’s Lemma

SN & WCR $\Longrightarrow$ CR

Definition (WCR)

$$\begin{tikzcd}
\forall\, a, b, c & & a \arrow[dl] \arrow[dr] & \\
& b \arrow[dr, dotted, two heads] & & c \arrow[dl, dotted, two heads] \\
\exists\, d & & d &
\end{tikzcd}$$

local peak

Question

how to prove WCR ?

Example

rewrite rules

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

Example

rewrite rules

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

three local peaks

$$\begin{tikzcd}
& \mathsf{f}(\underline{\mathsf{g}(\mathsf{b})}, \overline{\mathsf{g}(\mathsf{b})}) \arrow[dl, "1"'] \arrow[dr, "2"] & \\
\mathsf{f}(\mathsf{c}, \mathsf{g}(\mathsf{b})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{c})
\end{tikzcd}$$

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

$$\begin{tikzcd}
& \mathsf{f}(\underline{\mathsf{g}(\mathsf{b})}, \overline{\mathsf{g}(\mathsf{b})}) \arrow[dl, "1"'] \arrow[dr, "2"] & & & \overline{\mathsf{f}(\mathsf{a}, \mathsf{g}(\underline{\mathsf{g}(\mathsf{b})}))} \arrow[dl, "21"'] \arrow[dr, "\epsilon"] & \\
\mathsf{f}(\mathsf{c}, \mathsf{g}(\mathsf{b})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{c}) & \mathsf{f}(\mathsf{a}, \mathsf{g}(\mathsf{c})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{g}(\mathsf{b}))
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & \mathsf{f}(\underline{\mathsf{g}(\mathsf{b})}, \overline{\mathsf{g}(\mathsf{b})}) \arrow[dl, "1"'] \arrow[dr, "2"] & \\
\mathsf{f}(\mathsf{c}, \mathsf{g}(\mathsf{b})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{c})
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \overline{\mathsf{f}(\mathsf{a}, \mathsf{g}(\underline{\mathsf{g}(\mathsf{b})}))} \arrow[dl, "2\,1"'] \arrow[dr, "\epsilon"] & \\
\mathsf{f}(\mathsf{a}, \mathsf{g}(\mathsf{c})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{g}(\mathsf{b}))
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \overline{\mathsf{f}(\mathsf{a}, \underline{\mathsf{g}(\mathsf{b})})} \arrow[dl, "2"'] \arrow[dr, "\epsilon"] & \\
\mathsf{f}(\mathsf{a}, \mathsf{c}) & & \mathsf{f}(\mathsf{b}, \mathsf{b})
\end{tikzcd}$$

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

$$\begin{tikzcd}
& \mathsf{f}(\underline{\mathsf{g}(\mathsf{b})}, \overline{\mathsf{g}(\mathsf{b})}) \arrow[dl, "1"'] \arrow[dr, "2"] & \\
\mathsf{f}(\mathsf{c}, \mathsf{g}(\mathsf{b})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{c})
\end{tikzcd}
\quad
\begin{tikzcd}
& \overline{\mathsf{f}(\mathsf{a}, \mathsf{g}(\underline{\mathsf{g}(\mathsf{b})}))} \arrow[dl, "2\,1"'] \arrow[dr, "\epsilon"] & \\
\mathsf{f}(\mathsf{a}, \mathsf{g}(\mathsf{c})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{g}(\mathsf{b}))
\end{tikzcd}
\quad
\begin{tikzcd}
& \overline{\mathsf{f}(\mathsf{a}, \underline{\mathsf{g}(\mathsf{b})})} \arrow[dl, "2"'] \arrow[dr, "\epsilon"] & \\
\mathsf{f}(\mathsf{a}, \mathsf{c}) & & \mathsf{f}(\mathsf{b}, \mathsf{b})
\end{tikzcd}$$

parallel redexes

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

$$\begin{tikzcd}
& \mathsf{f}(\underline{\mathsf{g}(\mathsf{b})}, \overline{\mathsf{g}(\mathsf{b})}) \arrow[dl, "1"'] \arrow[dr, "2"] & \\
\mathsf{f}(\mathsf{c}, \mathsf{g}(\mathsf{b})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{c})
\end{tikzcd}$$

parallel redexes

$$\begin{tikzcd}
& \overline{\mathsf{f}(\mathsf{a}, \mathsf{g}(\underline{\mathsf{g}(\mathsf{b})}))} \arrow[dl, "2\,1"'] \arrow[dr, "\epsilon"] & \\
\mathsf{f}(\mathsf{a}, \mathsf{g}(\mathsf{c})) & & \mathsf{f}(\mathsf{g}(\mathsf{b}), \mathsf{g}(\mathsf{b}))
\end{tikzcd}$$

variable overlap

$$\begin{tikzcd}
& \overline{\mathsf{f}(\mathsf{a}, \underline{\mathsf{g}(\mathsf{b})})} \arrow[dl, "2"'] \arrow[dr, "\epsilon"] & \\
\mathsf{f}(\mathsf{a}, \mathsf{c}) & & \mathsf{f}(\mathsf{b}, \mathsf{b})
\end{tikzcd}$$

Example

rewrite rules

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

three local peaks

$$\begin{tikzcd}
& f(\underline{g(b)}, \overline{g(b)}) \arrow[dl, "1"'] \arrow[dr, "2"] & \\
f(c, g(b)) & & f(g(b), c)
\end{tikzcd}$$

parallel redexes

$$\begin{tikzcd}
& \overline{f(a, g(\underline{g(b)}))} \arrow[dl, "2\,1"'] \arrow[dr, "\epsilon"] & \\
f(a, g(c)) & & f(g(b), g(b))
\end{tikzcd}$$

variable overlap

$$\begin{tikzcd}
& \overline{f(a, \underline{g(b)})} \arrow[dl, "2"'] \arrow[dr, "\epsilon"] & \\
f(a, c) & & f(b, b)
\end{tikzcd}$$

overlapping redexes

Example

rewrite rules

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

three local peaks

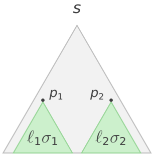
$$\begin{tikzcd} & f(\underline{g(b)}, \overline{g(b)}) \arrow[dl, "1"'] \arrow[dr, "2"] & \\ f(c, g(b)) & & f(g(b), c) \end{tikzcd}$$

$$\begin{tikzcd} & \overline{f(a, g(\underline{g(b)}))} \arrow[dl, "2\,1"'] \arrow[dr, "\epsilon"] & \\ f(a, g(c)) & & f(g(b), g(b)) \end{tikzcd}$$

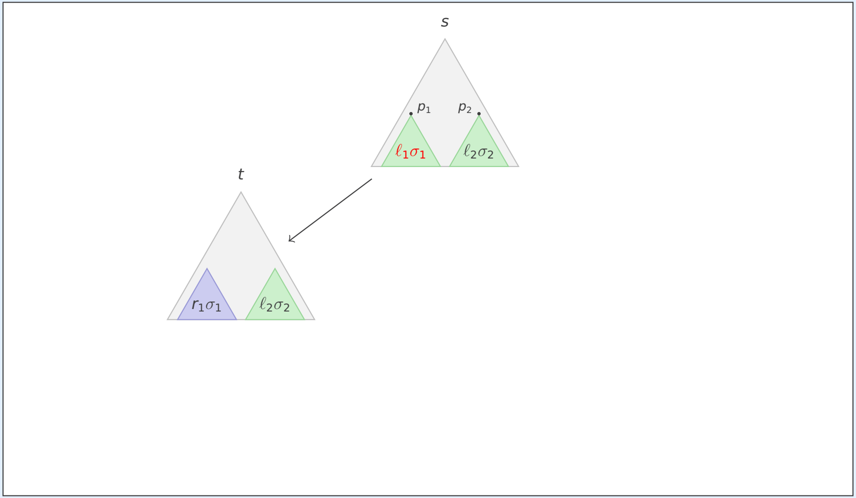
$$\begin{tikzcd} & \overline{f(a, \underline{g(b)})} \arrow[dl, "2"'] \arrow[dr, "\epsilon"] & \\ f(a, c) & & f(b, b) \end{tikzcd}$$

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

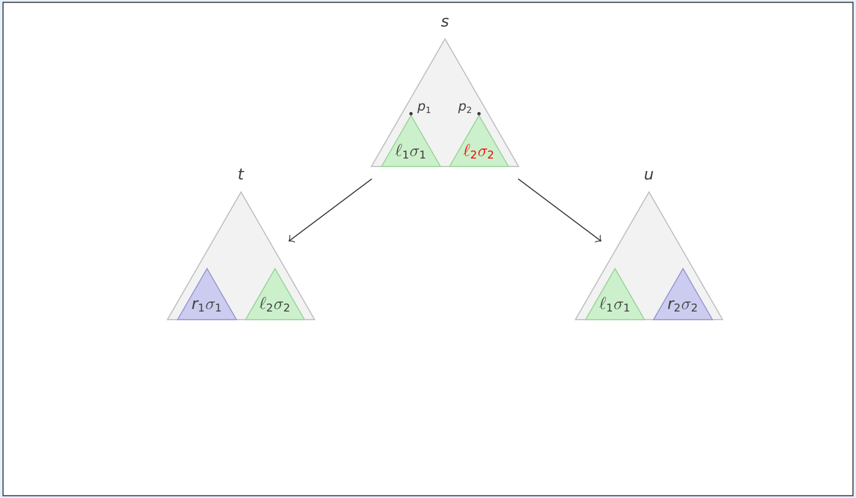
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 1: parallel redexes



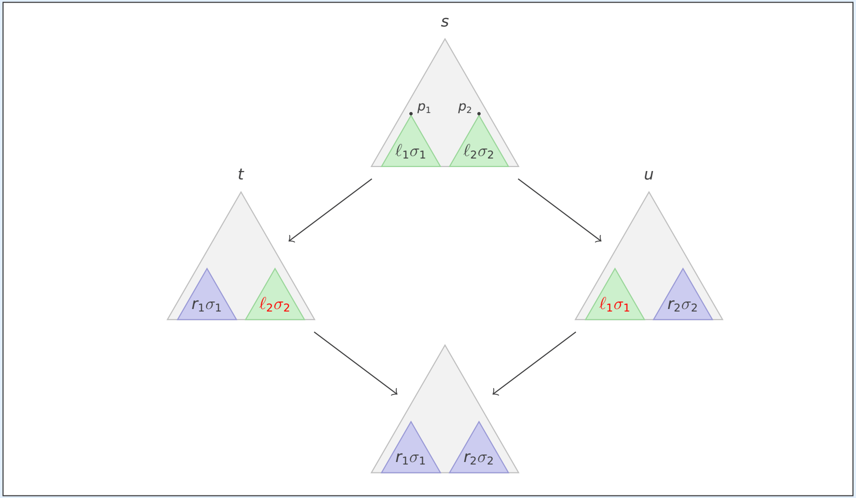
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 1: parallel redexes



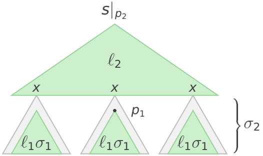
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 1: parallel redexes



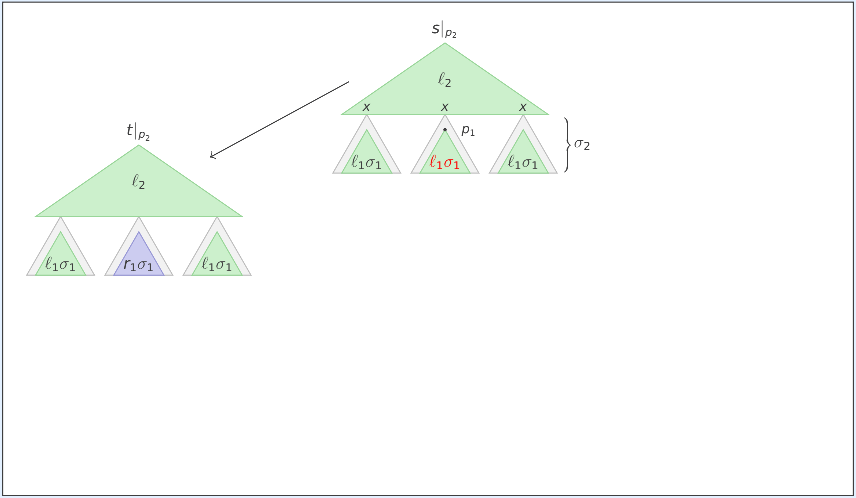
local peak $t \xleftarrow[p_1 \,|\, \ell_1 \to r_1 \,|\, \sigma_1]{} s \xrightarrow[p_2 \,|\, \ell_2 \to r_2 \,|\, \sigma_2]{} u$ case 1: parallel redexes



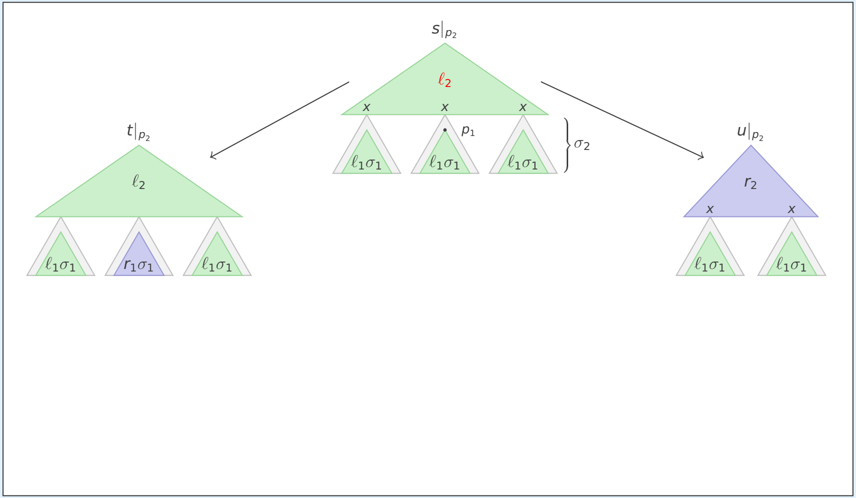
local peak $t \xleftarrow[p_1\,|\,\ell_1 \to r_1\,|\,\sigma_1]{} s \xrightarrow[p_2\,|\,\ell_2 \to r_2\,|\,\sigma_2]{} u$ case 2: variable overlap



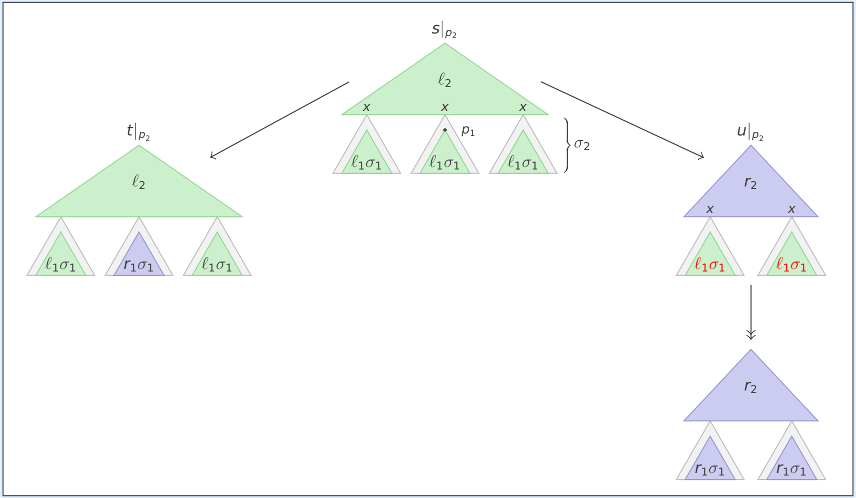
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 2: variable overlap



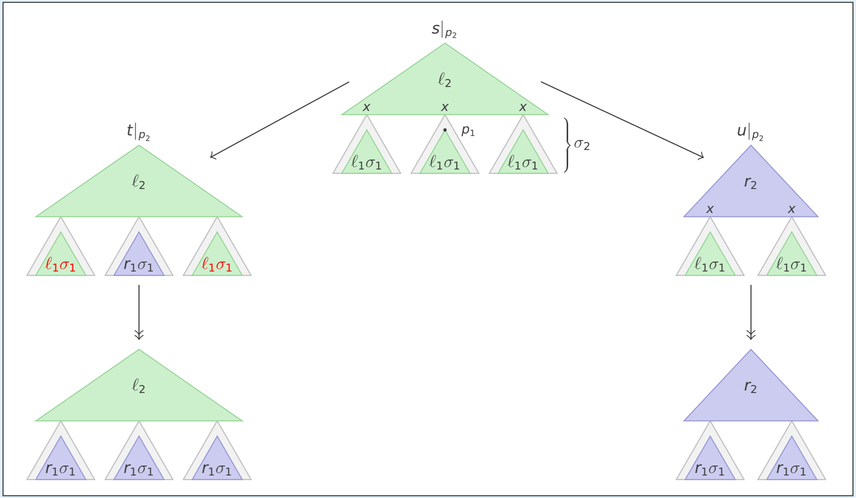
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 2: variable overlap



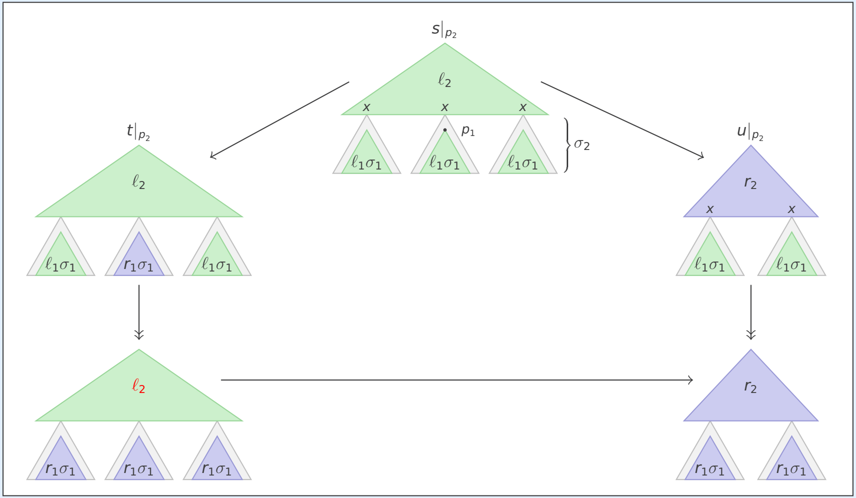
local peak $t \xleftarrow[p_1 \,|\, \ell_1 \to r_1 \,|\, \sigma_1]{} s \xrightarrow[p_2 \,|\, \ell_2 \to r_2 \,|\, \sigma_2]{} u$ case 2: variable overlap



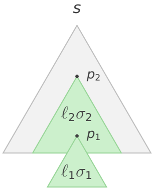
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 2 : variable overlap



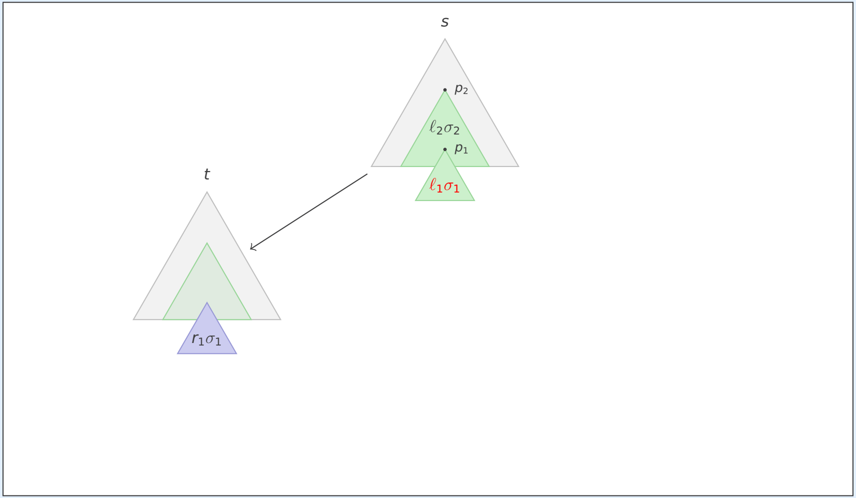
local peak $t \xleftarrow[p_1 \mid \ell_1 \to r_1 \mid \sigma_1]{} s \xrightarrow[p_2 \mid \ell_2 \to r_2 \mid \sigma_2]{} u$ case 2: variable overlap



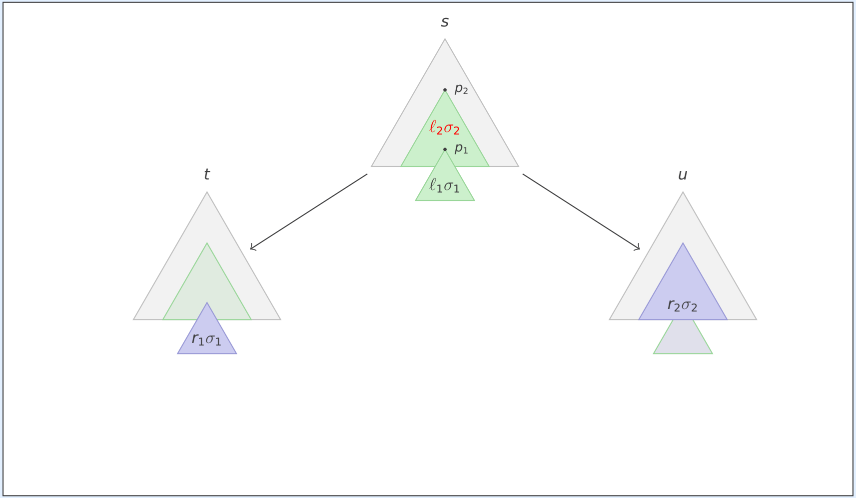
local peak $t \xleftarrow{p_1 \mid \ell_1 \to r_1 \mid \sigma_1} s \xrightarrow{p_2 \mid \ell_2 \to r_2 \mid \sigma_2} u$ case 3: overlapping redexes



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



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 $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$

  ③ ℓ_1 and $\ell_2|_p$ are unifiable

  ④ if $p = \epsilon$ then $\ell_1 \to r_1$ and $\ell_2 \to r_2$ are not variants

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 $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$
  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

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 $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$
  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
- $\ell_2\sigma[r_1\sigma]_p \leftarrow \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma \to r_2\sigma$

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 $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$

  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

- $\ell_2\sigma[r_1\sigma]_p \leftarrow \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma \to r_2\sigma$ critical peak

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 $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$

  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

- $\ell_2\sigma[r_1\sigma]_p \leftarrow \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma \to r_2\sigma$ critical peak

- $\ell_2\sigma[r_1\sigma]_p \approx r_2\sigma$ critical pair

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 $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$
  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
- $\ell_2\sigma[r_1\sigma]_p \leftarrow \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma \to r_2\sigma$ critical peak
- $\ell_2\sigma[r_1\sigma]_p \approx r_2\sigma$ critical pair
- critical pair $s \approx t$ is joinable if $s \downarrow t$

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 $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(\ell_2)$

  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

- $\ell_2\sigma[r_1\sigma]_p \leftarrow \ell_2\sigma[\ell_1\sigma]_p = \ell_2\sigma \to r_2\sigma$ 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

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

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 $\langle \mathsf{e} \cdot u \to u, 1, (x \cdot y) \cdot z \to x \cdot (y \cdot z) \rangle$

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

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 $\langle (u\cdot v)\cdot w \to u\cdot(v\cdot w),\ 1,\ (x\cdot y)\cdot z \to x\cdot(y\cdot z)\rangle$

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. $(u \cdot (v \cdot w)) \cdot z \xleftarrow{1} ((u \cdot v) \cdot w) \cdot z \to (u \cdot v) \cdot (w \cdot z)$

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

❶ $\langle \mathsf{e} \cdot u \to u, 1, (x \cdot y) \cdot z \to x \cdot (y \cdot z) \rangle$

❷ $\langle u^{-} \cdot u \to \mathsf{e}, 1, (x \cdot y) \cdot z \to x \cdot (y \cdot z) \rangle$

❸ $\langle (u \cdot v) \cdot w \to u \cdot (v \cdot w), 1, (x \cdot y) \cdot z \to x \cdot (y \cdot z) \rangle$

critical peaks

❶ $u \cdot z \xleftarrow{1} (\mathsf{e} \cdot u) \cdot z \to \mathsf{e} \cdot (u \cdot z)$

❷ $\mathsf{e} \cdot z \xleftarrow{1} (u^{-} \cdot u) \cdot z \to u^{-} \cdot (u \cdot z)$

❸ $(u \cdot (v \cdot w)) \cdot z \xleftarrow{1} ((u \cdot v) \cdot w) \cdot z \to (u \cdot v) \cdot (w \cdot z)$

Theorem (Knuth & Bendix 1970)

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

Outline

1. Summary of Lecture 5
2. Lexicographic Path Order
3. Unification
4. Critical Pairs
5. **Exercises**
6. Further Reading

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

1. **Summary of Lecture 5**
2. **Lexicographic Path Order**
3. **Unification**
4. **Critical Pairs**
5. **Exercises**
6. **Further Reading**

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)

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