Automated Reasoning

Georg Moser

Institute of Computer Science @ UIBK

Winter 2013

Happy New Year!

Summary Last Lecture

Definition

- a literal L is maximal if $\exists$ ground σ such that for no other literal M: $M\sigma \succ_{\mathsf{L}} L\sigma$
- L is strictly maximal if $\exists$ ground σ such that for no other literal M: $M\sigma \succcurlyeq_{\mathsf{L}} L\sigma$; here $\succcurlyeq_{\mathsf{L}}$ denotes the reflexive closure

Definition

ordered resolution

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma}$$

ordered factoring

$$\frac{C \vee A \vee B}{(C \vee A)\sigma}$$

1. σ is a mgu of the atomic formulas A and B
2. $A\sigma$ is strictly maximal with respect to $C\sigma$; $\neg B\sigma$ is maximal with respect to $D\sigma$

Definition

subsumption and resolution can be combined in the following ways

1. forward subsumption
   newly derived clauses subsumed by existing clauses are deleted
2. backward subsumption
   existing clauses C subsumed by newly derived clauses D become inactive
   inactive clauses are reactivated, if D is no ancestor of current clause
3. replacement
   the set of all clauses (derived and intital) are frequently reduced under subsumption

Theorem

(ordered) resolution is complete under forward subsumption and tautology elimination

Outline of the Lecture

Early Approaches in Automated Reasoning

short recollection of Herbrand's theorem, Gilmore's prover, method of Davis and Putnam

Starting Points

resolution, tableau provers, Skolemisation, ordered resolution, redundancy and deletion

Automated Reasoning with Equality

paramodulation, ordered completion and proof orders, superposition

Applications of Automated Reasoning

Neuman-Stubblebinde Key Exchange Protocol, group theory, resolution and paramodulation as decision procedure, ...

Outline of the Lecture

Early Approaches in Automated Reasoning

short recollection of Herbrand's theorem, Gilmore's prover, method of Davis and Putnam

Starting Points

resolution, tableau provers, Skolemisation, ordered resolution, redundancy and deletion

Automated Reasoning with Equality

paramodulation, ordered completion and proof orders, superposition

Applications of Automated Reasoning

Neuman-Stubblebinde Key Exchange Protocol, group theory, resolution and paramodulation as decision procedure, ...

Paramodulation Calculus

Definition

- let $\Box$ be a fresh constant; let $\mathcal{L}$ be our basic language
- terms of $\mathcal{L} \cup \{\Box\}$ such that $\Box$ occurs exactly once, are called contexts
- empty context is denoted as $\Box$
- for context $C[\Box]$ and a term t
  we write $C[t]$ for the replacement of $\Box$ by t

Paramodulation Calculus

Definition

- let $\Box$ be a fresh constant; let $\mathcal{L}$ be our basic language
- terms of $\mathcal{L} \cup \{\Box\}$ such that $\Box$ occurs exactly once, are called contexts
- empty context is denoted as $\Box$
- for context $C[\Box]$ and a term t
  we write $C[t]$ for the replacement of $\Box$ by t

Example

- let $\mathcal{L} = \{\mathsf{c}, \mathsf{f}, \mathsf{P}\}$
- $\mathsf{P}(\mathsf{f}(\Box)) =: C[\Box]$ is a context
- $C[\mathsf{f}(\mathsf{c})] = \mathsf{P}(\mathsf{f}(\mathsf{f}(\mathsf{c})))$

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad\qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

- σ_1 is a mgu of A and B (A, B atomic)

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

- σ_1 is a mgu of A and B (A, B atomic)
- σ_2 is a mgu of s and s'

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s \neq s'}{C\sigma_2} \qquad \frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

- σ_1 is a mgu of A and B (A, B atomic)
- σ_2 is a mgu of s and s'

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad\qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s \neq s'}{C\sigma_2} \qquad\qquad \frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

- σ_1 is a mgu of A and B (A, B atomic)
- σ_2 is a mgu of s and s'

Example

consider $\mathcal{C} = \{\mathsf{c} \neq \mathsf{d}, \mathsf{b} = \mathsf{d}, \mathsf{a} \neq \mathsf{d} \vee \mathsf{a} = \mathsf{c}, \mathsf{a} = \mathsf{b} \vee \mathsf{a} = \mathsf{d}\}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathsf{b} = \mathsf{d} \quad \mathsf{a} = \mathsf{b} \vee \mathsf{a} = \mathsf{d}}{\mathsf{a} = \mathsf{d} \vee \mathsf{a} = \mathsf{d}}}{\mathsf{a} = \mathsf{d}} \qquad \mathsf{c} \neq \mathsf{d}}{\mathsf{a} \neq \mathsf{c}} \qquad \dfrac{\dfrac{\mathsf{a} = \mathsf{d} \quad \mathsf{a} \neq \mathsf{d} \vee \mathsf{a} = \mathsf{c}}{\mathsf{d} \neq \mathsf{d} \vee \mathsf{a} = \mathsf{c}}}{\mathsf{a} = \mathsf{c}}}{\square}$$

Definition

- define the paramodulation operator $\mathrm{Res}_{\mathsf{P}}(\mathcal{C})$ as follows:

$$\mathrm{Res}_{\mathsf{P}}(\mathcal{C}) = \{D \mid D \text{ is paramodulant, etc. with premises in } \mathcal{C}\}$$

Definition

- define the paramodulation operator $\mathrm{Res}_{\mathrm{P}}(\mathcal{C})$ as follows:

$$\mathrm{Res}_{\mathrm{P}}(\mathcal{C}) = \{D \mid D \text{ is paramodulant, etc. with premises in } \mathcal{C}\}$$

- n^{th} (unrestricted) iteration $\mathrm{Res}_{\mathrm{P}}^{n}$ ($\mathrm{Res}_{\mathrm{P}}^{*}$) of the operator $\mathrm{Res}_{\mathrm{P}}$ is defined as before

Definition

- define the paramodulation operator $\mathrm{Res}_{\mathsf{P}}(\mathcal{C})$ as follows:

$$\mathrm{Res}_{\mathsf{P}}(\mathcal{C}) = \{D \mid D \text{ is paramodulant, etc. with premises in } \mathcal{C}\}$$

- n^{th} (unrestricted) iteration $\mathrm{Res}^n_{\mathsf{P}}$ ($\mathrm{Res}^*_{\mathsf{P}}$) of the operator $\mathrm{Res}_{\mathsf{P}}$ is defined as before

Theorem

paramodulation is sound and complete: if F is a sentence and $\mathcal{C}$ its clause form, then F is unsatisfiable iff $\square \in \mathrm{Res}^*_{\mathsf{P}}(\mathcal{C})$

Definition

- define the paramodulation operator $\mathrm{Res}_{\mathsf{P}}(\mathcal{C})$ as follows:

$$\mathrm{Res}_{\mathsf{P}}(\mathcal{C}) = \{D \mid D \text{ is paramodulant, etc. with premises in } \mathcal{C}\}$$

- n^{th} (unrestricted) iteration $\mathrm{Res}_{\mathsf{P}}^{n}$ ($\mathrm{Res}_{\mathsf{P}}^{*}$) of the operator $\mathrm{Res}_{\mathsf{P}}$ is defined as before

Theorem

paramodulation is sound and complete: if F is a sentence and $\mathcal{C}$ its clause form, then F is unsatisfiable iff $\square \in \mathrm{Res}_{\mathsf{P}}^{*}(\mathcal{C})$

Proof Plan.

lemmas

model existence

completeness of paramodulation

Definition

- define the paramodulation operator $\mathrm{Res}_{\mathrm{P}}(\mathcal{C})$ as follows:

$$\mathrm{Res}_{\mathrm{P}}(\mathcal{C}) = \{D \mid D \text{ is paramodulant, etc. with premises in } \mathcal{C}\}$$

- n^{th} (unrestricted) iteration $\mathrm{Res}_{\mathrm{P}}^{n}$ ($\mathrm{Res}_{\mathrm{P}}^{*}$) of the operator $\mathrm{Res}_{\mathrm{P}}$ is defined as before

Theorem

paramodulation is sound and complete: if F is a sentence and $\mathcal{C}$ its clause form, then F is unsatisfiable iff $\square \in \mathrm{Res}_{\mathrm{P}}^{*}(\mathcal{C})$

Proof Pl

$\mathcal{C}$ set of consistent ground clauses
$\Rightarrow$ $\mathcal{C}$ admits satisfaction properties
$+$ lifting lemmas

lemmas

model existence $\rightarrow$ completeness of paramodulation

A Problem with Lifting

Claim

- let τ_1 and τ_2 be a ground and consider
$$\frac{C\tau_1 \vee (s = t)\tau_1 \quad D\tau_2 \vee L\tau_2[s'\tau_2]}{C\tau_1 \vee D\tau_2 \vee L\tau_2[t\tau_2]}$$
where $s\tau_1 = s'\tau_2$
- $\exists$ mgu σ of s and s', such that σ is more general then τ_1 and τ_2 and the following paramodulation step is valid
$$\frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma}$$

A Problem with Lifting

Claim

- let τ_1 and τ_2 be a ground and consider
$$\frac{C\tau_1 \vee (s = t)\tau_1 \quad D\tau_2 \vee L\tau_2[s'\tau_2]}{C\tau_1 \vee D\tau_2 \vee L\tau_2[t\tau_2]}$$
where $s\tau_1 = s'\tau_2$
- $\exists$ mgu σ of s and s', such that σ is more general then τ_1 and τ_2 and the following paramodulation step is valid
$$\frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma}$$

Fact

observe that paramodulation into variables is allowed

Example

- consider the following unit clauses

$$\mathsf{a} = \mathsf{b} \qquad \mathsf{f}(x) = \mathsf{c}$$

  the only possible (non-ground) paramodulation inference is $\mathsf{f}(\mathsf{b}) = \mathsf{c}$

Example

- consider the following unit clauses

$$\mathsf{a} = \mathsf{b} \qquad \mathsf{f}(x) = \mathsf{c}$$

  the only possible (non-ground) paramodulation inference is $\mathsf{f}(\mathsf{b}) = \mathsf{c}$

- consider the following ground step:

$$\frac{\mathsf{a} = \mathsf{b} \quad \mathsf{f}(\mathsf{f}(\mathsf{a})) = \mathsf{c}}{\mathsf{f}(\mathsf{f}(\mathsf{b})) = \mathsf{c}}$$

  then no lifting is possible: oops ☹...

Example

- consider the following unit clauses

$$\mathsf{a} = \mathsf{b} \qquad \mathsf{f}(x) = \mathsf{c}$$

  the only possible (non-ground) paramodulation inference is $\mathsf{f}(\mathsf{b}) = \mathsf{c}$

- consider the following ground step:

$$\frac{\mathsf{a} = \mathsf{b} \quad \mathsf{f}(\mathsf{f}(\mathsf{a})) = \mathsf{c}}{\mathsf{f}(\mathsf{f}(\mathsf{b})) = \mathsf{c}}$$

  then no lifting is possible: oops ☹. . .

- we add the functional reflexivity equation $\mathsf{f}(x) = \mathsf{f}(x)$ from which we get $\mathsf{f}(\mathsf{a}) = \mathsf{f}(\mathsf{b})$ by paramodulation into a variable

Example

- consider the following unit clauses

$$\mathsf{a} = \mathsf{b} \qquad \mathsf{f}(x) = \mathsf{c}$$

  the only possible (non-ground) paramodulation inference is $\mathsf{f}(\mathsf{b}) = \mathsf{c}$

- consider the following ground step:

$$\frac{\mathsf{a} = \mathsf{b} \quad \mathsf{f}(\mathsf{f}(\mathsf{a})) = \mathsf{c}}{\mathsf{f}(\mathsf{f}(\mathsf{b})) = \mathsf{c}}$$

  then no lifting is possible: oops ☹...

- we add the functional reflexivity equation $\mathsf{f}(x) = \mathsf{f}(x)$ from which we get $\mathsf{f}(\mathsf{a}) = \mathsf{f}(\mathsf{b})$ by paramodulation into a variable

- then lifting becomes possible (using two steps)

$$\frac{\dfrac{\mathsf{a} = \mathsf{b} \quad \mathsf{f}(x) = \mathsf{f}(x)}{\mathsf{f}(\mathsf{a}) = \mathsf{f}(\mathsf{b})} \qquad \mathsf{f}(x) = \mathsf{c}}{\mathsf{f}(\mathsf{f}(\mathsf{b})) = \mathsf{c}}$$

Definition

$f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ is called functional reflexivity equation

Definition

$f(x_1, \dots, x_n) = f(x_1, \dots, x_n)$ is called functional reflexivity equation

Lemma

- *let* τ_1 *and* τ_2 *be a ground and consider*

$$\frac{C\tau_1 \vee (s = t)\tau_1 \quad D\tau_2 \vee L\tau_2[x\tau_2]}{C\tau_1 \vee D\tau_2 \vee L\tau_2[f(t\tau_1)]}$$

  where $x\tau_2 = f(s'\tau_3)$ *and* $s\tau_1 = s'\tau_3$

- *then the following paramodulation step is valid, trivially more general than the ground step*

$$\frac{\dfrac{C \vee s = t \quad f(x) = f(x)}{C \vee f(s) = f(t)} \qquad D \vee L[x]}{C \vee D \vee L[f(t)]}$$

Definition

$f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ is called functional reflexivity equation

Lemma

- *let τ_1 and τ_2 be a ground and consider*

$$\frac{C\tau_1 \vee (s = t)\tau_1 \quad D\tau_2 \vee L\tau_2[x\tau_2]}{C\tau_1 \vee D\tau_2 \vee L\tau_2[f(t\tau_1)]}$$

  where $x\tau_2 = f(s'\tau_3)$ and $s\tau_1 = s'\tau_3$

- *then the following paramodulation step is valid, trivially more general than the ground step*

$$\frac{\dfrac{C \vee s = t \quad f(x) = f(x)}{C \vee f(s) = f(t)} \qquad D \vee L[x]}{C \vee D \vee L[f(t)]}$$

Proof.

on the whiteboard

Definition

$f(x_1, \dots, x_n) = f(x_1, \dots, x_n)$ is called functional reflexivity equation

Lemma

- *let τ_1 and τ_2 be a ground and consider*

$$\frac{C\tau_1 \vee (s = t)\tau_1 \quad D\tau_2 \vee L\tau_2[x\tau_2]}{C\tau_1 \vee D\tau_2 \vee L\tau_2[f(t\tau_1)]}$$

  where $x\tau_2 = f(s'\tau_3)$ and $s\tau_1 = s'\tau_3$

- *then the following paramodulation step is valid, trivially more general than the ground step*

$$\frac{\dfrac{C \vee s = t \quad f(x) = f(x)}{C \vee f(s) = f(t)} \qquad D \vee L[x]}{C \vee D \vee L[f(t)]}$$

Proof.

on the whiteboard ∎

Theorem

paramodulation is sound and complete: if F is a sentence and $\mathcal{C}$ its clause form (containing all functional reflexive equations), then F is unsatisfiable iff $\square \in \mathsf{Res}^*_{\mathsf{P}}(\mathcal{C})$

Proof.

in proof, we follow the standard procedure of combining model existence + (updated) lifting lemma ∎

Theorem

paramodulation is sound and complete: if F is a sentence and $\mathcal{C}$ its clause form (containing all functional reflexive equations), then F is unsatisfiable iff $\square \in \mathrm{Res}^*_{\mathrm{P}}(\mathcal{C})$

Proof.

in proof, we follow the standard procedure of combining model existence + (updated) lifting lemma ∎

Discussion

- alternative completenesss proof employs an adaption of the semantic tree argument
- paramodulation is inefficient
- one idea to reduce the search space is to combine ordered resolution with paramodulation: ordered paramodulation

Ordered Paramodulation Calculus

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s \neq s'}{C\sigma_2} \qquad \frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

Ordered Paramodulation Calculus

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s \neq s'}{C\sigma_2} \qquad \frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

- same conditions on σ_1, σ_2 as before

Ordered Paramodulation Calculus

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s \neq s'}{C\sigma_2} \qquad \frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

- same conditions on σ_1, σ_2 as before
- $A\sigma_1$ is strictly maximal with respect to $C\sigma_1$; $\neg B\sigma_1$ is maximal with respect to $D\sigma_1$

Ordered Paramodulation Calculus

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s \neq s'}{C\sigma_2} \qquad \frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

- same conditions on σ_1, σ_2 as before
- $A\sigma_1$ is strictly maximal with respect to $C\sigma_1$; $\neg B\sigma_1$ is maximal with respect to $D\sigma_1$
- the equation $(s = t)\sigma_2$ and the literal $L[s']\sigma_2$ are maximal with respect to $D\sigma_2$

Ordered Paramodulation Calculus

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma_1} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma_1}$$

$$\frac{C \vee s \neq s'}{C\sigma_2} \qquad \frac{C \vee s = t \quad D \vee L[s']}{(C \vee D \vee L[t])\sigma_2}$$

- same conditions on σ_1, σ_2 as before
- $A\sigma_1$ is strictly maximal with respect to $C\sigma_1$; $\neg B\sigma_1$ is maximal with respect to $D\sigma_1$
- the equation $(s = t)\sigma_2$ and the literal $L[s']\sigma_2$ are maximal with respect to $D\sigma_2$

Theorem

ordered paramodulation is sound and complete

Example

re-consider $\mathcal{C}$

$$\mathsf{c} \neq \mathsf{d} \quad \mathsf{b} = \mathsf{d} \quad \mathsf{a} \neq \mathsf{d} \vee \mathsf{a} = \mathsf{c} \quad \mathsf{a} = \mathsf{b} \vee \mathsf{a} = \mathsf{d}$$

together with the literal order:

$$\mathsf{a} \neq \mathsf{b} \succ \mathsf{a} = \mathsf{b} \succ \mathsf{a} \neq \mathsf{c} \succ \mathsf{a} = \mathsf{c} \succ \mathsf{a} \neq \mathsf{d} \succ \mathsf{a} = \mathsf{d}$$
$$\succ \mathsf{b} \neq \mathsf{d} \succ \mathsf{b} = \mathsf{d} \succ \mathsf{c} \neq \mathsf{d} \succ \mathsf{c} = \mathsf{d}$$

Example

re-consider $\mathcal{C}$

$$c \neq d \quad b = d \quad a \neq d \lor a = c \quad a = b \lor a = d$$

together with the literal order:

$$a \neq b \succ a = b \succ a \neq c \succ a = c \succ a \neq d \succ a = d$$
$$\succ b \neq d \succ b = d \succ c \neq d \succ c = d$$

the following derivation is no longer admissible

$$\dfrac{\dfrac{\dfrac{\dfrac{b = d \quad a = b \lor a = d}{a = d \lor a = d}}{a = d} \qquad c \neq d}{a \neq c} \qquad \dfrac{\dfrac{\begin{array}{c}\Pi \\ a = d\end{array} \quad a \neq d \lor a = c}{d \neq d \lor a = c}}{a = c}}{\square}$$

Example

re-consider $\mathcal{C}$

$$c \neq d \quad b = d \quad a \neq d \vee a = c \quad a = b \vee a = d$$

together with the literal order:

$$a \neq b \succ a = b \succ a \neq c \succ a = c \succ a \neq d \succ a = d$$
$$\succ b \neq d \succ b = d \succ c \neq d \succ c = d$$

the following derivation is no longer admissible

$$\dfrac{\dfrac{\dfrac{\dfrac{b = d \quad a = b \vee a = d}{a = d \vee a = d}}{a = d} \quad c \neq d}{a \neq c} \quad \dfrac{\dfrac{\overset{\Pi}{a = d} \quad a \neq d \vee a = c}{d \neq d \vee a = c}}{a = c}}{\square}$$

Example (cont'd)

$$\mathsf{a} \neq \mathsf{b} \succ \mathsf{a} = \mathsf{b} \succ \mathsf{a} \neq \mathsf{c} \succ \mathsf{a} = \mathsf{c} \succ \mathsf{a} \neq \mathsf{d} \succ \mathsf{a} = \mathsf{d}$$
$$\succ \mathsf{b} \neq \mathsf{d} \succ \mathsf{b} = \mathsf{d} \succ \mathsf{c} \neq \mathsf{d} \succ \mathsf{c} = \mathsf{d}$$

the following derivation is admissible

$$\dfrac{\mathsf{c} \neq \mathsf{d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\mathsf{b} = \mathsf{d} \quad \mathsf{a} = \mathsf{b} \vee \mathsf{a} = \mathsf{d}}{\mathsf{a} = \mathsf{d} \vee \mathsf{a} = \mathsf{d}}}{\mathsf{a} = \mathsf{d}} \qquad \dfrac{\begin{array}{c}\Pi \\ \mathsf{a} = \mathsf{d}\end{array} \quad \mathsf{a} \neq \mathsf{d} \vee \mathsf{a} = \mathsf{c}}{\mathsf{a} \neq \mathsf{d} \vee \mathsf{c} = \mathsf{d}}}{\mathsf{d} \neq \mathsf{d} \vee \mathsf{c} = \mathsf{d}}}{\mathsf{c} = \mathsf{d}}}{\square}$$

Example (cont'd)

$$\mathsf{a} \neq \mathsf{b} \succ \mathsf{a} = \mathsf{b} \succ \mathsf{a} \neq \mathsf{c} \succ \mathsf{a} = \mathsf{c} \succ \mathsf{a} \neq \mathsf{d} \succ \mathsf{a} = \mathsf{d}$$
$$\succ \mathsf{b} \neq \mathsf{d} \succ \mathsf{b} = \mathsf{d} \succ \mathsf{c} \neq \mathsf{d} \succ \mathsf{c} = \mathsf{d}$$

the following derivation is admissible

$$\dfrac{\mathsf{c} \neq \mathsf{d} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\mathsf{b} = \mathsf{d} \quad \mathsf{a} = \mathsf{b} \lor \mathsf{a} = \mathsf{d}}{\mathsf{a} = \mathsf{d} \lor \mathsf{a} = \mathsf{d}}}{\mathsf{a} = \mathsf{d}} \qquad \dfrac{\begin{array}{c}\Pi \\ \mathsf{a} = \mathsf{d}\end{array} \quad \mathsf{a} \neq \mathsf{d} \lor \mathsf{a} = \mathsf{c}}{\mathsf{a} \neq \mathsf{d} \lor \mathsf{c} = \mathsf{d}}}{\mathsf{d} \neq \mathsf{d} \lor \mathsf{c} = \mathsf{d}}}{\mathsf{c} = \mathsf{d}}}{\square}$$

Discussion

- ordered paramodulation is still too ineffienct
- various refinements have been introduced, one is the superposition calculus

Employ Rewriting Techniques

Definitions

- rewrite relation . . .

Employ Rewriting Techniques

Definitions

- rewrite relation . . .
- normal form . . .

Employ Rewriting Techniques

Definitions

- rewrite relation . . .
- normal form . . .
- reduction order . . .

Employ Rewriting Techniques

Definitions

- rewrite relation ...
- normal form ...
- reduction order ...
- lexicographic path order (LPO), reduction order ...

Employ Rewriting Techniques

Definitions

- rewrite relation ...
- normal form ...
- reduction order ...
- lexicographic path order (LPO), reduction order ...
- confluent ...

Employ Rewriting Techniques

Definitions

- rewrite relation ...
- normal form ...
- reduction order ...
- lexicographic path order (LPO), reduction order ...
- confluent ...
- an equation $s = t$ converges (or has a rewrite proof) in $\mathcal{R}$ if s and t are joinable: $s \downarrow t$

Employ Rewriting Techniques

Definitions

- rewrite relation . . .
- normal form . . .
- reduction order . . .
- lexicographic path order (LPO), reduction order . . .
- confluent . . .
- an equation $s = t$ converges (or has a rewrite proof) in $\mathcal{R}$ if s and t are joinable: $s \downarrow t$

Facts

1. a convergent (confluent & terminating) TRS forms a decision procedure for the underlying equational theory: $s \leftrightarrow^* t$ iff $s \downarrow t$

Employ Rewriting Techniques

Definitions

- rewrite relation ...
- normal form ...
- reduction order ...
- lexicographic path order (LPO), reduction order ...
- confluent ...
- an equation $s = t$ converges (or has a rewrite proof) in $\mathcal{R}$ if s and t are joinable: $s \downarrow t$

Facts

1. a convergent (confluent & terminating) TRS forms a decision procedure for the underlying equational theory: $s \leftrightarrow^* t$ iff $s \downarrow t$
2. normalisation in a convergent TRS amounts to a don't care nondeterminism

Completion

Definition (superposition of rewrite rules)

$$\frac{s \to t \quad w[u] \to v}{(w[t] = v)\sigma}$$

σ mgu of s and u and u not a variable; then $(w[t] = v)\sigma$ is a critical pair

Completion

Definition (superposition of rewrite rules)

$$\frac{s \to t \quad w[u] \to v}{(w[t] = v)\sigma}$$

σ mgu of s and u and u not a variable; then $(w[t] = v)\sigma$ is a critical pair

Theorem

a terminating TRS $\mathcal{R}$ is confluent iff all critical pairs between rules in $\mathcal{R}$ converge

Completion

Definition (superposition of rewrite rules)

$$\frac{s \to t \quad w[u] \to v}{(w[t] = v)\sigma}$$

σ mgu of s and u and u not a variable; then $(w[t] = v)\sigma$ is a critical pair

Theorem

a terminating TRS $\mathcal{R}$ is confluent iff all critical pairs between rules in $\mathcal{R}$ converge

Example

LPO is not total; x, y, u, v variables:

$$\mathsf{f}(x, y) \not>_{\mathsf{lpo}} \mathsf{f}(u, w) \qquad \mathsf{f}(u, w) \not>_{\mathsf{lpo}} \mathsf{f}(x, y)$$

Ordered Rewriting

Definitions

- reduction orders that are total on ground terms are called complete
- $\succ$ a reduction order; $\mathcal{E}$ a set of equations; consider

$$\mathcal{E}^{\succ} = \{s\sigma \to t\sigma \mid s = t \in \mathcal{E}, s\sigma \succ t\sigma\}$$

- rules in $\mathcal{E}^{\succ}$ are called reductive instances of equations in $\mathcal{E}$
- rewrite relation $\to_{\mathcal{E}^{\succ}}$ represents ordered rewriting

Ordered Rewriting

Definitions

- reduction orders that are total on ground terms are called complete
- $\succ$ a reduction order; $\mathcal{E}$ a set of equations; consider

$$\mathcal{E}^{\succ} = \{s\sigma \to t\sigma \mid s = t \in \mathcal{E}, s\sigma \succ t\sigma\}$$

- rules in $\mathcal{E}^{\succ}$ are called reductive instances of equations in $\mathcal{E}$
- rewrite relation $\to_{\mathcal{E}^{\succ}}$ represents ordered rewriting

Example

- let $\succ_{\mathsf{lpo}}$ be a LPO induced by the precedence $+ \succ \mathsf{a} \succ \mathsf{b} \succ \mathsf{c}$
- $\mathsf{b} + \mathsf{c} \succ_{\mathsf{lpo}} \mathsf{c} + \mathsf{b} \succ_{\mathsf{lpo}} \mathsf{c}$
- commutativity $x + y = y + x$ yields the ordered rewrite derivation:

$$(\mathsf{b} + \mathsf{c}) + \mathsf{c} \to (\mathsf{c} + \mathsf{b}) + \mathsf{c} \to \mathsf{c} + (\mathsf{c} + \mathsf{b})$$

Definition

equations $\mathcal{E}$ are ground convergent wrt $\succ$ if $\mathcal{E}^{\succ}$ is ground convergent

Definition

equations $\mathcal{E}$ are ground convergent wrt $\succ$ if $\mathcal{E}^{\succ}$ is ground convergent

Definition (superposition with equations)

$$\frac{s = t \quad w[u] = v}{(w[t] = v)\sigma}$$

- σ is mgu of s and u; $t\sigma \not\succeq s\sigma$, $v\sigma \not\succeq w[u]\sigma$ and u is not a variable
- $(w[t] = v)\sigma$ is an ordered critical pair

Definition

equations $\mathcal{E}$ are ground convergent wrt $\succ$ if $\mathcal{E}^{\succ}$ is ground convergent

Definition (superposition with equations)

$$\frac{s = t \quad w[u] = v}{(w[t] = v)\sigma}$$

- σ is mgu of s and u; $t\sigma \not\succeq s\sigma$, $v\sigma \not\succeq w[u]\sigma$ and u is not a variable
- $(w[t] = v)\sigma$ is an ordered critical pair

Theorem

$\succ$ a complete reduction order; a set of equations E is ground convergent wrt $\succ$ iff $\forall$ ordered critical pairs $(w[t] = v)\sigma$ (with overlapping term $w[u]\sigma$) and $\forall$ ground substitutions τ: if $w[u]\sigma\tau \succ w[t]\sigma\tau$ and $w[u]\sigma\tau \succ v\sigma\tau$ then $w[t]\sigma\tau \downarrow v\sigma\tau$

Ordered Completion

deduction $\qquad \mathcal{E}; \mathcal{R} \vdash \mathcal{E} \cup \{s = t\}; \mathcal{R}$

if $s \leftrightarrow_{\mathcal{E} \cup \mathcal{R}} w \leftrightarrow_{\mathcal{E} \cup \mathcal{R}} t$, $s \not\succeq w$, $t \not\succeq w$

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\preceq w$, $t \not\preceq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\succeq w$, $t \not\succeq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$
deletion	$\mathcal{E} \cup \{s = s\};\mathcal{R} \vdash \mathcal{E};\mathcal{R}$	

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\preceq w$, $t \not\preceq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$
deletion	$\mathcal{E} \cup \{s = s\};\mathcal{R} \vdash \mathcal{E};\mathcal{R}$	
simplification	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E} \cup \{u = t\};\mathcal{R}$	if $s \to_{\mathcal{R}} u$

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\succeq w$, $t \not\succeq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$
deletion	$\mathcal{E} \cup \{s = s\};\mathcal{R} \vdash \mathcal{E};\mathcal{R}$	
simplification	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E} \cup \{u = t\};\mathcal{R}$	if $s \to_{\mathcal{R}} u$
composition	$\mathcal{E};\mathcal{R} \cup \{s \to t\} \vdash \mathcal{E};\mathcal{R} \cup \{s \to u\}$	if $r \to_{\mathcal{R}} u$

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\preceq w$, $t \not\preceq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$
deletion	$\mathcal{E} \cup \{s = s\};\mathcal{R} \vdash \mathcal{E};\mathcal{R}$	
simplification	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E} \cup \{u = t\};\mathcal{R}$	if $s \to_{\mathcal{R}} u$
composition	$\mathcal{E};\mathcal{R} \cup \{s \to t\} \vdash \mathcal{E};\mathcal{R} \cup \{s \to u\}$	if $r \to_{\mathcal{R}} u$
collapse	$\mathcal{E};\mathcal{R} \cup \{s[w] \to t\} \vdash \mathcal{E} \cup \{s[u] = t\};\mathcal{R}$	
	if $w \to_{\mathcal{R}} u$ and either $t \succ u$ or $w \neq s[w]$	

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\preceq w$, $t \not\preceq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$
deletion	$\mathcal{E} \cup \{s = s\};\mathcal{R} \vdash \mathcal{E};\mathcal{R}$	
simplification	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E} \cup \{u = t\};\mathcal{R}$	if $s \to_{\mathcal{R}} u$
composition	$\mathcal{E};\mathcal{R} \cup \{s \to t\} \vdash \mathcal{E};\mathcal{R} \cup \{s \to u\}$	if $r \to_{\mathcal{R}} u$
collapse	$\mathcal{E};\mathcal{R} \cup \{s[w] \to t\} \vdash \mathcal{E} \cup \{s[u] = t\};\mathcal{R}$	
	if $w \to_{\mathcal{R}} u$ and either $t \succ u$ or $w \neq s[w]$	

Definition

- a sequence $(\mathcal{E}_0;\mathcal{R}_0) \vdash (\mathcal{E}_1;\mathcal{R}_1) \vdash \cdots$ is called a derivation usually $\mathcal{E}_0$ is the set of initial equations and $\mathcal{R}_0 = \varnothing$

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\succeq w$, $t \not\succeq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$
deletion	$\mathcal{E} \cup \{s = s\};\mathcal{R} \vdash \mathcal{E};\mathcal{R}$	
simplification	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E} \cup \{u = t\};\mathcal{R}$	if $s \to_{\mathcal{R}} u$
composition	$\mathcal{E};\mathcal{R} \cup \{s \to t\} \vdash \mathcal{E};\mathcal{R} \cup \{s \to u\}$	if $r \to_{\mathcal{R}} u$
collapse	$\mathcal{E};\mathcal{R} \cup \{s[w] \to t\} \vdash \mathcal{E} \cup \{s[u] = t\};\mathcal{R}$	
	if $w \to_{\mathcal{R}} u$ and either $t \succ u$ or $w \neq s[w]$	

Definition

- a sequence $(\mathcal{E}_0;\mathcal{R}_0) \vdash (\mathcal{E}_1;\mathcal{R}_1) \vdash \cdots$ is called a derivation usually $\mathcal{E}_0$ is the set of initial equations and $\mathcal{R}_0 = \varnothing$
- its limit is $(\mathcal{E}_\infty;\mathcal{R}_\infty)$; here $\mathcal{E}_\infty = \bigcup_{i\geqslant 0}\bigcap_{j\geqslant i}\mathcal{E}_j$; $\mathcal{R}_\infty = \bigcup_{i\geqslant 0}\bigcap_{j\geqslant i}\mathcal{R}_j$

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\preceq w$, $t \not\preceq w$	
orientation	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E};\mathcal{R} \cup \{s \to t\}$	if $s \succ t$
deletion	$\mathcal{E} \cup \{s = s\};\mathcal{R} \vdash \mathcal{E};\mathcal{R}$	
simplification	$\mathcal{E} \cup \{s = t\};\mathcal{R} \vdash \mathcal{E} \cup \{u = t\};\mathcal{R}$	if $s \to_{\mathcal{R}} u$
composition	$\mathcal{E};\mathcal{R} \cup \{s \to t\} \vdash \mathcal{E};\mathcal{R} \cup \{s \to u\}$	if $r \to_{\mathcal{R}} u$
collapse	$\mathcal{E};\mathcal{R} \cup \{s[w] \to t\} \vdash \mathcal{E} \cup \{s[u] = t\};\mathcal{R}$	
	if $w \to_{\mathcal{R}} u$ and either $t \succ u$ or $w \neq s[w]$	

Definition

- a sequence $(\mathcal{E}_0;\mathcal{R}_0) \vdash (\mathcal{E}_1;\mathcal{R}_1) \vdash \cdots$ is called a derivation usually $\mathcal{E}_0$ is the set of initial equations and $\mathcal{R}_0 = \varnothing$
- its limit is $(\mathcal{E}_\infty;\mathcal{R}_\infty)$; here $\mathcal{E}_\infty = \bigcup_{i\geqslant 0}\bigcap_{j\geqslant i}\mathcal{E}_j$; $\mathcal{R}_\infty = \bigcup_{i\geqslant 0}\bigcap_{j\geqslant i}\mathcal{R}_j$

Definition

- a proof of $s = t$ wrt $\mathcal{E};\mathcal{R}$ is

$$s = s_0\ \rho_0\ s_1\ \rho_1\ s_2 \cdots s_{n-1}\ \rho_{n-1}\ s_n = t \qquad n \geqslant 0$$

1. $(s_i\ \rho_i\ s_{i+1}) = (w[u\sigma] \leftrightarrow w[v\sigma])$ with $u = v \in \mathcal{E}$
2. $(s_i\ \rho_i\ s_{i+1}) = (w[u\sigma] \to w[v\sigma])$ with $u \to v \in \mathcal{E}^{\succ} \cup \mathcal{R}$
3. $(s_i\ \rho_i\ s_{i+1}) = (w[u\sigma] \leftarrow w[v\sigma])$ with $v \to u \in \mathcal{E}^{\succ} \cup \mathcal{R}$

Definition

- a proof of $s = t$ wrt $\mathcal{E};\mathcal{R}$ is

$$s = s_0 \ \rho_0 \ s_1 \ \rho_1 \ s_2 \cdots s_{n-1} \ \rho_{n-1} \ s_n = t \qquad n \geqslant 0$$

  1. $(s_i \ \rho_i \ s_{i+1}) = (w[u\sigma] \leftrightarrow w[v\sigma])$ with $u = v \in \mathcal{E}$
  2. $(s_i \ \rho_i \ s_{i+1}) = (w[u\sigma] \rightarrow w[v\sigma])$ with $u \rightarrow v \in \mathcal{E}^{\succ} \cup \mathcal{R}$
  3. $(s_i \ \rho_i \ s_{i+1}) = (w[u\sigma] \leftarrow w[v\sigma])$ with $v \rightarrow u \in \mathcal{E}^{\succ} \cup \mathcal{R}$

- a proof of form

$$s = s_0 \rightarrow s_1 \rightarrow s_2 \cdots \rightarrow s_m \leftarrow \cdots s_{n-1} \leftarrow s_n = t$$

  is called rewrite proof

Definition

- a proof of $s = t$ wrt $\mathcal{E};\mathcal{R}$ is

$$s = s_0 \ \rho_0 \ s_1 \ \rho_1 \ s_2 \cdots s_{n-1} \ \rho_{n-1} \ s_n = t \qquad n \geqslant 0$$

  1. $(s_i \ \rho_i \ s_{i+1}) = (w[u\sigma] \leftrightarrow w[v\sigma])$ with $u = v \in \mathcal{E}$
  2. $(s_i \ \rho_i \ s_{i+1}) = (w[u\sigma] \rightarrow w[v\sigma])$ with $u \rightarrow v \in \mathcal{E}^{\succ} \cup \mathcal{R}$
  3. $(s_i \ \rho_i \ s_{i+1}) = (w[u\sigma] \leftarrow w[v\sigma])$ with $v \rightarrow u \in \mathcal{E}^{\succ} \cup \mathcal{R}$

- a proof of form

$$s = s_0 \rightarrow s_1 \rightarrow s_2 \cdots \rightarrow s_m \leftarrow \cdots s_{n-1} \leftarrow s_n = t$$

  is called rewrite proof

Fact

1. *$\exists$ rewrite proof iff the equations converge wrt $\mathcal{R} \cup \mathcal{E}^{\succ}$*
2. *whenever $\mathcal{E};\mathcal{R} \vdash \mathcal{E}';\mathcal{R}'$ then the same equations are provable in $\mathcal{E};\mathcal{R}$ as in $\mathcal{E}';\mathcal{R}'$; however proofs may become simpler*