Automated Theorem Proving

Georg Moser

Institute of Computer Science @ UIBK

Winter 2015

Summary Last Lecture

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)
- σ_2 is a mgu of s and s'

Theorem

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

Summary Last Lecture

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'

Theorem

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

Summary Last Lecture

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'

Theorem

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

Outline of the Lecture

Early Approaches in Automated Reasoning

Herbrand's theorem for dummies, Gilmore's prover, method of Davis and Putnam

Starting Points

resolution, tableau provers, Skolemisation, redundancy and deletion

Automated Reasoning with Equality

ordered resolution, paramodulation, ordered completion and proof orders, superposition

Applications of Automated Reasoning

Neuman-Stubblebinde Key Exchange Protocol, Robbins problem

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:

$$\mathsf{a} \neq \mathsf{b} \succ_{\mathsf{L}} \mathsf{a} = \mathsf{b} \succ_{\mathsf{L}} \mathsf{a} \neq \mathsf{c} \succ_{\mathsf{L}} \mathsf{a} = \mathsf{c} \succ_{\mathsf{L}} \mathsf{a} \neq \mathsf{d} \succ_{\mathsf{L}} \mathsf{a} = \mathsf{d}$$
$$\succ_{\mathsf{L}} \mathsf{b} \neq \mathsf{d} \succ_{\mathsf{L}} \mathsf{b} = \mathsf{d} \succ_{\mathsf{L}} \mathsf{c} \neq \mathsf{d} \succ_{\mathsf{L}} \mathsf{c} = \mathsf{d}$$

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:

$$\mathsf{a} \neq \mathsf{b} \succ_{\mathsf{L}} \mathsf{a} = \mathsf{b} \succ_{\mathsf{L}} \mathsf{a} \neq \mathsf{c} \succ_{\mathsf{L}} \mathsf{a} = \mathsf{c} \succ_{\mathsf{L}} \mathsf{a} \neq \mathsf{d} \succ_{\mathsf{L}} \mathsf{a} = \mathsf{d}$$
$$\succ_{\mathsf{L}} \mathsf{b} \neq \mathsf{d} \succ_{\mathsf{L}} \mathsf{b} = \mathsf{d} \succ_{\mathsf{L}} \mathsf{c} \neq \mathsf{d} \succ_{\mathsf{L}} \mathsf{c} = \mathsf{d}$$

the following derivation is no longer admissible

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

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:

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

the following derivation is no longer admissible

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

Example (cont'd)

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

the following derivation is admissible

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

Example (cont'd)

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

the following derivation is admissible

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

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 $s = t$ is joinable (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 $s = t$ is joinable (or has a rewrite proof) in $\mathcal{R}$ if s and t are joinable: $s \downarrow t$

Facts

1. a complete (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 $s = t$ is joinable (or has a rewrite proof) in $\mathcal{R}$ if s and t are joinable: $s \downarrow t$

Facts

1. a complete (confluent & terminating) TRS forms a decision procedure for the underlying equational theory: $s \leftrightarrow^* t$ iff $s \downarrow t$
2. normalisation in a complete 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 $\mathcal{R}$ are joinable

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 $\mathcal{R}$ are joinable

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 complete wrt $\succ$ if $\mathcal{E}^{\succ}$ is complete on ground terms

Definition

equations $\mathcal{E}$ are ground complete wrt $\succ$ if $\mathcal{E}^{\succ}$ is complete on ground terms

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 complete wrt $\succ$ if $\mathcal{E}^{\succ}$ is complete on ground terms

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 complete 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 $w[t]\sigma\tau \downarrow v\sigma\tau$