Automated Theorem Proving

Georg Moser

Institute of Computer Science @ UIBK

Winter 2015

Summary Last Lecture

Definition

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

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

- 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

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

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, 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, Robbins problem

Ordered Completion

deduction	$\mathcal{E};\mathcal{R} \vdash \mathcal{E} \cup \{s = t\};\mathcal{R}$	
	if $s \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} w \leftrightarrow_{\mathcal{E}\cup\mathcal{R}} t$, $s \not\succ w$, $t \not\succ w$	
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 $v \to u \in \mathcal{E}^{\succ} \cup \mathcal{R}$
- a proof of form

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

  is called rewrite proof

Fact

1. *$\exists$ rewrite proof iff the equations are joinable 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*

Definition

s encompasses t if $s = C[t\sigma]$ for some context C and some substitution σ

Definition

cost measure of proof steps

$$\text{cost of } s[u] \ \rho \ s[v] = \begin{cases} (\{s[u]\}, u, \rho, s[v]) & \text{if } s[u] \succ s[v] \\ (\{s[v]\}, v, \rho, s[u]) & \text{if } s[v] \succ s[u] \\ (\{s[u], s[v]\}, \bot, \bot, \bot) & \text{otherwise} \end{cases}$$

cost measure is lexicographically compared as follows:

1. multiset extension of $\succ$
2. encompassment order
3. some order with $\leftrightarrow \, > \, \to$ and $\leftrightarrow \, > \, \leftarrow$
4. reduction order $\succ$

$\bot$ is supposed to be minimal in all orders; let $\succ_\pi$ the multiset extension of the cost measure; then $\succ_\pi$ denotes a well-founded order on proofs

Fact

each completion step decreases the cost of certain proofs

Proof Sketch.

- consider orientation that replaces an equation $s = t$ by rule $s \to t$
- yields proof transformation

$$(u[s\sigma] \leftrightarrow u[t\sigma]) \Rightarrow (u[s\sigma] \to u[t\sigma])$$

- cost of $(u[s\sigma] \leftrightarrow u[t\sigma]) >$ cost of $(u[s\sigma] \to u[t\sigma])$

∎

recall: $\mathcal{E}_\infty = \bigcup_{i\geqslant 0}\bigcap_{j\geqslant i}\mathcal{E}_j$; $\mathcal{R}_\infty = \bigcup_{i\geqslant 0}\bigcap_{j\geqslant i}\mathcal{R}_j$

Definition

a derivation is fair if each ordered critical pair $u = v \in \mathcal{E}_\infty \cup \mathcal{R}_\infty$ is an element of some $\mathcal{E}_i$

Theorem

let $(\mathcal{E}_0; \mathcal{R}_0), (\mathcal{E}_1; \mathcal{R}_1), \dots$ be a fair ordered completion derivation with $\mathcal{R}_0 = \varnothing$; then the following is equivalent:

1. *$s = t$ is a consequence of $\mathcal{E}_0$*
2. *$s = t$ has a rewrite proof in $\mathcal{E}_\infty^{\succ} \cup \mathcal{R}_\infty$*
3. *$\exists$ i such that $s = t$ has a rewrite proof in $\mathcal{E}_i^{\succ} \cup \mathcal{R}_i$*

Definitions

- let $\mathcal{E}$ be a set of equations and $s = t$ an equation (possibly containing variables); then $\mathcal{E} \models s = t$ is the word problem for $\mathcal{E}$
- the word problem becomes a refutation theorem proving problem once we consider the clause form of the negation of the word problem:
  1. a set of positive unit equations in $\mathcal{E}$
  2. a ground disequation obtained by negation and Skolemisation of $s = t$

Completeness of Superposition

Corollary

superposition with equations is sound and complete, that is, if $\mathcal{C}$ is the clause representation of the (negated) word problem $\mathcal{E} \models s = t$, then the saturation of $\mathcal{C}$ wrt to superposition (and equality resolution) contains $\square$ iff $\mathcal{E} \models s = t$

Proof.

1. let $\mathcal{C}'$ denote the saturation and let $\square \in \mathcal{C}'$
2. then $\mathcal{E} \models s = t$ due to soundness of superposition
3. otherwise assume $\square \notin \mathcal{C}'$
4. then $s = t$ does not have a proof in $\mathcal{C}'$
5. with the theorem we conclude that $\mathcal{E} \not\models s = t$

∎