Computational Logic

Automated Theorem Proving

Georg Moser

Institute of Computer Science @ UIBK

Winter 2015

Summary of Last Lectures

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 (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

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 $\Box$ iff $\mathcal{E} \models s = t$

NB: inference rules in ordered completion different from deduction can be conceived as redundancy elimination rules

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

Superposition for Horn Clauses

Idea (from logical programming)

- consider a set P of non-equational Horn clauses (= a logic program)
- define the operator:

$$T_P\colon I \mapsto \{A \mid A \subset B_1, \ldots, B_k \in \mathrm{Gr}(P) \text{ and } \forall\ i\ B_i \in I\}$$

- consider the least fixed point $\bigcup_{n\geqslant 0} T_p^n(\varnothing)$ of T_p
- then $\bigcup_{n\geqslant 0} T_p^n(\varnothing)$ denotes the unique minimal model of P

$A \subset B_1, \ldots, B_k$ produces A, if $\forall\ i\ B_i \in T_p^n(\varnothing)$ but $A \notin T_p^n(\varnothing)$

Definition

an equational Horn clause $C \equiv (u_1 = v_1, \ldots, u_k = v_k \supset s = t)$ is reductive for $s \to t$ (wrt to a reduction order $\succ$) if s is strictly maximal in C: (i) $s \succ t$, (ii) for all i: $s \succ u_i$, and (iii) for all i: $s \succ v_i$

NB: if C is reductive for $s \to t$, we write C as $u_1 = v_1, \ldots, u_k = v_k \supset s \to t$

Definition

- let $\mathcal{R}$ be a set of reductive clauses
- $\mathcal{R}$ induces the rewrite relation $\to_\mathcal{R}$: $s \to_\mathcal{R} t$ if
  1. $\exists$ reductive clause $C \supset l \to r$
  2. $\exists$ substitution σ such that $s = l\sigma$, $t = r\sigma$
  3. $\forall\ u' = v' \in C$: $u'\sigma \downarrow v'\sigma$

Definition (superposition of reductive conditional rewrite rules)

$$\frac{C \supset s \to t \quad D \supset w[u] \to v}{(C, D \supset w[t] \to v)\sigma}$$

σ is mgu of s and u and u is not a variable

Definitions

- $(C, D \supset w[t] \to v)\sigma$ is a conditional critical pair
- $(C, D \supset w[t] \to v)\sigma$ converges if $\forall\ \tau$ such that $C\sigma\tau$ and $D\sigma\tau$ converge: $w[t]\sigma\tau \downarrow v\sigma\tau$

Lemma

a reductive conditional rewrite system is confluent iff all critical pairs converge

Theorem

let $\succ$ be a reduction order and let $\mathcal{C}$ be a set of reductive equational Horn clauses; then the word problem is decidable if all critical pairs converge

Superposition Calculus

Definition

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma}\ \text{ORe} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma}\ \text{OFc}$$

$$\frac{C \vee s = t \quad D \vee \neg A[s']}{(C \vee D \vee \neg A[t])\sigma}\ \text{OPm(L)} \qquad \frac{C \vee s = t \quad D \vee A[s']}{(C \vee D \vee A[t])\sigma}\ \text{OPm(R)}$$

$$\frac{C \vee s = t \quad D \vee u[s'] \neq v}{(C \vee D \vee u[t] \neq v)\sigma}\ \text{SpL} \qquad \frac{C \vee s = t \quad D \vee u[s'] = v}{(C \vee D \vee u[t] = v)\sigma}\ \text{SpR}$$

$$\frac{C \vee s \neq t}{C\sigma}\ \text{ERR} \qquad \frac{C \vee u = v \vee s = t}{(C \vee v \neq t \vee u = t)\sigma}\ \text{EFc}$$

- ORe and OFc are ordered resolution and ordered factoring
- OPm(L), OPm(R), SpL, SpR stands for ordered paramodulation and superpostion (left or right)
- ERR means equality resolution and EFc means equality factoring

Definition (Definition (cont'd))

$$\frac{C \vee A \quad D \vee \neg B}{(C \vee D)\sigma}\ \text{ORe} \qquad \frac{C \vee A \vee B}{(C \vee A)\sigma}\ \text{OFc}$$

$$\frac{C \vee s = t \quad D \vee \neg A[s']}{(C \vee D \vee \neg A[t])\sigma}\ \text{OPm(L)} \qquad \frac{C \vee s = t \quad D \vee A[s']}{(C \vee D \vee A[t])\sigma}\ \text{OPm(R)}$$

$$\frac{C \vee s = t \quad D \vee u[s'] \neq v}{(C \vee D \vee u[t] \neq v)\sigma}\ \text{SpL} \qquad \frac{C \vee s = t \quad D \vee u[s'] = v}{(C \vee D \vee u[t] = v)\sigma}\ \text{SpR}$$

$$\frac{C \vee s \neq t}{C\sigma}\ \text{ERR} \qquad \frac{C \vee u = v \vee s = t}{(C \vee v \neq t \vee u = t)\sigma}\ \text{EFc}$$

constraints:

1. for the superposition rules: σ is a mgu of s and s', s' not a variable, $t\sigma \not\succeq s\sigma$, $v\sigma \not\succeq u[s']\sigma$, $(s = t)\sigma$ is strictly maximal wrt $C\sigma$
2. $\neg A[s']$ and $u[s'] \neq v$ are maximal, while $A[s']$ and $u[s'] = v$ are strictly maximal wrt $D\sigma$
3. $(s = t)\sigma \not\succeq (u[s'] = v)\sigma$

Definition

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

$$\mathrm{Res}_{\mathrm{SP}}(\mathcal{C}) = \{D \mid D \text{ is conclusion of ORe–EFc with premises in } \mathcal{C}\}$$

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

Example

re-consider $\mathcal{C} = \{\mathsf{c} \neq \mathsf{d}, \mathsf{b} = \mathsf{d}, \mathsf{a} \neq \mathsf{d} \vee \mathsf{a} = \mathsf{c}, \mathsf{a} = \mathsf{b} \vee \mathsf{a} = \mathsf{d}\}$ together with the term order: $\mathsf{a} \succ \mathsf{b} \succ \mathsf{c} \succ \mathsf{d}$; without equality factoring only the following tautology is derivable:

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

together with the literal order:

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

Candidate Models

Definitions

- let $\mathcal{O}$ be a clause inference operator
- let $\mathcal{I}$ denote a mapping that assigns to each ground clause set $\mathcal{C}$ an equality (Herbrand) interpretation, the candidate model $\mathcal{I}_{\mathcal{C}}$
- if $\mathcal{I}_{\mathcal{C}} \not\models \mathcal{C}$ there $\exists$ minimal counter-example C
- $\mathcal{O}$ has reduction property if
  1. $\forall$ clause sets $\mathcal{C}$
  2. $\forall$ minimal counter-examples C for $\mathcal{I}_{\mathcal{C}}$
  3. $\exists$ inference from $\mathcal{C}$ in $\mathcal{O}$

$$\frac{C_1 \quad \ldots \quad C_n \quad C}{D}$$

where $\mathcal{I}_{\mathcal{C}} \models C_i$, $\mathcal{I}_{\mathcal{C}} \not\models D$ and $C \succ_{\mathsf{C}} D$

Theorem

let $\mathcal{O}$ be sound and have the reduction property and let $\mathcal{C}$ be saturated wrt $\mathcal{O}$, then $\mathcal{C}$ is unsatisfiable iff $\mathcal{C}$ contains the empty clause

Assumption

in the following we assume a language that contains $=$ as only predicate; for now we restrict to ground clauses

equality Herbrand interpretations are respresentable by a convergent (wrt $\succ$) ground TRS

Definition

a clause $C \vee s = t$ is reductive if (i) $s \succ t$ and (ii) $s = t$ is strictly maximal wrt C

NB: a reductive clause may be viewed as a conditional rewrite rule, where negation is interpreted as non-derivability let $\mathcal{C}_C = \{D \in \mathcal{C} \mid C \succ_C D\}$

Definition

we define a mapping $\mathcal{I}$ that assigns to $\forall\, \mathcal{C}_C$ a convergent TRS $\mathcal{I}_{\mathcal{C}_C}$

$\mathcal{I}_{\mathcal{C}_C}$ is the set of all ground rewrite rules $s \to t$ such that

1. $\exists\, D = (C' \vee s = t) \in \mathcal{C}$ with $C \succ_C D$
2. D is reductive for $s = t$
3. D is counter-example for $\mathcal{I}_{\mathcal{C}_D}$
4. s is in normal form wrt $\mathcal{I}_{\mathcal{C}_D}$
5. C' is counter-example for $\mathcal{I}_{\mathcal{C}_D} \cup \{s = t\}$
6. we call D productive

Theorem

let $\mathcal{C}$ be a ground clause set not containing $\Box$; C a minimal counter-example to $\mathcal{I}_{\mathcal{C}}$, constructed as above; $\exists\, D \in \mathrm{Res}_{\mathrm{SP}}(\mathcal{C})$ such that $C \succ_C D$ and D is also a counter-example

Redundancy and Saturation

Definitions

- a ground clause C is redundant wrt a ground clause set $\mathcal{C}$ if $\exists\, C_1$, $\dots$, C_k in $\mathcal{C}$ such that

$$C_1, \dots, C_k \models C \qquad C \succ C_i$$

- a ground inference with main premise C

$$\frac{C_1 \quad \dots \quad C_n \quad C}{D}$$

  is redundant (wrt $\mathcal{C}$) if

  1. $D \succcurlyeq C$, or
  2. $\exists\, D_1, \dots, D_k$ with $D_i \in \mathcal{C}_C$ such that $D_1, \dots, D_k, C_1, \dots, C_n \models D$

- $\mathcal{C}$ is saturated upto redundancy if all inferences from non-redundant premises are redundant

Soundness and Completeness of Superposition

Theorem

let $\mathcal{O}$ be sound and have the reduction property and let $\mathcal{C}$ be saturated upto redundancy wrt $\mathcal{O}$, then $\mathcal{C}$ is unsatisfiable iff $\mathcal{C}$ contains the empty clause

Proof.

on the whiteboard ∎

Lemma

non-redundant superposition inferences are liftable

Theorem

superposition is sound and complete; let F be a sentence and $\mathcal{C}$ its clause form; then F is unsatisfiable iff $\Box \in \mathrm{Res}_{\mathrm{SP}}{}^*(\mathcal{C})$