Propositional and Predicate Logic - XI

Petr Gregor

KTIML MFF UK

WS 2015/2016

The general resolution rule

Let C_1, C_2 be clauses with distinct variables such that

$$C_1 = C_1' \sqcup \{A_1, \dots, A_n\}, \quad C_2 = C_2' \sqcup \{\neg B_1, \dots, \neg B_m\},$$

where $S = \{A_1, \dots, A_n, B_1, \dots, B_m\}$ is unifiable and $n, m \geq 1$. Then the clause

$$C = C_1'\sigma \cup C_2'\sigma,$$

where σ is a most general unification of S, is the *resolvent* of C_1 and C_2.

For example, in clauses $\{P(x), Q(x,z)\}$ *and* $\{\neg P(y), \neg Q(f(y), y)\}$ *we can* unify $S = \{Q(x,z), Q(f(y), y)\}$ applying a most general unification $\sigma = \{x/f(y), z/y\}$, and then resolve to a clause $\{P(f(y)), \neg P(y)\}$.

Remark *The condition on distinct variables can be satisfied by renaming variables apart. This is sometimes necessary, e.g. from* $\{\{P(x)\}, \{\neg P(f(x))\}\}$ *after renaming we can get* $\square$*, but* $\{P(x), P(f(x))\}$ *is not unifiable.*

Resolution in predicate logic - an example

Consider $T = \{\neg P(x,x),\ P(x,y) \rightarrow P(y,x),\ P(x,y) \wedge P(y,z) \rightarrow P(x,z)\}$.

Is $T \models (\exists x)\neg P(x, f(x))$? Equivalently, is the following T' unsatisfiable?

$T' = \{\{\neg P(x,x)\}, \{\neg P(x,y), P(y,x)\}, \{\neg P(x,y), \neg P(y,z), P(x,z)\}, \{P(x, f(x))\}\}$

$T' \vdash_R \square$

$\square$

x'/x

$\{P(x,x)\}$ $\quad$ $\{\neg P(x',x')\}$

$z/x, x'/x$

$\{\neg P(f(x),z), P(x,z)\}$ $\quad$ $\{P(f(x'),x')\}$

$y/f(x), x'/x$ $\quad$ $x/x', y/f(x')$

$\{\neg P(x,y), \neg P(y,z), P(x,z)\}$ $\quad$ $\{P(x', f(x'))\}$ $\quad$ $\{\neg P(x,y), P(y,x)\}$ $\quad$ $\{P(x', f(x'))\}$

Soundness of resolution

First we show soundness of the general resolution rule.

Proposition Let C be a resolvent of clauses C_1, C_2. For every L-structure $\mathcal{A}$,

$$\mathcal{A} \models C_1 \text{ and } \mathcal{A} \models C_2 \quad \Rightarrow \quad \mathcal{A} \models C.$$

Proof Let $C_1 = C_1' \sqcup \{A_1, \ldots, A_n\}$, $C_2 = C_2' \sqcup \{\neg B_1, \ldots, \neg B_m\}$, σ be a most general unification for $S = \{A_1, \ldots, A_n, B_1, \ldots, B_m\}$, and $C = C_1'\sigma \cup C_2'\sigma$.

- Since C_1, C_2 are open, it holds also $\mathcal{A} \models C_1\sigma$ and $\mathcal{A} \models C_2\sigma$.
- We have $C_1\sigma = C_1'\sigma \cup \{S\sigma\}$ and $C_2\sigma = C_2'\sigma \cup \{\neg(S\sigma)\}$.
- We show $\mathcal{A} \models C[e]$ for every e. If $\mathcal{A} \models S\sigma[e]$, then $\mathcal{A} \models C_2'\sigma[e]$, and thus $\mathcal{A} \models C[e]$. Otherwise $\mathcal{A} \not\models S\sigma[e]$, so $\mathcal{A} \models C_1'\sigma[e]$, and thus $\mathcal{A} \models C[e]$. $\square$

Theorem (soundness) *If S is resolution refutable, then S is unsatisfiable.*

Proof Let $S \vdash_R \square$. Suppose $\mathcal{A} \models S$ for some structure $\mathcal{A}$. By soundness of the general resolution rule we have $\mathcal{A} \models \square$, which is impossible. $\blacksquare$

Lifting lemma

A resolution proof on propositional level can be "lifted" to predicate level.

Lemma *Let $C_1^* = C_1\tau_1$, $C_2^* = C_2\tau_2$ be ground instances of clauses C_1, C_2 with distinct variables and C^* be a resolvent of C_1^* a C_2^*. Then there exists a resolvent C of C_1 and C_2 such that $C^* = C\tau_1\tau_2$ is a ground instance of C.*

Proof Assume that C^* is a resolvent of C_1^*, C_2^* through a literal $P(t_1,\ldots,t_k)$.

- We have $C_1 = C_1' \sqcup \{A_1,\ldots,A_n\}$ and $C_2 = C_2' \sqcup \{\neg B_1,\ldots,\neg B_m\}$, where $\{A_1,\ldots,A_n\}\tau_1 = \{P(t_1,\ldots,t_k)\}$ and $\{\neg B_1,\ldots,\neg B_m\}\tau_2 = \{\neg P(t_1,\ldots,t_k)\}$
- Thus $(\tau_1\tau_2)$ unifies $S = \{A_1,\ldots,A_n,B_1,\ldots,B_m\}$ and if σ is mgu of S from the unification algorithm, then $C = C_1'\sigma \cup C_2'\sigma$ is a resolvent of C_1, C_2.
- Moreover, $(\tau_1\tau_2) = \sigma(\tau_1\tau_2)$ by the property $(*)$ for σ, and hence

$$\begin{aligned}
C\tau_1\tau_2 &= (C_1'\sigma \cup C_2'\sigma)\tau_1\tau_2 = C_1'\sigma\tau_1\tau_2 \cup C_2'\sigma\tau_1\tau_2 = C_1'\tau_1 \cup C_2'\tau_2 \\
&= (C_1 \setminus \{A_1,\ldots,A_n\})\tau_1 \cup (C_2 \setminus \{\neg B_1,\ldots,\neg B_m\})\tau_2 \\
&= (C_1^* \setminus \{P(t_1,\ldots,t_k)\}) \cup (C_2^* \setminus \{\neg P(t_1,\ldots,t_k)\}) = C^*. \quad \square
\end{aligned}$$

Completeness

Corollary *Let S' be the set of all ground instances of clauses of formula S. If $S' \vdash_R C'$ (on prop. level) where C' is a ground clause, then $C' = C\sigma$ for some clause C and a ground substitution σ such that $S \vdash_R C$ (on pred. level).*

Proof By induction on the length of resolution proof using lifting lemma. $\square$

Theorem (completeness) *If S is unsatisfiable, then $S \vdash_R \square$.*

Proof If S is unsatisfiable, then by the (corollary of) Herbrand's theorem, also the set S' of all ground instances of clauses of S is unsatisfiable.

- By completeness of resolution in prop. logic, $S' \vdash_R \square$ (on prop. level).
- By the above corollary, there is a clause C and a ground substitution σ such that $\square = C\sigma$ and $S \vdash_R C$ (on pred. level).
- The only clause that has $\square$ as a ground instance is the clause $C = \square$. $\blacksquare$

Hilbert's calculus in predicate logic

- basic connectives and quantifier: $\neg$, $\rightarrow$, $(\forall x)$ (others are derived)
- allows to prove any formula (not just sentences)
- *logical axioms* (schemes of axioms):

$$
\begin{array}{rcl}
(i) & \varphi \rightarrow (\psi \rightarrow \varphi) & \\
(ii) & (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi)) & \\
(iii) & (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi) & \\
(iv) & (\forall x)\varphi \rightarrow \varphi(x/t) & \text{if } t \text{ is substitutable for } x \text{ to } \varphi \\
(v) & (\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi) & \text{if } x \text{ is not free in } \varphi
\end{array}
$$

  where φ, ψ, χ are any formulas (of a given language), t is any term, and x is any variable
- in a language with equality we include also the axioms of equality
- *rules of inference*

$$\frac{\varphi,\ \varphi \rightarrow \psi}{\psi} \quad \text{(modus ponens)}, \qquad \frac{\varphi}{(\forall x)\varphi} \quad \text{(generalization)}$$

Hilbert-style proofs

A *proof* (in *Hilbert-style*) of a formula φ from a theory T is a finite sequence $\varphi_0, \dots, \varphi_n = \varphi$ of formulas such that for every $i \leq n$

- φ_i is a logical axiom or $\varphi_i \in T$ (an axiom of the theory), or
- φ_i can be inferred from the previous formulas applying a rule of inference.

A formula φ is *provable* from T if it has a proof from T, denoted by $T \vdash_H \varphi$.

Theorem (soundness) *For every theory T and formula φ, $T \vdash_H \varphi \;\Rightarrow\; T \models \varphi$.*

Proof

- If φ is an axiom (logical or from T), then $T \models \varphi$ (l. axioms are tautologies),
- if $T \models \varphi$ and $T \models \varphi \rightarrow \psi$, then $T \models \psi$, i.e. modus ponens is sound,
- if $T \models \varphi$, then $T \models (\forall x)\varphi$, i.e. generalization is sound,
- thus every formula in a proof from T is valid in T. $\square$

Remark *The completeness holds as well, i.e. $T \models \varphi \Rightarrow T \vdash_H \varphi$.*