Theorem Proving in Isabelle

Lutz Schröder

January 18, 2005

Resolution

Resolution

Resolution

- Resolution uses unification to chain meta-implications together

Resolution

- Resolution uses unification to chain meta-implications together
- Less poetically put:

$$\frac{\psi_1 \Longrightarrow \psi_2 \quad \phi_1 \Longrightarrow \phi_2}{(\psi_1 \Longrightarrow \phi_2)\sigma} \, (\psi_2\sigma = \phi_1\sigma);$$

the constraint $\psi_2\sigma = \phi_1\sigma$ requires unification.

Resolution

- Resolution uses unification to chain meta-implications together
- Less poetically put:

$$\frac{\psi_1 \Longrightarrow \psi_2 \quad \phi_1 \Longrightarrow \phi_2}{(\psi_1 \Longrightarrow \phi_2)\sigma} \, (\psi_2\sigma = \phi_1\sigma);$$

the constraint $\psi_2\sigma = \phi_1\sigma$ requires unification.

A simple example

A simple example

Want to derive new rule

$$\frac{R \to P \to Q \quad R \quad P}{Q}.$$

A simple example

Want to derive new rule

$$\frac{R \longrightarrow P \longrightarrow Q \quad R \quad P}{Q}.$$

Associated proof tree:

$$\dfrac{\dfrac{R \longrightarrow P \longrightarrow Q \quad R}{P \longrightarrow Q}(\longrightarrow E) \qquad P}{Q}(\longrightarrow E)$$

A simple example

Want to derive new rule

$$\frac{R \to P \to Q \quad R \quad P}{Q}.$$

Associated proof tree:

$$\cfrac{\cfrac{R \to P \to Q \quad R}{P \to Q}\,(\to E) \qquad P}{Q}\,(\to E)$$

$\boxed{\text{Try this in Isabelle}}$

Another example

Another example

Have

$$\forall x\ y.\ Suc(x) = Suc(y) \longrightarrow x = y;$$

Another example

Have

$$\forall x\ y.\ Suc(x) = Suc(y) \to x = y;$$

Want to derive rule

$$\frac{Suc(m) = Suc(n)}{m = n},$$

Another example

Have

$$\forall x\ y.\ Suc(x) = Suc(y) \longrightarrow x = y;$$

Want to derive rule

$$\frac{Suc(m) = Suc(n)}{m = n},$$

i.e.

$$Suc(?m) = Suc(?n) \Longrightarrow ?m = ?n.$$

Another example (cont'd)

Another example (cont'd)

'Paper' proof:

$$\dfrac{\dfrac{\dfrac{\forall x\ y.\, Suc(x) = Suc(y) \longrightarrow x = y}{\forall y.\, Suc(?m) = Suc(y) \longrightarrow ?m = y}}{Suc(?m) = Suc(?n) \longrightarrow ?m = ?n} \qquad Suc(?m) = Suc(?n)}{?m = ?n}\,(\longrightarrow E)$$

(first two steps by $\forall E$)

Another example (cont'd)

'Paper' proof:

$$\dfrac{\dfrac{\dfrac{\forall x\ y.\, Suc(x) = Suc(y) \rightarrow x = y}{\forall y.\, Suc(?m) = Suc(y) \rightarrow ?m = y}}{Suc(?m) = Suc(?n) \rightarrow ?m = ?n} \qquad Suc(?m) = Suc(?n)}{?m = ?n}\,(\rightarrow E)$$

(first two steps by $\forall E$)

Check it out!

Lifting

Lifting

What about resolution with

$$(\to I)\ \frac{P \Longrightarrow Q}{P \to Q} \quad \text{or} \quad (\forall I)\ \frac{\bigwedge x.\, P}{\forall x.\, P} \quad ?$$

Problem: The premises contain meta-logical symbols ($\Longrightarrow$, $\bigwedge$), hence do not match conclusion of any other rule!

Lifting over assumptions

Lifting over assumptions

Solution for $(\longrightarrow I)$: introduce additional assumption in premise and conclusion;

Lifting over assumptions

Solution for $(\rightarrow I)$: introduce additional assumption in premise and conclusion;

Meta-rule:

$$\frac{\phi \Longrightarrow \psi}{(\theta \Longrightarrow \phi) \Longrightarrow (\theta \Longrightarrow \psi)}$$

Example

Example

Want to resolve $\longrightarrow I$ with $\wedge I$, i.e. $[\![?P; ?Q]\!] \Longrightarrow ?P \wedge ?Q$.

Example

Want to resolve $\longrightarrow I$ with $\wedge I$, i.e. $[\![?P; ?Q]\!] \Longrightarrow ?P \wedge ?Q$.

Lifting over an unknown assumption $?R$ yields

$$[\![?R \Longrightarrow ?P; ?R \Longrightarrow ?Q]\!] \Longrightarrow (?R \Longrightarrow ?P \wedge ?Q).$$

Example

Want to resolve $\longrightarrow I$ with $\wedge I$, i.e. $[\![?P; ?Q]\!] \Longrightarrow ?P \wedge ?Q$.

Lifting over an unknown assumption $?R$ yields

$$[\![?R \Longrightarrow ?P; ?R \Longrightarrow ?Q]\!] \Longrightarrow (?R \Longrightarrow ?P \wedge ?Q).$$

$\boxed{\text{Resolution with } \longrightarrow I}$, i.e. with $(?P \Longrightarrow ?Q) \Longrightarrow ?P \longrightarrow ?Q$:

$$[\![?R \Longrightarrow ?P; ?R \Longrightarrow ?Q]\!] \Longrightarrow (?R \longrightarrow ?P \wedge ?Q)$$

Lifting over parameters

Lifting over parameters

Solution for $\forall I$ and the like:

Lifting over parameters

Solution for $\forall I$ and the like:

- Introduce quantification over parameter x in premises and conclusion

Lifting over parameters

Solution for $\forall I$ and the like:

- Introduce quantification over parameter x in premises and conclusion
- Make all unknowns $?a$ depend on x: replace by $?a(x)$.

Lifting over parameters

Solution for $\forall I$ and the like:

- Introduce quantification over parameter x in premises and conclusion
- Make all unknowns $?a$ depend on x: replace by $?a(x)$.
- Meta-rule:

$$\frac{\phi \Longrightarrow \psi}{\bigwedge x.\, \phi^x \Longrightarrow \bigwedge x.\, \psi^x}$$

(ϕ^x is ϕ with parametrized unknowns)

An example

An example

Want to resolve $\wedge E1$, i.e. $?P \wedge ?Q \Longrightarrow ?P$, with $\forall I$, i.e. $\bigwedge x.\, ?P(x) \Longrightarrow \forall x.\, ?P(x)$.

Lift $\wedge E1$ over parameter x:

$$\bigwedge x.\, ?P(x) \wedge ?Q(x) \Longrightarrow \bigwedge x.\, ?P(x)$$

$\boxed{\text{Resolve with } \forall I}$:

$$\bigwedge x.\, ?P(x) \wedge ?Q(x) \Longrightarrow \forall x.\, ?P(x)$$