Delayed instantiation of existential variables in presence of a theory

Damien Rouhling

ENS Lyon

PSATTT13

Context

- Automated deduction
- Modulo theories
- PSYCHE
- First order?

Outline

1. First order proof search
    - First order rules
    - Modulo theories reasonning
2. Variables instantiation
    - Merging method
    - Sequentialized method
    - Equivalence criteria

Outline

1. First order proof search
   - First order rules
   - Modulo theories reasonning
2. Variables instantiation
   - Merging method
   - Sequentialized method
   - Equivalence criteria

Dealing with first order rules

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ x \notin FV(\Gamma) \qquad\qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}$$

Dealing with first order rules

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ x \notin FV(\Gamma) \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}$$

Universal and existential ($?x$) variables :

$$\frac{\Gamma \vdash A[\mathbf{x}]}{\Gamma \vdash \forall x.A}\ x \notin FV(\Gamma) \qquad \frac{\Gamma \vdash A[?x]}{\Gamma \vdash \exists x.A}$$

Dealing with first order rules

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\ x \notin FV(\Gamma) \qquad\qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}$$

Universal and existential ($?x$) variables :

$$\frac{\Gamma \vdash A[\mathbf{x}]}{\Gamma \vdash \forall x.A}\ x \notin FV(\Gamma) \qquad\qquad \frac{\Gamma \vdash A[?x]}{\Gamma \vdash \exists x.A}$$

Existential variables like $?x$ are solved by first-order unification at different points of the proof-tree.

Outline

1. First order proof search
   - First order rules
   - Modulo theories reasonning
2. Variables instantiation
   - Merging method
   - Sequentialized method
   - Equivalence criteria

The difficulty

- A theory as parameter
- Some function symbols are interpreted by the axioms
  $\exists x. (P(x+1) \Rightarrow P(2))$
- Generic process? Unification modulo theories?

Module provided by the user (Black box): decision procedure

Outline

1. First order proof search
   - First order rules
   - Modulo theories reasonning
2. Variables instantiation
   - Merging method
   - Sequentialized method
   - Equivalence criteria

Black Box specification for pure first order

- Input: a sequent of the form $\Gamma \vdash P\,(u)$
- Behaviour: finds $P\,(t)$ in Γ, outputs $mgu\,(t, u)$, if it exists

This is denoted by Black Box$(\Gamma \vdash P\,(u)) \to mgu\,(t, u)$.

A simple idea

$$\frac{\text{Black Box}(\Gamma, P(t) \vdash P(u)) \to mgu(t, u)}{\Gamma, P(t) \vdash P(u) \;\; \to mgu(t, u)}$$

A simple idea

$$\frac{\text{Black Box}(\Gamma, P(t) \vdash P(u)) \rightarrow mgu(t, u)}{\Gamma, P(t) \vdash P(u) \ \rightarrow mgu(t, u)}$$

$$\frac{\text{sequent } 1 \rightarrow \sigma_1 \qquad \text{sequent } 2 \rightarrow \sigma_2}{\text{sequent} \rightarrow mgu(\sigma_1, \sigma_2)}$$

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(?y) \vdash P(f(?x))}{\vdash P(?y) \Rightarrow P(f(?x))} \qquad \dfrac{P(f(z)) \vdash P(?x)}{\vdash P(f(z)) \Rightarrow P(?x)}}{\vdash (P(?y) \Rightarrow P(f(?x))) \wedge (P(f(z)) \Rightarrow P(?x))}}{\vdash \exists y.((P(y) \Rightarrow P(f(?x))) \wedge (P(f(z)) \Rightarrow P(?x)))}}{\vdash \exists x.\exists y.((P(y) \Rightarrow P(f(x))) \wedge (P(f(z)) \Rightarrow P(x)))}}{\vdash \forall z.\exists x.\exists y.((P(y) \Rightarrow P(f(x))) \wedge (P(f(z)) \Rightarrow P(x)))}$$

Example 1

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(?y) \vdash P(f(?x)) \;\; \to \sigma_1}{\vdash P(?y) \Rightarrow P(f(?x))} \qquad \dfrac{P(f(z)) \vdash P(?x) \;\; \to \sigma_2}{\vdash P(f(z)) \Rightarrow P(?x)}}{\vdash (P(?y) \Rightarrow P(f(?x))) \wedge (P(f(z)) \Rightarrow P(?x))}}{\vdash \exists y. ((P(y) \Rightarrow P(f(?x))) \wedge (P(f(z)) \Rightarrow P(?x)))}}{\vdash \exists x. \exists y. ((P(y) \Rightarrow P(f(x))) \wedge (P(f(z)) \Rightarrow P(x)))}}{\vdash \forall z. \exists x. \exists y. ((P(y) \Rightarrow P(f(x))) \wedge (P(f(z)) \Rightarrow P(x)))}}{}
$$

$\sigma_1 = mgu(?y, f(?x))$ and $\sigma_2 = mgu(f(z), ?x)$ are given by the Black Box

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P(?y) \vdash P(f(?x)) \quad \to \sigma_1}{\vdash P(?y) \Rightarrow P(f(?x)) \quad \to \sigma_1} \qquad \dfrac{P(f(z)) \vdash P(?x) \quad \to \sigma_2}{\vdash P(f(z)) \Rightarrow P(?x) \quad \to \sigma_2}}{\vdash (P(?y) \Rightarrow P(f(?x))) \wedge (P(f(z)) \Rightarrow P(?x))}}{\vdash \exists y. ((P(y) \Rightarrow P(f(?x))) \wedge (P(f(z)) \Rightarrow P(?x)))}}{\vdash \exists x. \exists y. ((P(y) \Rightarrow P(f(x))) \wedge (P(f(z)) \Rightarrow P(x)))}}{\vdash \forall z. \exists x. \exists y. ((P(y) \Rightarrow P(f(x))) \wedge (P(f(z)) \Rightarrow P(x)))}}{}$$

$\sigma_1 = mgu(?y, f(?x))$ and $\sigma_2 = mgu(f(z), ?x)$ are given by the Black Box

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P\,(?y)\vdash P\,(f\,(?x)) \;\to \sigma_1}{\vdash P\,(?y)\Rightarrow P\,(f\,(?x)) \;\to \sigma_1} \qquad \dfrac{P\,(f\,(z))\vdash P\,(?x) \;\to \sigma_2}{\vdash P\,(f\,(z))\Rightarrow P\,(?x) \;\to \sigma_2}}{\vdash (P\,(?y)\Rightarrow P\,(f\,(?x)))\wedge(P\,(f\,(z))\Rightarrow P\,(?x)) \;\to \sigma}}{\vdash \exists y.((P\,(y)\Rightarrow P\,(f\,(?x)))\wedge(P\,(f\,(z))\Rightarrow P\,(?x)))}}{\vdash \exists x.\exists y.((P\,(y)\Rightarrow P\,(f\,(x)))\wedge(P\,(f\,(z))\Rightarrow P\,(x)))}}{\vdash \forall z.\exists x.\exists y.((P\,(y)\Rightarrow P\,(f\,(x)))\wedge(P\,(f\,(z))\Rightarrow P\,(x)))}$$

$\sigma_1 = mgu\,(?y, f\,(?x))$ and $\sigma_2 = mgu\,(f\,(z)\,, ?x)$ are given by the Black Box
$\sigma = \sigma_1 \wedge \sigma_2$ is $mgu\,(\sigma_1, \sigma_2)$

Example 2

$$\vdash \exists x. \left(P\left(x\right) \Rightarrow \forall y. P\left(y\right)\right)$$

Example 2

$$\frac{\vdash P\left(?x\right) \Rightarrow \forall y.P\left(y\right)}{\vdash \exists x.\left(P\left(x\right) \Rightarrow \forall y.P\left(y\right)\right)}$$

Example 2

$$\dfrac{\dfrac{P\,(?x) \vdash \forall y.P\,(y)}{\vdash P\,(?x) \Rightarrow \forall y.P\,(y)}}{\vdash \exists x.\,(P\,(x) \Rightarrow \forall y.P\,(y))}$$

Example 2

$$\dfrac{\dfrac{\dfrac{P(?x) \vdash P(y)}{P(?x) \vdash \forall y. P(y)}}{\vdash P(?x) \Rightarrow \forall y. P(y)}}{\vdash \exists x. (P(x) \Rightarrow \forall y. P(y))}$$

Example 2

$$\dfrac{\dfrac{\dfrac{P\,(?x) \vdash P\,(y)}{P\,(?x) \vdash \forall y.P\,(y)}}{\vdash P\,(?x) \Rightarrow \forall y.P\,(y)}}{\vdash \exists x.\,(P\,(x) \Rightarrow \forall y.P\,(y))}$$

$?x \mapsto y$ is needed, but the side condition is no longer verified: check after instantiating.

Generalisation

$$\frac{\text{Black Box(sequent)} \rightarrow \sigma}{\text{sequent} \rightarrow \sigma}$$

Generalisation

$$\frac{\text{Black Box(sequent)} \to \sigma}{\text{sequent} \to \sigma}$$

$$\frac{\text{sequent } 1 \to \sigma_1 \qquad \text{sequent } 2 \to \sigma_2}{\text{sequent} \to \sigma_1 \wedge \sigma_2}$$

The operator $\wedge$:

- is commutative and associative
- gives $\perp$ if no solution
- behaves well with instantiations

Local knowledge of the prooftree $\Rightarrow$ backtrack

Example

$$\frac{\dfrac{\dfrac{\vdash ?y < 2?x \qquad \vdash ?x > 3 \qquad \vdash ?x < 6}{\vdash (?y < 2?x) \wedge (?x > 3) \wedge (?x < 6)}}{\vdash \exists y.((y < 2?x) \wedge (?x > 3) \wedge (?x < 6))}}{\vdash \exists x.\exists y.((y < 2x) \wedge (x > 3) \wedge (x < 6))}$$

Example

$$\cfrac{\vdash ?y < 2?x \ \rightarrow \sigma_0 \qquad \vdash ?x > 3 \ \rightarrow \sigma_1 \qquad \vdash ?x < 6 \ \rightarrow \sigma_2}{\cfrac{\vdash (?y < 2?x) \wedge (?x > 3) \wedge (?x < 6)}{\cfrac{\vdash \exists y.((y < 2?x) \wedge (?x > 3) \wedge (?x < 6))}{\vdash \exists x.\exists y.((y < 2x) \wedge (x > 3) \wedge (x < 6))}}}$$

$\sigma_0 = (?y \in]-\infty, 2?x[)$, $\sigma_1 = (?x \in]3, +\infty[)$ and $\sigma_2 = (?x \in]-\infty, 6[)$.

Example

$$\dfrac{\dfrac{\dfrac{\vdash ?y < 2?x \ \rightarrow \sigma_0 \qquad \vdash ?x > 3 \ \rightarrow \sigma_1 \qquad \vdash ?x < 6 \ \rightarrow \sigma_2}{\vdash (?y < 2?x) \wedge (?x > 3) \wedge (?x < 6) \ \rightarrow \sigma_0 \wedge \sigma_1 \wedge \sigma_2 = \sigma}}{\vdash \exists y. ((y < 2?x) \wedge (?x > 3) \wedge (?x < 6))}}{\vdash \exists x. \exists y. ((y < 2x) \wedge (x > 3) \wedge (x < 6))}$$

$\sigma_0 = (?y \in]{-\infty}, 2?x[)$, $\sigma_1 = (?x \in]3, +\infty[)$ and $\sigma_2 = (?x \in]{-\infty}, 6[)$.
$\sigma = (?x \in \{4, 5\}, ?y \in]{-\infty}, 2?x[)$

Example

$$\cfrac{\cfrac{\vdash ?y < 2?x \ \to \sigma_0 \qquad \vdash ?x > 3 \ \to \sigma_1 \qquad \vdash ?x < 6 \ \to \sigma_2}{\vdash (?y < 2?x) \wedge (?x > 3) \wedge (?x < 6) \ \to \sigma_0 \wedge \sigma_1 \wedge \sigma_2 = \sigma} \ \sigma' = \mathit{bind}(\sigma)}{\cfrac{\vdash \exists y.\,((y < 2?x) \wedge (?x > 3) \wedge (?x < 6)) \ \to \sigma'}{\vdash \exists x.\exists y.\,((y < 2x) \wedge (x > 3) \wedge (x < 6)) \ \to \sigma''} \ \sigma'' = \mathit{bind}(\sigma')}$$

$\sigma_0 = (?y \in]-\infty, 2?x[)$, $\sigma_1 = (?x \in]3, +\infty[)$ and $\sigma_2 = (?x \in]-\infty, 6[)$.
$\sigma = (?x \in \{4, 5\}, ?y \in]-\infty, 2?x[)$
$\sigma' = (?x \in \{4, 5\})$
$\sigma'' = \emptyset$

Example

$$\dfrac{\dfrac{\dfrac{\vdash ?y < 2?x \ \rightarrow \sigma_0 \qquad \vdash ?x > 3 \ \rightarrow \sigma_1 \qquad \vdash ?x < 6 \ \rightarrow \sigma_2}{\vdash (?y < 2?x) \wedge (?x > 3) \wedge (?x < 6) \ \rightarrow \sigma_0 \wedge \sigma_1 \wedge \sigma_2 = \sigma}}{\vdash \exists y. ((y < 2?x) \wedge (?x > 3) \wedge (?x < 6)) \ \rightarrow \sigma'} \ \sigma' = \mathit{bind}\,(\sigma)}{\vdash \exists x. \exists y. ((y < 2x) \wedge (x > 3) \wedge (x < 6)) \ \rightarrow \sigma''} \ \sigma'' = \mathit{bind}\,(\sigma')$$

$\sigma_0 = (?y \in]-\infty, 2?x[)$, $\sigma_1 = (?x \in]3, +\infty[)$ and $\sigma_2 = (?x \in]-\infty, 6[)$.
$\sigma = (?x \in \{4, 5\}, ?y \in]-\infty, 2?x[)$
$\sigma' = (?x \in \{4, 5\})$
$\sigma'' = \emptyset$

Structures: a “substitution” maps each variable to a set of interval, according to its dependencies. $\wedge$ does the good intersections.

Example

$$\dfrac{\dfrac{\dfrac{\vdash ?y < 2?x \ \rightarrow \sigma_0 \qquad \vdash ?x > 3 \ \rightarrow \sigma_1 \qquad \vdash ?x < 6 \ \rightarrow \sigma_2}{\vdash (?y < 2?x) \wedge (?x > 3) \wedge (?x < 6) \ \rightarrow \sigma_0 \wedge \sigma_1 \wedge \sigma_2 = \sigma}\ \sigma' = \mathit{bind}\,(\sigma)}{\vdash \exists y.\,((y < 2?x) \wedge (?x > 3) \wedge (?x < 6)) \ \rightarrow \sigma'}\ \sigma'' = \mathit{bind}\,(\sigma')}{\vdash \exists x.\exists y.\,((y < 2x) \wedge (x > 3) \wedge (x < 6)) \ \rightarrow \sigma''}$$

The output “substitution” σ'' $(= \emptyset)$ isn't $\perp$: we can instantiate.

Example

$$\dfrac{\dfrac{\dfrac{\vdash \sigma\left(?y, \sigma'\left(?x\right)\right) < 2\sigma'\left(?x\right) \qquad \vdash \sigma'\left(?x\right) > 3 \qquad \vdash \sigma'\left(?x\right) < 6}{\vdash \left(\sigma\left(?y, \sigma'\left(?x\right)\right) < 2\sigma'\left(?x\right)\right) \land \left(\sigma'\left(?x\right) > 3\right) \land \left(\sigma'\left(?x\right) < 6\right)}}{\vdash \exists y. \left(\left(y < 2\sigma'\left(?x\right)\right) \land \left(\sigma'\left(?x\right) > 3\right) \land \left(\sigma'\left(?x\right) < 6\right)\right)}}{\vdash \exists x. \exists y. \left(\left(y < 2x\right) \land \left(x > 3\right) \land \left(x < 6\right)\right)}$$

Outline

A practical point of view

$$\frac{\text{Black Box}(\text{sequent}, \sigma) \rightarrow \sigma'}{\sigma \rightarrow \text{sequent} \rightarrow \sigma'}$$

A practical point of view

$$\frac{\sigma \to \text{sequent 1} \to \sigma_0 \qquad \sigma_0 \to \text{sequent 2} \to \sigma'}{\sigma \to \text{sequent} \to \sigma'}$$

or

$$\frac{\sigma_1 \to \text{sequent 1} \to \sigma' \qquad \sigma \to \text{sequent 2} \to \sigma_1}{\sigma \to \text{sequent} \to \sigma'}$$

Example

$$\emptyset \to \vdash \exists x.\,((x > 3) \wedge (x < 6)) \;\; \to ?$$

Example

$$\frac{\tilde{\emptyset} \rightarrow \vdash (?x > 3) \wedge (?x < 6) \quad \rightarrow ?}{\emptyset \rightarrow \vdash \exists x. ((x > 3) \wedge (x < 6)) \quad \rightarrow ?}$$

Example

$$\dfrac{\dfrac{\tilde{\emptyset} \rightarrow \vdash ?x > 3 \ \rightarrow \sigma_1 \qquad ? \rightarrow \vdash ?x < 6 \ \rightarrow ?}{\tilde{\emptyset} \rightarrow \vdash (?x > 3) \land (?x < 6) \ \rightarrow ?}}{\emptyset \rightarrow \vdash \exists x. ((x > 3) \land (x < 6)) \ \rightarrow ?}$$

$\sigma_1 = (?x \in]3, \infty[)$

Example

$$\frac{\dfrac{\tilde{\emptyset} \rightarrow \vdash ?x > 3 \ \rightarrow \sigma_1 \qquad \sigma_1 \rightarrow \vdash ?x < 6 \ \rightarrow \sigma_2}{\tilde{\emptyset} \rightarrow \vdash (?x > 3) \wedge (?x < 6) \ \rightarrow ?}}{\emptyset \rightarrow \vdash \exists x. ((x > 3) \wedge (x < 6)) \ \rightarrow ?}$$

$\sigma_1 = (?x \in]3, \infty[)$
$\sigma_2 = (?x \in \{4, 5\})$

Example

$$\dfrac{\tilde{\emptyset} \rightarrow \vdash ?x > 3 \ \rightarrow \sigma_1 \qquad \sigma_1 \rightarrow \vdash ?x < 6 \ \rightarrow \sigma_2}{\dfrac{\tilde{\emptyset} \rightarrow \vdash (?x > 3) \wedge (?x < 6) \ \rightarrow \sigma_2}{\emptyset \rightarrow \vdash \exists x. ((x > 3) \wedge (x < 6)) \ \rightarrow ?}}$$

$\sigma_1 = (?x \in]3, \infty[)$
$\sigma_2 = (?x \in \{4, 5\})$

Example

$$\dfrac{\dfrac{\tilde{\emptyset} \rightarrow \vdash ?x > 3 \;\rightarrow \sigma_1 \qquad \sigma_1 \rightarrow \vdash ?x < 6 \;\rightarrow \sigma_2}{\tilde{\emptyset} \rightarrow \vdash (?x > 3) \wedge (?x < 6) \;\rightarrow \sigma_2}}{\emptyset \rightarrow \vdash \exists x. ((x > 3) \wedge (x < 6)) \;\rightarrow \sigma} \; \sigma = bind\,(\sigma_2)$$

$\sigma_1 = (?x \in]3, \infty[)$
$\sigma_2 = (?x \in \{4, 5\})$
$\sigma = \emptyset$

Outline

With an “on-the-fly” instantiation system

- Soundness of the Black Box (dependencies)
- Generality of the “substitutions”
- Pseudo-generality of the instantiation choices
- Good backtracking

Between the two methods

- A leaf = a relation between "substitutions"
- A node = a relation composed with another
- Good relations: soundness and completeness of the Black Box
- Good backtracking

Conclusion

- Several instantiation schemes
- Some notions to clarify:
  - Stream production
  - Structure of the "substitutions" $\Rightarrow$ structure of the merge operation
  - How to manage the choices?

Conclusion

- Several instantiation schemes
- Some notions to clarify:
  - Stream production
  - Structure of the “substitutions” $\Rightarrow$ structure of the merge operation
  - How to manage the choices?

Thank you for your attention!