Goéland: A Concurrent Tableau-Based ATP that Produces Machine-Checkable Proofs

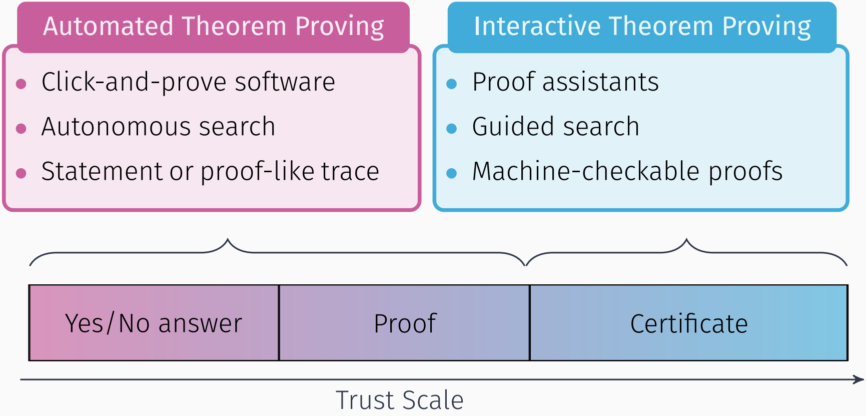
EuroProofNet School on Natural Formal Mathematics

Julie Cailler

June 3, 2025

VeriDis Team
University of Lorraine
CNRS, Inria, LORIA

Computer-Assisted Proofs



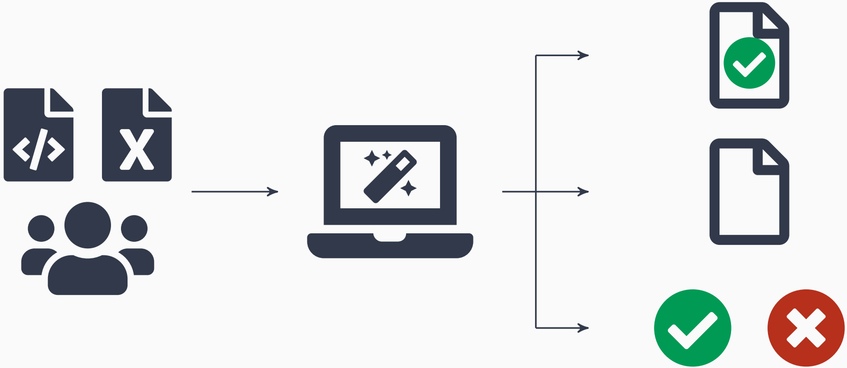
Automated Theorem Proving

- Click-and-prove software
- Autonomous search
- Statement or proof-like trace

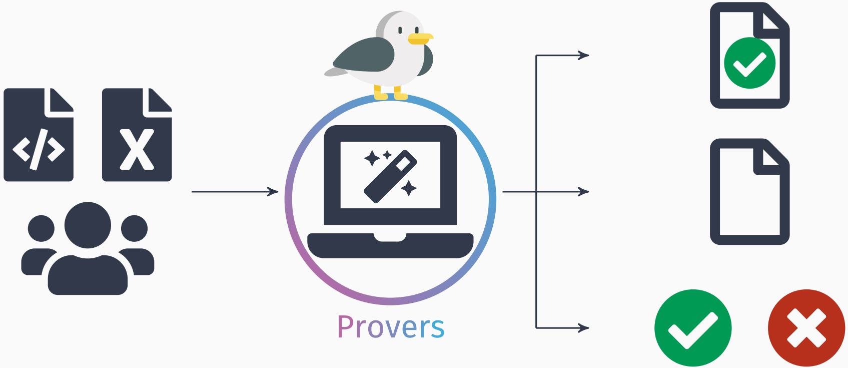
Interactive Theorem Proving

- Proof assistants
- Guided search
- Machine-checkable proofs

Big Picture



Big Picture



Provers

1. Preliminary Notions

Context

First-Order Logic (FOL)

- Expressivity: elements and properties about them
- Semi-decidable
- Efficient reasoning methods

Tableaux: Origin & Strengths

- Beth and Hintikka
- Extended by Smullyan and Fitting
- Unaltered original formula
- Output a proof

Method of Analytic Tableaux

Principle

- A set of axioms and one conjecture
- Refutation
- Syntactic rules: $\odot, \alpha, \delta, \beta, \gamma$
- Close all the branches

$$
\begin{array}{cl}
\neg(\exists x.\ P(x) \Rightarrow (P(a) \land P(b))) & \\ \hline
\neg(P(a) \Rightarrow (P(a) \land P(b))) & \gamma_{\neg\exists} \\ \hline
P(a), \neg(P(a) \land P(b)) & \alpha_{\neg\Rightarrow} \\ \hline
\begin{array}{cc}
\begin{array}{cl}
\neg P(a) & \\ \hline
\odot & \odot
\end{array}
&
\begin{array}{cl}
\neg P(b) & \\ \hline
\neg(P(b) \Rightarrow (P(a) \land P(b))) & \gamma_{\neg\exists} \\ \hline
P(b), \neg(P(a) \land P(b)) & \alpha_{\neg\Rightarrow} \\ \hline
\odot & \odot
\end{array}
\end{array} & \beta_{\neg\land}
\end{array}
$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\frac{Human(Socrates), \neg Human(Socrates)}{\odot}\ \odot$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$Human(Socrates)$$
$$\forall x.\ \neg Human(x)$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\cfrac{\begin{array}{c} Human(Socrates) \\ \forall x.\ \neg Human(x) \end{array}}{\neg Human(X)}\ \gamma\forall$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\dfrac{\dfrac{\begin{array}{c}Human(Socrates)\\ \forall x.\ \neg Human(x)\end{array}}{\neg Human(Socrates)}\,\gamma\forall}{\sigma = \{X \mapsto Socrates\}}\,\odot_{\sigma}$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\forall x.\ P(x)$$
$$\neg P(a) \lor \neg P(b)$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\forall x.\ P(x)$$

$$\frac{\neg P(a) \lor \neg P(b)}{P(X)}\ \gamma\forall$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\cfrac{\cfrac{\begin{array}{c}\forall x.\ P(x)\\ \neg P(a) \lor \neg P(b)\end{array}}{P(X)}\,\gamma_\forall}{\neg P(a) \qquad\qquad \neg P(b)}\,\beta_\lor$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\dfrac{\dfrac{\begin{array}{c}\forall x.\ P(x)\\ \neg P(a) \lor \neg P(b)\end{array}}{P(X)}\ \gamma_{\forall}}{\neg P(a) \qquad\qquad \neg P(b)}\ \beta_{\lor}$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\cfrac{\cfrac{\begin{array}{c}\forall x.\ P(x)\\ \neg P(a) \vee \neg P(b)\end{array}}{P(X)}\ \gamma_\forall}{\neg P(a) \qquad\qquad \neg P(b)}\ \beta_\vee$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$
\dfrac{
  \dfrac{
    \begin{array}{c}\forall x.\ P(x)\\ \neg P(a) \lor \neg P(b)\end{array}
  }{P(X)}\,\gamma_{\forall}
}{
  \dfrac{\neg P(a)}{\sigma = \{X \mapsto a\}}\,\odot_{\sigma}
  \qquad\qquad
  \neg P(b)
}\,\beta_{\lor}
$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\cfrac{\begin{array}{c}\forall x.\ P(x)\\ \cfrac{\neg P(a) \lor \neg P(b)}{P(a)}\,\gamma_{\forall}\end{array}}{\cfrac{\neg P(a)}{\sigma = \{X \mapsto a\}}\,\odot_{\sigma} \qquad\qquad \neg P(b)}\,\beta_{\lor}$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\begin{array}{c} \forall x.\ P(x) \\ \dfrac{\neg P(a) \vee \neg P(b)}{P(a)}\,\gamma_\forall \\ \hline \begin{array}{cc} \dfrac{\neg P(a)}{\sigma = \{X \mapsto a\}}\,\odot_\sigma & \qquad \dfrac{\neg P(b)}{P(X_2)}\,\gamma_\forall \end{array} \end{array}\,\beta_\vee$$

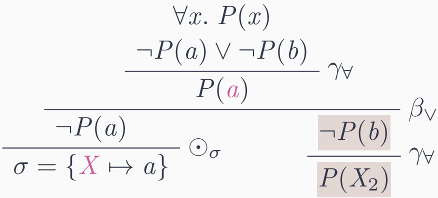
Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)



$\forall x.\ P(x)$

$\neg P(a) \vee \neg P(b)$

$\gamma_\forall$

$P(a)$

$\beta_\vee$

$\neg P(a)$

$\odot_\sigma$

$\sigma = \{X \mapsto a\}$

$\neg P(b)$

$\gamma_\forall$

$P(X_2)$

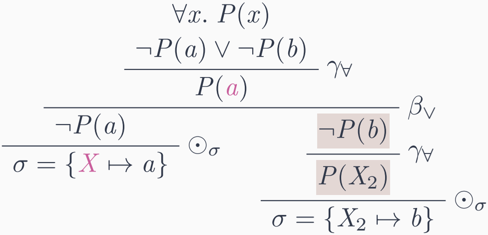
Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)



$$\forall x.\ P(x)$$

$$\dfrac{\neg P(a) \vee \neg P(b)}{P(a)}\ \gamma_\forall$$

$$\beta_\vee$$

$$\dfrac{\neg P(a)}{\sigma = \{X \mapsto a\}}\ \odot_\sigma \qquad \dfrac{\dfrac{\neg P(b)}{P(X_2)}\ \gamma_\forall}{\sigma = \{X_2 \mapsto b\}}\ \odot_\sigma$$

Tableau-Based Proof-Search Procedure

Rules

- $\odot$: Closure rule
- α, β: Expand the tree
- γ: Free variables
- δ: Skolemization

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\dfrac{\dfrac{\begin{array}{c}\forall x.\ P(x)\\ \neg P(a) \lor \neg P(b)\end{array}}{P(a)}\,\gamma_\forall}{\dfrac{\neg P(a)}{\sigma = \{X \mapsto a\}}\,\odot_\sigma \qquad \dfrac{\dfrac{\neg P(b)}{P(b)}\,\gamma_\forall}{\sigma = \{X_2 \mapsto b\}}\,\odot_\sigma}\,\beta_\lor$$

2. Fairness Management in Tableau Proof-Search Procedure: a Concurrent Approach

Fairness Management

Unfairness Sources

- The selection of a branch B
- Determining whether B should be closed or expanded
- If B is to be closed, the choice of a pair of complementary literals and thus a closing substitution
- If B is to be expanded, the selection of a formula to which an expansion rule is applied

Fairness Management

Unfairness Sources

- The selection of a branch B
- Determining whether B should be closed or expanded
- If B is to be closed, the choice of a pair of complementary literals and thus a closing substitution
- If B is to be expanded, the selection of a formula to which an expansion rule is applied

State-of-the-Art Answers & Heuristics

- Limit the number of application of γ-rules
- Iterative deepening
- Rules ordering ($\odot \prec \alpha \prec \delta \prec \beta \prec \gamma$)

Motivating Example

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))$$

Motivating Example

$$\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \vee Q(x)) \wedge \forall y.\ S(x))\end{array}}{\begin{array}{c}P(X) \vee Q(X)\\ \forall y.\ S(X)\end{array}}\ \gamma_{\forall} + \alpha_{\wedge}$$

Motivating Example

$$
\begin{array}{cl}
\neg P(a) & \\
\neg Q(b) & \\
\neg S(c) & \\
\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x)) & \\
\cline{1-1}
P(X) \lor Q(X) & \gamma_{\forall} + \alpha_{\land} \\
\forall y.\ S(X) & \\
\cline{1-1}
\begin{array}{ccc} P(X) & \qquad\qquad & Q(X) \\ \forall y.\ S(X) & & \forall y.\ S(X) \end{array} & \beta_{\lor}
\end{array}
$$

Motivating Example

$$\begin{array}{cl}
\neg P(a) & \\
\neg Q(b) & \\
\neg S(c) & \\
\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x)) & \\ \cline{1-1}
P(X) \lor Q(X) & \gamma_\forall + \alpha_\land \\
\forall y.\ S(X) & \\ \cline{1-1}
\begin{array}{ccc} P(X) & \qquad\qquad & Q(X) \\ \forall y.\ S(X) & & \forall y.\ S(X) \end{array} & \beta_\lor
\end{array}$$

Motivating Example

$$\dfrac{\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \vee Q(x)) \wedge \forall y.\ S(x))\end{array}}{\begin{array}{c}P(X) \vee Q(X)\\ \forall y.\ S(X)\end{array}}\ \gamma_\forall + \alpha_\wedge}{\dfrac{\begin{array}{c}P(X)\\ \forall y.\ S(X)\end{array}}{\sigma = \{X \mapsto a\}}\ \odot_\sigma \qquad\qquad \begin{array}{c}Q(X)\\ \forall y.\ S(X)\end{array}}\ \beta_\vee$$

Motivating Example

$$
\begin{array}{c}
\neg P(a) \\
\neg Q(b) \\
\neg S(c) \\
\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{P(a) \lor Q(a)} \ \gamma_\forall + \alpha_\land \\
\dfrac{\forall y.\ S(a)}{\begin{array}{cc} \dfrac{\begin{array}{c} P(a) \\ \forall y.\ S(a) \end{array}}{\sigma = \{X \mapsto a\}} \ \odot_\sigma & \qquad\qquad \begin{array}{c} Q(a) \\ \forall y.\ S(a) \end{array} \end{array}} \ \beta_\lor
\end{array}
$$

Motivating Example

$$\neg P(a)$$

$$\neg Q(b)$$

$$\neg S(c)$$

$$\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{P(a) \lor Q(a)}\ \gamma_\forall + \alpha_\land$$

$$\forall y.\ S(a)$$

$$\begin{array}{cc} \hline P(a) & Q(a) \\ \dfrac{\forall y.\ S(a)}{\sigma = \{X \mapsto a\}}\ \odot_\sigma & \dfrac{\forall y.\ S(a)}{S(a)}\ \gamma_\forall \end{array}\ \beta_\lor$$

Motivating Example

$$\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x)\lor Q(x))\land\forall y.\ S(x))\end{array}}{\dfrac{\begin{array}{c}P(a)\lor Q(a)\\ \forall y.\ S(a)\end{array}}{\dfrac{\begin{array}{c}P(a)\\ \forall y.\ S(a)\end{array}}{\sigma=\{X\mapsto a\}}\ \odot_\sigma \qquad\qquad \dfrac{\dfrac{\begin{array}{c}Q(a)\\ \forall y.\ S(a)\end{array}}{S(a)}\ \gamma_\forall}{\begin{array}{c}P(X_2)\lor Q(X_2)\\ \forall y.\ S(X_2)\end{array}}\ \gamma_\forall+\alpha_\land}\ \beta_\lor}\ \gamma_\forall+\alpha_\land$$

Motivating Example

$$\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))\end{array}}{\dfrac{\begin{array}{c}P(a) \lor Q(a)\\ \forall y.\ S(a)\end{array}}{\dfrac{\begin{array}{c}P(a)\\ \forall y.\ S(a)\end{array}}{\sigma = \{X \mapsto a\}}\ \odot_\sigma \qquad \begin{array}{c}Q(a)\\ \dfrac{\dfrac{\dfrac{\forall y.\ S(a)}{S(a)}\ \gamma_\forall}{\begin{array}{c}P(X_2) \lor Q(X_2)\\ \forall y.\ S(X_2)\end{array}}\ \gamma_\forall + \alpha_\land}{\begin{array}{c}P(X_2)\\ \forall y.\ S(X_2)\end{array} \qquad \begin{array}{c}Q(X_2)\\ \forall y.\ S(X_2)\end{array}}\ \beta_\lor\end{array}}\ \beta_\lor}\ \gamma_\forall + \alpha_\land$$

Motivating Example

$$\neg P(a)$$

$$\neg Q(b)$$

$$\neg S(c)$$

$$\dfrac{\forall x.\ ((P(x) \vee Q(x)) \wedge \forall y.\ S(x))}{\begin{array}{c} P(a) \vee Q(a) \\ \forall y.\ S(a) \end{array}}\ \gamma_\forall + \alpha_\wedge$$

$$\dfrac{\begin{array}{c} P(a) \vee Q(a) \\ \forall y.\ S(a) \end{array}}{P(a) \qquad\qquad\qquad Q(a)}\ \beta_\vee$$

$$P(a)$$

$$\dfrac{\forall y.\ S(a)}{\sigma = \{X \mapsto a\}}\ \odot_\sigma$$

$$Q(a)$$

$$\dfrac{\forall y.\ S(a)}{S(a)}\ \gamma_\forall$$

$$\dfrac{S(a)}{\begin{array}{c} P(X_2) \vee Q(X_2) \\ \forall y.\ S(X_2) \end{array}}\ \gamma_\forall + \alpha_\wedge$$

$$\dfrac{\begin{array}{c} P(X_2) \vee Q(X_2) \\ \forall y.\ S(X_2) \end{array}}{P(X_2) \qquad\qquad Q(X_2)}\ \beta_\vee$$

$$P(X_2) \qquad\qquad\qquad Q(X_2)$$

$$\dfrac{\forall y.\ S(X_2)}{\cdots} \qquad\qquad \dfrac{\forall y.\ S(X_2)}{\cdots}$$

Motivating Example — A Better Heuristic

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))$$

Motivating Example — A Better Heuristic

$$\frac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))\end{array}}{\begin{array}{c}P(X) \lor Q(X)\\ \forall y.\ S(X)\end{array}}\ \gamma_{\forall} + \alpha_{\land}$$

Motivating Example — A Better Heuristic

$$\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))\end{array}}{\dfrac{\begin{array}{c}P(X) \lor Q(X)\\ \forall y.\ S(X)\end{array}}{\begin{array}{cc}P(X) & Q(X)\\ \forall y.\ S(X) & \forall y.\ S(X)\end{array}}\ \beta_{\lor}}\ \gamma_{\forall} + \alpha_{\land}$$

Motivating Example — A Better Heuristic

$$\begin{array}{c}
\neg P(a) \\
\neg Q(b) \\
\neg S(c) \\
\dfrac{\forall x.\, ((P(x) \lor Q(x)) \land \forall y.\, S(x))}{\dfrac{\begin{array}{c} P(X) \lor Q(X) \\ \forall y.\, S(X) \end{array}}{\begin{array}{cc} \begin{array}{c} P(X) \\ \dfrac{\forall y.\, S(X)}{S(X)}\, \gamma_\forall \end{array} & \begin{array}{c} Q(X) \\ \forall y.\, S(X) \end{array} \end{array}}\, \beta_\lor}\, \gamma_\forall + \alpha_\land
\end{array}$$

Motivating Example — A Better Heuristic

$$
\begin{array}{c}
\neg P(a)\\
\neg Q(b)\\
\neg S(c)\\
\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{\dfrac{\begin{array}{c}P(X) \lor Q(X)\\ \forall y.\ S(X)\end{array}}{\begin{array}{cc} \dfrac{\dfrac{\begin{array}{c}P(X)\\ \forall y.\ S(X)\end{array}}{S(X)}\ \gamma_\forall}{\sigma = \{X \mapsto c\}}\ \odot_\sigma & \begin{array}{c}Q(X)\\ \forall y.\ S(X)\end{array}\end{array}}\ \beta_\lor}\ \gamma_\forall + \alpha_\land
\end{array}
$$

Motivating Example — A Better Heuristic

$$\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))\end{array}}{\dfrac{\begin{array}{c}P(c) \lor Q(c)\\ \forall y.\ S(c)\end{array}}{\begin{array}{cc}\begin{array}{c}P(c)\\ \dfrac{\dfrac{\forall y.\ S(c)}{S(c)}\ \gamma_\forall}{\sigma = \{X \mapsto c\}}\ \odot_\sigma\end{array} & \begin{array}{c}Q(c)\\ \forall y.\ S(c)\end{array}\end{array}}\ \beta_\lor}\ \gamma_\forall + \alpha_\land$$

Motivating Example — A Better Heuristic

$$\begin{array}{c}
\neg P(a)\\
\neg Q(b)\\
\neg S(c)\\
\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{P(c) \lor Q(c)}\ \gamma_\forall + \alpha_\land \\
\dfrac{\forall y.\ S(c)}{P(c) \qquad\qquad\qquad Q(c)}\ \beta_\lor \\
\dfrac{\dfrac{\forall y.\ S(c)}{S(c)}\ \gamma_\forall}{\sigma = \{X \mapsto c\}}\ \odot_\sigma \qquad\qquad \dfrac{\forall y.\ S(c)}{S(c)}\ \gamma_\forall
\end{array}$$

Motivating Example — A Better Heuristic

$$\begin{array}{c}
\neg P(a)\\
\neg Q(b)\\
\neg S(c)\\
\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{P(c) \lor Q(c)}\;\gamma_\forall + \alpha_\land\\
\dfrac{\forall y.\ S(c)}{\begin{array}{cc}
\begin{array}{c} P(c)\\ \dfrac{\dfrac{\forall y.\ S(c)}{S(c)}\;\gamma_\forall}{\sigma = \{X \mapsto c\}}\;\odot_\sigma \end{array} &
\begin{array}{c} Q(c)\\ \dfrac{\dfrac{\forall y.\ S(c)}{S(c)}\;\gamma_\forall}{\odot}\;\odot_\sigma \end{array}
\end{array}}\;\beta_\lor
\end{array}$$

Exploring Branches in Parallel?

Approach

- Each branch searches for a local solution
- Management of multiple solutions with successive attempts and backtracking
- Forbid previously tried solutions
- Iterative deepening, limit of γ-rule and rules ordering

Exploring Branches in Parallel?

Approach

- Each branch searches for a local solution
- Management of multiple solutions with successive attempts and backtracking
- Forbid previously tried solutions
- Iterative deepening, limit of γ-rule and rules ordering

New Challenges

- Free variable dependency
- Communication between branches

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))$$

Solving Fairness Issues with Concurrency

$$\cfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \vee Q(x)) \wedge \forall y.\ S(x))\end{array}}{\begin{array}{c}P(X) \vee Q(X)\\ \forall y.\ S(X)\end{array}}\ \gamma_{\forall} + \alpha_{\wedge}$$

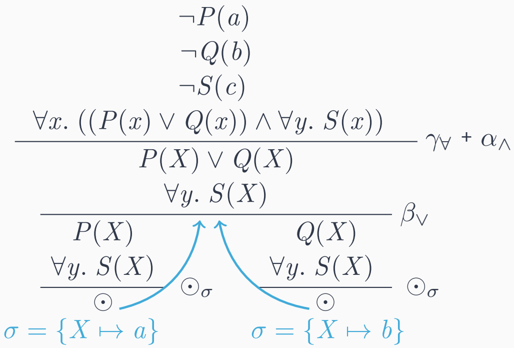
Solving Fairness Issues with Concurrency

$$\begin{array}{cl}
\neg P(a) & \\
\neg Q(b) & \\
\neg S(c) & \\
\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x)) & \gamma_{\forall} + \alpha_{\land} \\ \cline{1-1}
P(X) \lor Q(X) & \\
\forall y.\ S(X) & \beta_{\lor} \\ \cline{1-1}
\begin{array}{cc} P(X) & Q(X) \\ \forall y.\ S(X) & \forall y.\ S(X) \end{array} &
\end{array}$$

Solving Fairness Issues with Concurrency

$$
\begin{array}{c}
\neg P(a) \\
\neg Q(b) \\
\neg S(c) \\
\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{P(X) \lor Q(X)}\ \gamma_{\forall} + \alpha_{\land} \\
\dfrac{\forall y.\ S(X)}{\begin{array}{cc}
P(X) & Q(X) \\
\dfrac{\forall y.\ S(X)}{\odot}\ \odot_{\sigma} & \dfrac{\forall y.\ S(X)}{\odot}\ \odot_{\sigma} \\
\sigma = \{X \mapsto a\} & \sigma = \{X \mapsto b\}
\end{array}}\ \beta_{\lor}
\end{array}
$$

Solving Fairness Issues with Concurrency



$\neg P(a)$

$\neg Q(b)$

$\neg S(c)$

$\forall x.\ ((P(x) \vee Q(x)) \wedge \forall y.\ S(x))$ — $\gamma_\forall$ + $\alpha_\wedge$

$P(X) \vee Q(X)$

$\forall y.\ S(X)$ — $\beta_\vee$

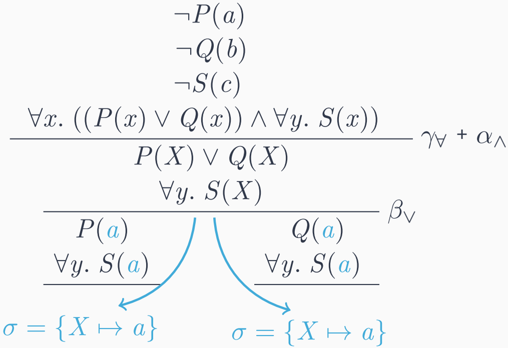
$P(X)$ | $Q(X)$

$\forall y.\ S(X)$ | $\forall y.\ S(X)$

$\odot$ — $\odot_\sigma$ | $\odot$ — $\odot_\sigma$

$\sigma = \{X \mapsto a\}$ | $\sigma = \{X \mapsto b\}$

Solving Fairness Issues with Concurrency



$$\neg P(a)$$

$$\neg Q(b)$$

$$\neg S(c)$$

$$\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))$$

$$\gamma_\forall + \alpha_\land$$

$$P(X) \lor Q(X)$$

$$\forall y.\ S(X)$$

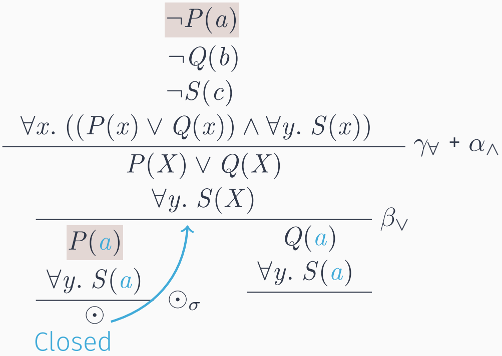
$$\beta_\lor$$

$$P(a) \qquad Q(a)$$

$$\forall y.\ S(a) \qquad \forall y.\ S(a)$$

$$\sigma = \{X \mapsto a\} \qquad \sigma = \{X \mapsto a\}$$

Solving Fairness Issues with Concurrency



$\neg P(a)$

$\neg Q(b)$

$\neg S(c)$

$\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))$

$\gamma_\forall + \alpha_\land$

$P(X) \lor Q(X)$

$\forall y.\ S(X)$

$\beta_\lor$

$P(a)$

$\forall y.\ S(a)$

$\odot$

$\odot_\sigma$

Closed

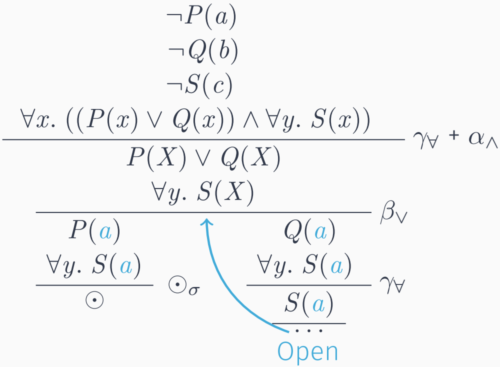
$Q(a)$

$\forall y.\ S(a)$

Solving Fairness Issues with Concurrency

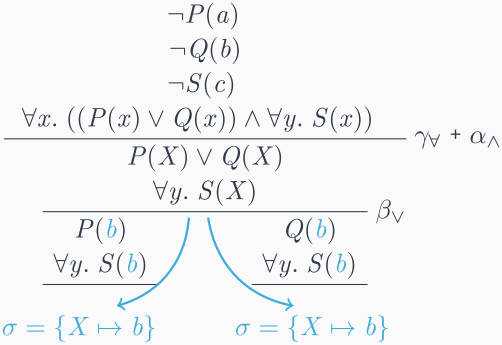
$$
\begin{array}{c}
\neg P(a) \\
\neg Q(b) \\
\neg S(c) \\
\dfrac{\forall x.\ ((P(x) \vee Q(x)) \wedge \forall y.\ S(x))}{\begin{array}{c} P(X) \vee Q(X) \\ \dfrac{\forall y.\ S(X)}{\begin{array}{cc} \begin{array}{c} P(a) \\ \dfrac{\forall y.\ S(a)}{\odot}\ \odot_{\sigma} \end{array} & \begin{array}{c} Q(a) \\ \dfrac{\forall y.\ S(a)}{S(a)}\ \gamma_{\forall} \end{array} \end{array}}\ \beta_{\vee} \end{array}}\ \gamma_{\forall} + \alpha_{\wedge}
\end{array}
$$

Solving Fairness Issues with Concurrency



$$\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))\end{array}}{\dfrac{\begin{array}{c}P(X) \lor Q(X)\\ \forall y.\ S(X)\end{array}}{\dfrac{\begin{array}{c}P(a)\\ \forall y.\ S(a)\end{array}}{\odot}\ \odot_{\sigma} \qquad \dfrac{\begin{array}{c}Q(a)\\ \forall y.\ S(a)\end{array}}{\dfrac{S(a)}{\cdots}}\ \gamma_{\forall}}\ \beta_{\lor}}\ \gamma_{\forall} + \alpha_{\land}$$

Solving Fairness Issues with Concurrency



$$\neg P(a)$$

$$\neg Q(b)$$

$$\neg S(c)$$

$$\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))$$

$\gamma_\forall$ + $\alpha_\land$

$$P(X) \lor Q(X)$$

$$\forall y.\ S(X)$$

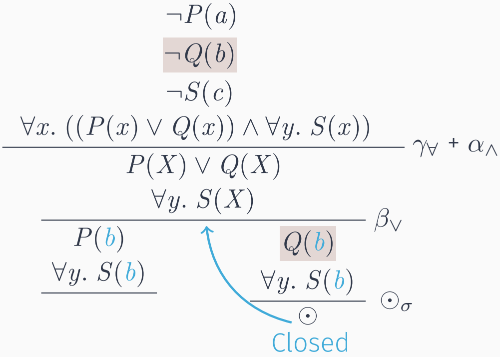
$\beta_\lor$

$$P(b) \qquad Q(b)$$

$$\forall y.\ S(b) \qquad \forall y.\ S(b)$$

$$\sigma = \{X \mapsto b\} \qquad \sigma = \{X \mapsto b\}$$

Solving Fairness Issues with Concurrency



$\neg P(a)$

$\neg Q(b)$

$\neg S(c)$

$\forall x. ((P(x) \lor Q(x)) \land \forall y. S(x))$

$\gamma_\forall$ + $\alpha_\land$

$P(X) \lor Q(X)$

$\forall y. S(X)$

$\beta_\lor$

$P(b)$

$\forall y. S(b)$

$Q(b)$

$\forall y. S(b)$

$\odot_\sigma$

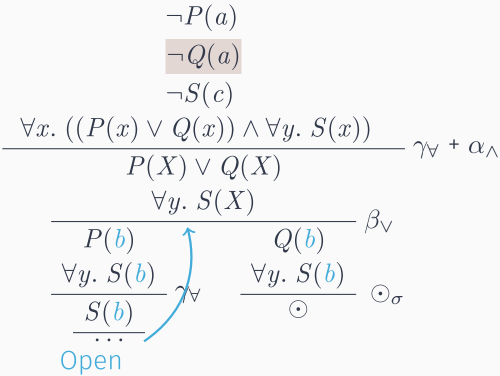
$\odot$

Closed

Solving Fairness Issues with Concurrency

$$\dfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x)\lor Q(x))\land\forall y.\ S(x))\end{array}}{\begin{array}{c}P(X)\lor Q(X)\\ \dfrac{\forall y.\ S(X)}{\begin{array}{cc}P(b) & Q(b)\\ \dfrac{\forall y.\ S(b)}{S(b)}\ \gamma_\forall & \dfrac{\forall y.\ S(b)}{\odot}\ \odot_\sigma\end{array}}\ \beta_\lor\end{array}}\ \gamma_\forall + \alpha_\land$$

Solving Fairness Issues with Concurrency



$$\neg P(a)$$

$$\neg Q(a)$$

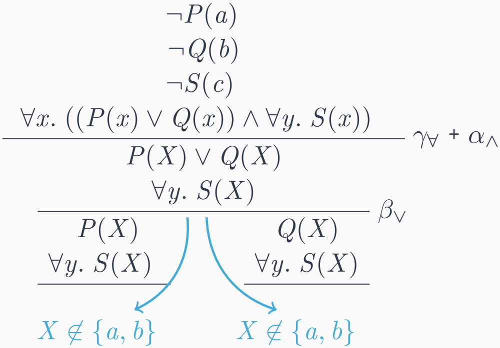
$$\neg S(c)$$

$$\cfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{\begin{array}{c} P(X) \lor Q(X) \\ \forall y.\ S(X) \end{array}}\ \gamma_{\forall} + \alpha_{\land}$$

$$\cfrac{}{\begin{array}{c} P(b) \\ \cfrac{\forall y.\ S(b)}{\cfrac{S(b)}{\cdots}}\ \gamma_{\forall} \end{array} \qquad \begin{array}{c} Q(b) \\ \cfrac{\forall y.\ S(b)}{\odot}\ \odot_{\sigma} \end{array}}\ \beta_{\lor}$$

Open

Solving Fairness Issues with Concurrency



$$\neg P(a)$$

$$\neg Q(b)$$

$$\neg S(c)$$

$$\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{\begin{array}{c} P(X) \lor Q(X) \\ \forall y.\ S(X) \end{array}}\ \gamma_{\forall} + \alpha_{\land}$$

$$\dfrac{}{\begin{array}{c} P(X) \\ \forall y.\ S(X) \end{array} \qquad \begin{array}{c} Q(X) \\ \forall y.\ S(X) \end{array}}\ \beta_{\lor}$$

$$X \notin \{a, b\} \qquad X \notin \{a, b\}$$

Solving Fairness Issues with Concurrency

$$\neg P(a)$$

$$\neg Q(b)$$

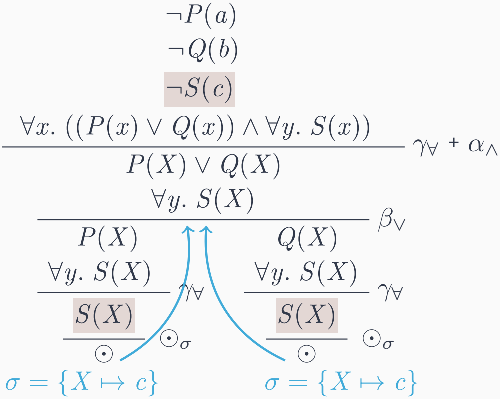
$$\neg S(c)$$

$$\dfrac{\forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))}{P(X) \lor Q(X)}\ \gamma_\forall + \alpha_\land$$

$$\dfrac{\forall y.\ S(X)}{P(X) \qquad\qquad\qquad Q(X)}\ \beta_\lor$$

$$\dfrac{\forall y.\ S(X)}{S(X)}\ \gamma_\forall \qquad \dfrac{\forall y.\ S(X)}{S(X)}\ \gamma_\forall$$

Solving Fairness Issues with Concurrency



$$\neg P(a)$$

$$\neg Q(b)$$

$$\neg S(c)$$

$$\dfrac{\forall x.\ ((P(x) \vee Q(x)) \wedge \forall y.\ S(x))}{\begin{array}{c} P(X) \vee Q(X) \\ \forall y.\ S(X) \end{array}} \ \gamma_{\forall} + \alpha_{\wedge}$$

$$\beta_{\vee}$$

$$\begin{array}{c} P(X) \\ \dfrac{\forall y.\ S(X)}{\dfrac{S(X)}{\odot} \ \odot_{\sigma}} \ \gamma_{\forall} \end{array} \qquad \begin{array}{c} Q(X) \\ \dfrac{\forall y.\ S(X)}{\dfrac{S(X)}{\odot} \ \odot_{\sigma}} \ \gamma_{\forall} \end{array}$$

$$\sigma = \{X \mapsto c\} \qquad \sigma = \{X \mapsto c\}$$

Solving Fairness Issues with Concurrency

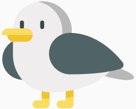
$$\cfrac{\begin{array}{c}\neg P(a)\\ \neg Q(b)\\ \neg S(c)\\ \forall x.\ ((P(x) \lor Q(x)) \land \forall y.\ S(x))\end{array}}{\cfrac{\begin{array}{c}P(c) \lor Q(c)\\ \forall y.\ S(c)\end{array}}{\begin{array}{cc} \begin{array}{c} P(c)\\ \cfrac{\forall y.\ S(c)}{\cfrac{S(c)}{\odot}\;\odot_\sigma}\;\gamma_\forall \\ \sigma = \{X \mapsto c\}\end{array} & \begin{array}{c} Q(c)\\ \cfrac{\forall y.\ S(c)}{\cfrac{S(c)}{\odot}\;\odot_\sigma}\;\gamma_\forall \\ \sigma = \{X \mapsto c\}\end{array}\end{array}}\;\beta_\lor}\;\gamma_\forall + \alpha_\land$$

Contributions

- A tableau-based proof-search procedure
- Concurrent exploration of branches
- Tackle fairness challenges
- Eager closure
- Backtrack and forbidden substitutions
- Completeness proof of the procedure
- Implemented into a tool: `Goéland`

3. The **Goéland** Automated Theorem Prover

The `Goéland` Tool



Proof-Search Procedure

- Concurrent proof-search procedure
- Eager closure
- Completeness proof

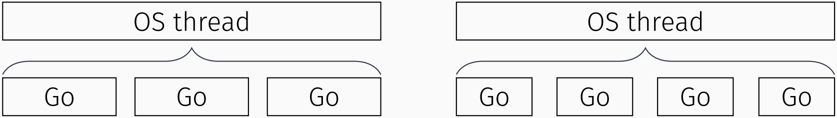
Additional Functionnalities

- Equality reasoning
- Deduction modulo theory
- Polymorphic types
- Alternative modes: incomplete, interactive, shared memory, ...
- Outputs: `Rocq`, `LambdaPi`, `Lisa` and `SC-TPTP`

The Goéland Tool

Implementation

- 40 000 lines of code
- Go programming language
- Designed for concurrency
- Goroutines: N:M lightweight threads



Theory Reasoning

Motivation and Challenges

- Reason within specific contexts (arithmetic, industrial problems, ...)
- Deal with a large number of axioms
- Handle multiple theories

Background Reasoners

- Equality
- Deduction modulo theory (DMT)

Deduction Modulo Theory

Principle

- Turns axioms into rewrite rules
- Triggers only relevant axioms
- Produces shorter proof
- Not limited to one theory

Main Heuristic

$(\forall \vec{x}.)\ A \Leftrightarrow F$ where:

- A is an atomic formula
- F is a non-atomic formula

Polarized DMT

$(\forall \vec{x}.)\ A \Rightarrow F$ where:

- A is an atomic formula
- F is a non-atomic formula

Axiom: $\forall x.\ P(x) \Leftrightarrow \forall y.\ Q(x, y) \land S(x, y)$

Rule: $P(X) \rightarrow \forall y.\ Q(X, y) \land S(X, y)$

Protocol of the Experiments

- Thousand of Problems for Theorem Provers (TPTP) library (v8.1.2)
- Syntactic (SYN) and set theory (SET) categories
- First-order logic (FOL)
- `Goéland` and its variants, `Zenon` (+ modulo), `Princess`, `Vampire` and `E`
- 300 seconds of timeout
- Intel Xeon E5-2680 v4 2.4GHz 2×14-core processor with 128GB

`Goéland` Variants over SYN and SET

	SYN (288 problems)		SET (464 problems)	
`Goéland`	**209**	(1.2 s)	**124**	(18.6 s)
`Goéland+EQ`	**213**	(0.3 s)	**101**	(15.6 s)
`Goéland+DMT`	**209**	(1.3 s)	**217**	(5.9 s)
`Goéland+DMT+EQ`	**213**	(0.5 s)	**192**	(10.2 s)
`Goéland+DMT` +Polarized	**202**	(0.3 s)	**164**	(1.5 s)

All Provers on FOF

	FOF (5396 problems)
`Goéland`	**613** (10 482 s — 17.1 s)
`Goéland+DMT`	**770** (6 935 s — 9 s)
`Goéland+DMT+EQ`	**801** (10 060 s — 12.5 s)
`Zenon`	**1 382** (9 026 s — 6.5 s)
`Zenon Modulo`	**1 389** (10 028 s — 7.2 s)
`Princess`	**1 621** (23 200 s — 14.3 s)
`Vampire`	**3 342** (42 873 s — 12.8 s)
`E`	**3 939** (39 638 s — 10.1 s)

Analysis

Promising Results and Features

- Deduction modulo theory
- Output proofs

Performances Issues

- Less problems solved than other ATP
- Memory management
- Equality reasoner
- Proof size

4. Production of Proof Certificate

Skolemization

Skolemization

- δ-rule
- $\exists$ and $\neg\forall$
- Introduces a *fresh* Skolem symbol
- The symbol is parametrized by the free variables of the branch

$$\exists z.\ P(z)$$

Skolemization

Skolemization

- δ-rule
- $\exists$ and $\neg\forall$
- Introduces a *fresh* Skolem symbol
- The symbol is parametrized by the free variables of the branch

$$\frac{\exists z.\ P(z)}{P(c)}\ \delta_{\exists}$$

Skolemization

Skolemization

- δ-rule
- $\exists$ and $\neg\forall$
- Introduces a *fresh* Skolem symbol
- The symbol is parametrized by the free variables of the branch

$$\begin{array}{c} \cdots \\ Q(X, Y) \\ \exists z.P(z) \end{array}$$

Skolemization

Skolemization

- δ-rule
- $\exists$ and $\neg\forall$
- Introduces a *fresh* Skolem symbol
- The symbol is parametrized by the free variables of the branch

$$\dfrac{\begin{array}{c}\vdots \\ Q(X, Y) \\ \exists z. P(z)\end{array}}{P(sko(X, Y))}\ \delta_{\exists}$$

Advanced Skolemization Strategies

Motivations

- Shorter proofs
- Faster proof search

Inner Skolemization (δ^+-rule)

- Extension of δ-rule
- Uses only the free variables of the formula
- Extensions: δ^{+^+}, δ^*, ...

$$\begin{array}{c} \dots \\ Q(X, Y) \\ \exists z.\ P(z) \end{array}$$

Advanced Skolemization Strategies

Motivations

- Shorter proofs
- Faster proof search

Inner Skolemization (δ^+-rule)

- Extension of δ-rule
- Uses only the free variables of the formula
- Extensions: δ^{+^+}, δ^*, ...

$$\frac{\begin{array}{c}\dots\\ Q(X, Y)\\ \exists z.\ P(z)\end{array}}{P(c)}\ \delta^+_\exists$$

Advanced Skolemization Strategies

Motivations

- Shorter proofs
- Faster proof search

Inner Skolemization (δ^+-rule)

- Extension of δ-rule
- Uses only the free variables of the formula
- Extensions: δ^{+^+}, δ^*, ...

$$\begin{array}{c} \ldots \\ Q(X, Y) \\ \exists z.\ P(z, X) \end{array}$$

Advanced Skolemization Strategies

Motivations

- Shorter proofs
- Faster proof search

Inner Skolemization (δ^{+}-rule)

- Extension of δ-rule
- Uses only the free variables of the formula
- Extensions: $\delta^{+^{+}}$, δ^{*}, ...

$$\frac{\begin{array}{c}\dots\\ Q(X,Y)\\ \exists z.\ P(z,X)\end{array}}{P(sko(X))}\ \delta^{+}_{\exists}$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(f(X)) & \delta_{\neg\forall} \\ \hline
\neg(D(X_2) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X_2), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\sigma = \{X_2 \mapsto f(X)\} & \odot_\sigma
\end{array}$$

(a) Outer Skolemization tableau.

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(c) & \delta^{+}_{\neg\forall} \\ \hline
\sigma = \{X \mapsto c\} & \odot_\sigma
\end{array}$$

(b) Inner Skolemization tableau.

Translation to Machine-Checkable Proofs

Gentzen-Schütte Calculus (GS3)

- Equivalent to tableaux: 1-to-1 mapping between rules
- Easily translatable to proof assistants
- No free variables

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(f(X)) & \delta_{\neg\forall} \\ \hline
\neg(D(X_2) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X_2), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\sigma = \{X_2 \mapsto f(X)\} & \odot_\sigma
\end{array}$$

(a) Outer Skolemization tableau proof.

$$\begin{array}{cl}
 & \\ \hline
\ldots, \neg D(c'), D(c'), \neg(\forall y\ D(y)) \vdash & \mathsf{ax} \\ \hline
\ldots, \neg(D(c') \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \ldots, \neg D(c') \vdash & \neg\exists \\ \hline
\ldots, D(c), \neg(\forall y\ D(y)) \vdash & \neg\forall \\ \hline
\ldots, \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) \vdash & \neg\exists
\end{array}$$

(b) Equivalent GS3.

Outer Skolemization Only ☹

Why?

- δ-rule: the symbol has to be *fresh*
- γ-rule: must be instantiated by its final value
- Closure rule: unification with *any* term
- Problem: we use a term *before* its introduction

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(c) & \delta^{+}_{\neg\forall} \\ \hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

(a) Inner Skolemization tableau proof.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\ldots, D(c), \neg(\forall y\ D(y)), \neg D(c) \vdash}\ \text{ax}}{\ldots, D(c), \neg(\forall y\ D(y)) \vdash}\ \neg\forall\ (\star)}{\ldots, \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash}\ \neg\Rightarrow}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) \vdash}\ \neg\exists$$

(b) Incorrect equivalent `GS3`.

A Deskolemization Strategy

Idea

Perform all the Skolemization steps before the other rules, so the Skolem symbol is necessarily fresh.

Key Notion

- Formulas that *depend* on a Skolem symbol
- A formula F needs to be processed before another formula G iff G makes use of a Skolem symbol generated by F

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\
\cline{1-1}
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\
\cline{1-1}
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\
\cline{1-1}
\neg D(c) & \delta^{+}_{\neg\forall} \\
\cline{1-1}
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\
\hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\
\hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\
\hline
\neg D(c) & \delta^{+}_{\neg\forall} \\
\hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

$$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) \vdash$$

Example

$$\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}{\dfrac{\neg(D(X) \Rightarrow \forall y\ D(y))}{\dfrac{D(X), \neg(\forall y\ D(y))}{\dfrac{\neg D(c)}{\sigma = \{X \mapsto c\}}\ \odot_{\sigma}}\ \delta^{+}_{\neg\forall}}\ \alpha_{\neg\Rightarrow}}\ \gamma_{\neg\exists}$$

$$\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y))}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\ \neg\exists$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}{\neg(D(X) \Rightarrow \forall y\ D(y))}\ \gamma_{\neg\exists}}{D(X), \neg(\forall y\ D(y))}\ \alpha_{\neg\Rightarrow}}{\neg D(c)}\ \delta^{+}_{\neg\forall}}{\sigma = \{X \mapsto c\}}\ \odot_{\sigma}$$

$$\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y))}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\ \neg\exists$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}{\neg(D(X) \Rightarrow \forall y\ D(y))}\ \gamma_{\neg\exists}}{D(X), \neg(\forall y\ D(y))}\ \alpha_{\neg\Rightarrow}}{\neg D(c)}\ \delta^{+}_{\neg\forall}}{\sigma = \{X \mapsto c\}}\ \odot_{\sigma}$$

$$\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash}\ \neg\Rightarrow}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\ \neg\exists$$

Example

$$\begin{prooftree}
\AxiomC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))$}
\RightLabel{$\gamma_{\neg\exists}$}
\UnaryInfC{$\neg(D(X) \Rightarrow \forall y\ D(y))$}
\RightLabel{$\alpha_{\neg\Rightarrow}$}
\UnaryInfC{$D(X), \neg(\forall y\ D(y))$}
\RightLabel{$\delta^{+}_{\neg\forall}$}
\UnaryInfC{$\neg D(c)$}
\RightLabel{$\odot_{\sigma}$}
\UnaryInfC{$\sigma = \{X \mapsto c\}$}
\end{prooftree}$$

$$\begin{prooftree}
\AxiomC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash$}
\RightLabel{$\neg\Rightarrow$}
\UnaryInfC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash$}
\RightLabel{$\neg\exists$}
\UnaryInfC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))$}
\end{prooftree}$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}{\neg(D(X) \Rightarrow \forall y\ D(y))}\,\gamma_{\neg\exists}}{D(X), \neg(\forall y\ D(y))}\,\alpha_{\neg\Rightarrow}}{\neg D(c)}\,\delta^{+}_{\neg\forall}}{\sigma = \{X \mapsto c\}}\,\odot_{\sigma}$$

$$\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash}\,\neg\Rightarrow}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\,\neg\exists$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(c) & \delta^{+}_{\neg\forall} \\ \hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash & \\ \hline\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash & \mathrm{W} \times 2 \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \neg\exists
\end{array}$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}{\neg(D(X) \Rightarrow \forall y\ D(y))}\ \gamma_{\neg\exists}}{D(X), \neg(\forall y\ D(y))}\ \alpha_{\neg\Rightarrow}}{\neg D(c)}\ \delta^{+}_{\neg\forall}}{\sigma = \{X \mapsto c\}}\ \odot_{\sigma}$$

$$\dfrac{\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash}\ \mathsf{W} \times 2}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash}\ \neg\Rightarrow}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\ \neg\exists$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}{\neg(D(X) \Rightarrow \forall y\ D(y))}\,\gamma_{\neg\exists}}{D(X), \neg(\forall y\ D(y))}\,\alpha_{\neg\Rightarrow}}{\neg D(c)}\,\delta^{+}_{\neg\forall}}{\sigma = \{X \mapsto c\}}\,\odot_{\sigma}$$

$$\dfrac{\dfrac{\begin{array}{c}\dfrac{}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash}\,\neg\forall \\ \hline\hline \neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash\end{array}\,\mathsf{W} \times 2}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash}\,\neg\Rightarrow}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\,\neg\exists$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(c) & \delta^{+}_{\neg\forall} \\ \hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash & \neg\forall \\ \hline\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash & \mathsf{W} \times 2 \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \neg\exists
\end{array}$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(c) & \delta^{+}_{\neg\forall} \\ \hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash & \neg\forall \\ \hline\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash & \mathsf{W} \times 2 \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \neg\exists
\end{array}$$

Example

$$\begin{prooftree}
\AxiomC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))$}
\RightLabel{$\gamma_{\neg\exists}$}
\UnaryInfC{$\neg(D(X) \Rightarrow \forall y\ D(y))$}
\RightLabel{$\alpha_{\neg\Rightarrow}$}
\UnaryInfC{$D(X), \neg(\forall y\ D(y))$}
\RightLabel{$\delta^{+}_{\neg\forall}$}
\UnaryInfC{$\neg D(c)$}
\RightLabel{$\odot_{\sigma}$}
\UnaryInfC{$\sigma = \{X \mapsto c\}$}
\end{prooftree}$$

$$\begin{prooftree}
\AxiomC{}
\RightLabel{$\neg\exists$}
\UnaryInfC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash$}
\RightLabel{$\neg\forall$}
\UnaryInfC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash$}
\doubleLine
\RightLabel{$\mathsf{W} \times 2$}
\UnaryInfC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash$}
\RightLabel{$\neg\Rightarrow$}
\UnaryInfC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash$}
\RightLabel{$\neg\exists$}
\UnaryInfC{$\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))$}
\end{prooftree}$$

Example

$$
\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \cline{1-1}
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \cline{1-1}
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \cline{1-1}
\neg D(c) & \delta^{+}_{\neg\forall} \\ \cline{1-1}
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}
$$

$$
\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \\ \cline{1-1}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \neg\exists \\ \cline{1-1}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash & \neg\forall \\ \hline\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash & \mathrm{W} \times 2 \\ \cline{1-1}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \cline{1-1}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \neg\exists
\end{array}
$$

Example

$$\cfrac{\cfrac{\cfrac{\cfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}{\neg(D(X) \Rightarrow \forall y\ D(y))}\,\gamma_{\neg\exists}}{D(X), \neg(\forall y\ D(y))}\,\alpha_{\neg\Rightarrow}}{\neg D(c)}\,\delta^{+}_{\neg\forall}}{\sigma = \{X \mapsto c\}}\,\odot_{\sigma}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash}\,\neg\exists}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash}\,\neg\forall}{\overline{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash}}\,\mathsf{W} \times 2}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash}\,\neg\Rightarrow}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\,\neg\exists$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(c) & \delta^{+}_{\neg\forall} \\ \hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

$$\begin{array}{cl}
 & \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \neg\exists \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash & \neg\forall \\ \hline\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash & \mathrm{W} \times 2 \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \neg\exists
\end{array}$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\ \hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\ \hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\ \hline
\neg D(c) & \delta^{+}_{\neg\forall} \\ \hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)), \neg D(c) \vdash & \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \neg\exists \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash & \neg\forall \\ \hline\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash & \mathsf{W} \times 2 \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\ \hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \neg\exists
\end{array}$$

Example

$$\begin{array}{cl}
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \\
\hline
\neg(D(X) \Rightarrow \forall y\ D(y)) & \gamma_{\neg\exists} \\
\hline
D(X), \neg(\forall y\ D(y)) & \alpha_{\neg\Rightarrow} \\
\hline
\neg D(c) & \delta^{+}_{\neg\forall} \\
\hline
\sigma = \{X \mapsto c\} & \odot_{\sigma}
\end{array}$$

$$\begin{array}{cl}
\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)), \neg D(c) \vdash & \mathsf{ax} \\
\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \neg\Rightarrow \\
\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash & \neg\exists \\
\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash & \neg\forall \\
\hline\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash & \mathsf{W} \times 2 \\
\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash & \neg\Rightarrow \\
\hline
\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)) & \neg\exists
\end{array}$$

Experiments

Implementation

- δ, δ^{+} and $\delta^{+^{+}}$ Skolemization strategies
- `GS3` proofs
- Deskolemization algorithms

Evaluation Protocol

- Same setup as previous tests
- 3 Skolemization strategies + DMT
- Number of problems solved
- `Rocq` output
- Size of the proof (number of branches)

Results

	Problems Proved	Percentage Certified	Avg. Size Increase	Max. Size Increase
`Goéland`	261	100 %	0 %	-
`Goéland`+δ^{+}	272	100 %	8.1 %	5.3
`Goéland`+$\delta^{+^{+}}$	274	100 %	10.6 %	10.3
`Goéland+DMT`	363	100 %	0 %	-
`Goéland+DMT`+δ^{+}	375	100 %	4.5 %	3.9
`Goéland+DMT`+$\delta^{+^{+}}$	377	100 %	7.4 %	5.2

Contributions

- An optimization of the deskolemization algorithm for δ^{+}
- A deskolemization algorithm for $\delta^{+^{+}}$
- Soundness proof for both translations
- Output of GS3 proof into `Rocq`, `LambdaPi`, `Lisa` and `SC-TPTP`
- Promising results
- 100% of the proofs are certified
- Far below the theoretical bound

Conclusion

Contributions

`Goéland`

- Fairness between branches managed by concurrency
- Completeness of the procedure
- Promising results (DMT)

Proof Certification

- A sound generic deskolemization algorithm
- Output of the proofs into `Rocq`, `LambdaPi`, `Lisa` and `SC-TPTP`

Future Work

`Goéland`

- Performance improvement (memory management, equality, Rust, …)
- Heuristics, simulate "intuition" with learning methods, …
- Modular and generic prover
- Non-classical logic & theories

Proof Certification

- Reduce the number of branches by the use of lemmas
- Integration of theories
- `SC-TPTP Utils` and proof elaboration
- Framework for verification of tableau proofs: `TableauxRocq`

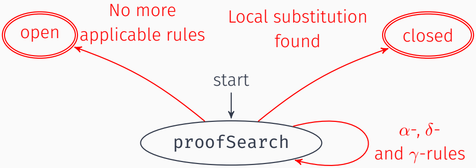
Thank you! ☺

`https://github.com/GoelandProver/Goeland`

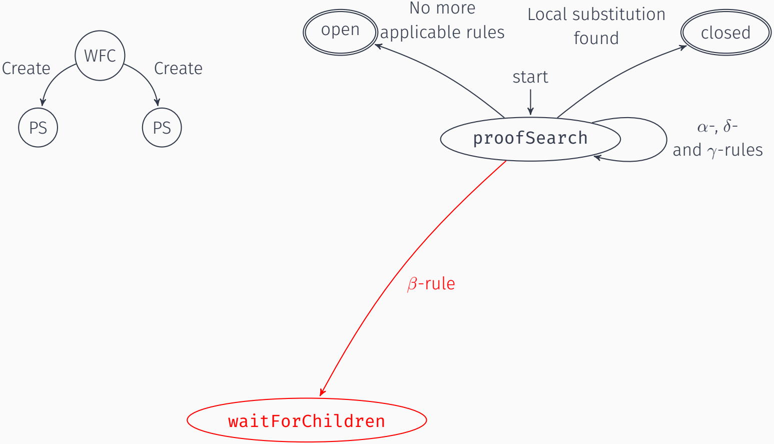
`https://github.com/SC-TPTP/sc-tptp`

Procedures Interactions

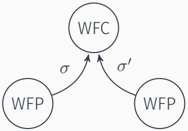
Procedures Interactions

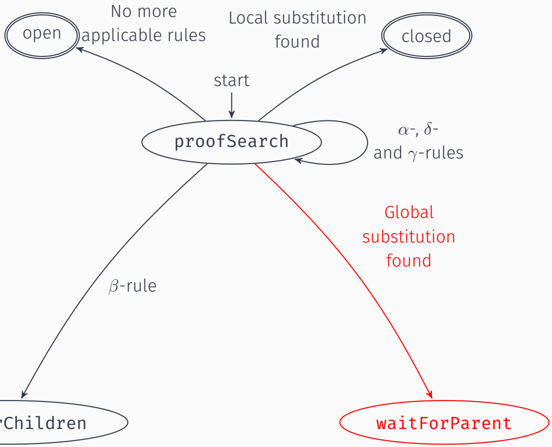


Procedures Interactions

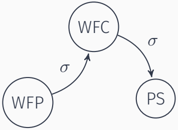


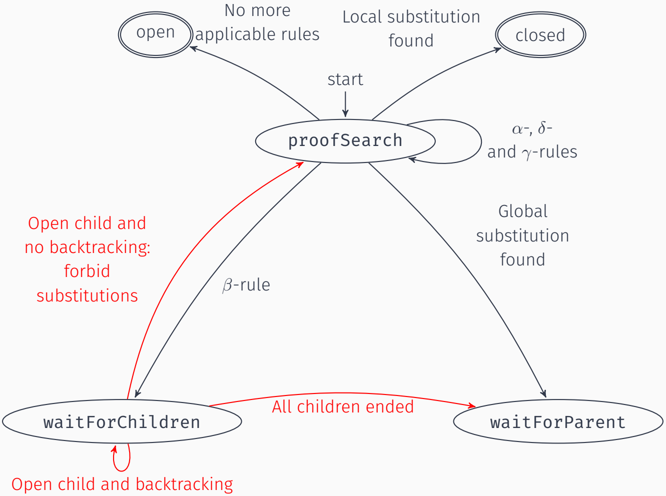
Procedures Interactions



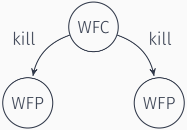


Procedures Interactions





Procedures Interactions



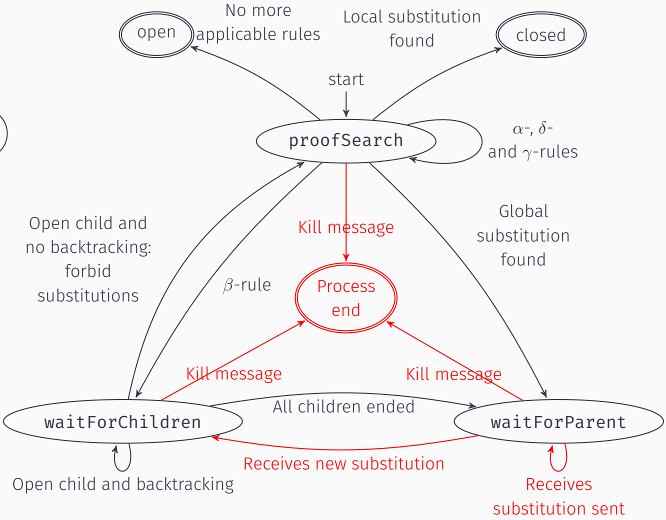
WFC

kill

kill

WFP

WFP



open

No more applicable rules

start

Local substitution found

closed

proofSearch

α-, δ- and γ-rules

Open child and no backtracking: forbid substitutions

β-rule

Kill message

Process end

Global substitution found

Kill message

Kill message

waitForChildren

All children ended

waitForParent

Receives new substitution

Open child and backtracking

Receives substitution sent

Reasoning Modulo Theory

Simple Set Theory

- A_1: $\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b$
- A_2: $\forall a, b.\ a = b \Leftrightarrow a \subseteq b \land b \subseteq a$
- C: $\forall a.\ a \subseteq a$

$$A_1 \land A_2 \land \neg C$$

$$\begin{aligned}&(\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b)\\ \land\ &(\forall a, b.\ a = b \Leftrightarrow a \subseteq b \land b \subseteq a)\\ \land\ &\neg(\forall a.\ a \subseteq a)\end{aligned}$$

Reasoning Modulo Theory

$$\dfrac{\begin{array}{c}(\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b) \land (\forall a, b.\ a = b \Leftrightarrow a \subseteq b \land b \subseteq a)\\ \land \neg(\forall a.\ a \subseteq a)\end{array}}{\dfrac{\begin{array}{c}\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b, \forall a, b.\ a = b \Leftrightarrow a \subseteq b \land b \subseteq a,\\ \neg(\forall a.\ a \subseteq a)\end{array}}{\dfrac{\dfrac{\dfrac{\neg(a \subseteq a)}{\forall b.\ A \subseteq b \Leftrightarrow \forall x.\ x \in A \Rightarrow x \in b}\,\gamma_{\forall}}{A \subseteq B \Leftrightarrow \forall x.\ x \in A \Rightarrow x \in B}\,\gamma_{\forall}}{\dfrac{A \subseteq B, x \in A \Rightarrow x \in B}{\sigma = \{A \mapsto a, B \mapsto a\}}\,\odot_{\sigma} \qquad \dfrac{\neg(A \subseteq B), \neg(\forall x.\ x \in A \Rightarrow x \in B)}{\dfrac{\neg(a \subseteq a), \neg(\forall x.\ x \in a \Rightarrow x \in a)}{\dfrac{\neg(s \in a \Rightarrow s \in a)}{\dfrac{\neg(s \in a), (s \in a)}{\odot}\,\odot}\,\alpha_{\neg\Rightarrow}}\,\delta_{\neg\forall}}\,\sigma}\,\beta_{\Leftrightarrow}}\,\delta_{\neg\forall}}\,\alpha_{\land}$$

Reasoning Modulo Theory

$$\dfrac{\begin{array}{c}(\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b) \land (\forall a, b.\ a = b \Leftrightarrow a \subseteq b \land b \subseteq a) \\ \land \neg(\forall a.\ a \subseteq a)\end{array}}{\begin{array}{c}\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b, \forall a, b.\ a = b \Leftrightarrow a \subseteq b \land b \subseteq a, \\ \neg(\forall a.\ a \subseteq a)\end{array}}\ \alpha_{\land}$$

$$\dfrac{}{\neg(a \subseteq a)}\ \delta_{\neg\forall}$$

$$\dfrac{}{\forall b.\ A \subseteq b \Leftrightarrow \forall x.\ x \in A \Rightarrow x \in b}\ \gamma_{\forall}$$

$$\dfrac{}{A \subseteq B \Leftrightarrow \forall x.\ x \in A \Rightarrow x \in B}\ \gamma_{\forall}$$

$$\dfrac{}{\dfrac{A \subseteq B, x \in A \Rightarrow x \in B}{\sigma = \{A \mapsto a, B \mapsto a\}}\ \odot_{\sigma} \qquad \dfrac{\neg(A \subseteq B), \neg(\forall x.\ x \in A \Rightarrow x \in B)}{\dfrac{\neg(a \subseteq a), \neg(\forall x.\ x \in a \Rightarrow x \in a)}{\dfrac{\neg(s \in a \Rightarrow s \in a)}{\dfrac{\neg(s \in a), (s \in a)}{\odot}\ \odot}\ \alpha_{\neg\Rightarrow}}\ \delta_{\neg\forall}}\ \sigma}\ \beta_{\Leftrightarrow}$$

Deduction Modulo Theory (DMT)

Principle

Turns axioms into rewrite rules

Main Heuristic

$(\forall \vec{x}.)\ A \Leftrightarrow F$ where:

- A is an atomic formula
- F is a non-atomic formula

Axiom: $\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b$
Rule: $A \subseteq B \rightarrow \forall x.\ x \in A \Rightarrow x \in B$

Axiom: $\forall a, b.\ a = b \Leftrightarrow a \subseteq b \wedge b \subseteq a$
Rule: $A = B \rightarrow A \subseteq B \wedge B \subseteq A$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \rightarrow \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \rightarrow A \subseteq B \land B \subseteq A$$

$$\neg(\forall a.\ a \subseteq a)$$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \to \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \to A \subseteq B \land B \subseteq A$$

$$\frac{\neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\, \delta_{\neg\forall}$$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \to \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \to A \subseteq B \land B \subseteq A$$

$$\frac{\neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\ \delta_{\neg\forall}$$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \to \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \to A \subseteq B \wedge B \subseteq A$$

$$\cfrac{\cfrac{\neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\ \delta_{\neg\forall}}{\neg(\forall x.\ x \in a \Rightarrow x \in a)} \to (A \mapsto a, B \mapsto a)$$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \rightarrow \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \rightarrow A \subseteq B \land B \subseteq A$$

$$\cfrac{\cfrac{\neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\ \delta_{\neg\forall}}{\neg(\forall x.\ x \in a \Rightarrow x \in a)} \rightarrow (A \mapsto a, B \mapsto a)$$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \rightarrow \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \rightarrow A \subseteq B \land B \subseteq A$$

$$\cfrac{\cfrac{\cfrac{\neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\ \delta_{\neg\forall}}{\neg(\forall x.\ x \in a \Rightarrow x \in a)}\ \rightarrow (A \mapsto a, B \mapsto a)}{\neg(s \in a \Rightarrow s \in a)}\ \delta_{\neg\forall}$$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \rightarrow \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\ \delta_{\neg\forall}}{\neg(\forall x.\ x \in a \Rightarrow x \in a)}\ \rightarrow (A \mapsto a, B \mapsto a)}{\neg(s \in a \Rightarrow s \in a)}\ \delta_{\neg\forall}}{\neg(s \in a), (s \in a)}\ \alpha_{\neg\Rightarrow}$$

Deduction Modulo Theory (DMT)

Rewrite Rules

$$A \subseteq B \rightarrow \forall x.\ x \in A \Rightarrow x \in B$$
$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\;\delta_{\neg\forall}}{\neg(\forall x.\ x \in a \Rightarrow x \in a)}\;\rightarrow (A \mapsto a, B \mapsto a)}{\neg(s \in a \Rightarrow s \in a)}\;\delta_{\neg\forall}}{\neg(s \in a), (s \in a)}\;\alpha_{\neg\Rightarrow}}{\odot}\;\odot$$

Deduction Modulo Theory (DMT)

Benefits

- Avoid combinatorial explosion
- “Useless” axioms aren’t triggered
- Shorter proof
- Not limited to one theory

Integration

- Triggered when a predicate is generated
- Backtrack if multiples rules are available
- Polarized extension to handle $\Rightarrow$

Scale-Up Experimental Results (1)

	SYN (207 problems)	SET (113 problems)
2	**1.5 s**	**20 s** (+4)
4	**0.6 s**	**15 s** (+5)
8	**0.4 s**	**12 s** (+8)
16	**0.8 s**	**8.7 s** (+10)
28	**0.3 s** (+ 2)	**8.7 s** (+11)

Table 1: Scale-up experimental results of `Goéland`.

Scale-Up Experimental Results (2)

	SYN (207 problems)	SET (208 problems)
2	**1.4 s** (+ 1)	**6.1 s** (+ 5)
4	**1.3 s**	**5.3 s** (+ 8)
8	**1.1 s**	**4.7 s** (+ 7)
16	**0.6 s** (+ 1)	**4.2 s** (+ 9)
28	**0.4 s** (+ 2)	**3.1 s** (+ 9)

Table 2: Scale-up experimental results of `Goéland+DMT`.

Proof Tree and Segments

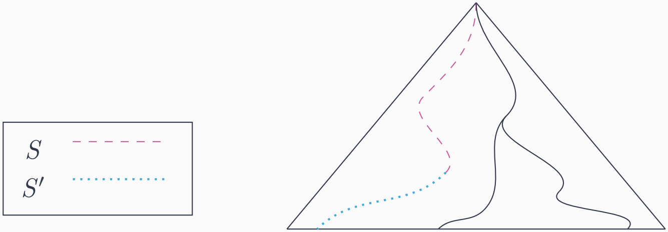


Figure 4: S is an initial segment, S' is a branch, and $S \sqsubseteq S'$.

Mapping

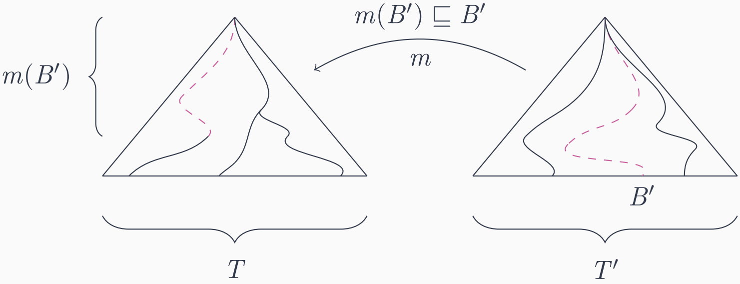


Figure 5: The branch B' is mapped to the initial segment $m(B')$, which means B' contains at least all the formulas of $m(B')$.

Mapping Progression

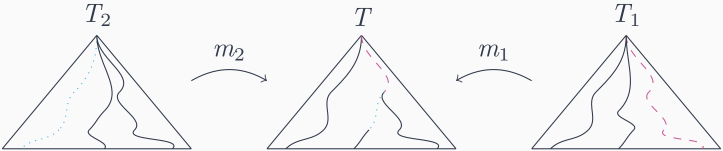


Figure 6: m_2 is “more extended” than m_1

Proof

Key Ideas of the Proof

- We consider a proof (T, σ) for a formula F with a reintroduction limit l
- We consider the proof (T', σ') generated by `Goéland` with the same limit
- We build a mapping between T and T' and show that every branch is T is going to have at least all the formulas than the equivalent one in T

Critical Points

- The agreement mechanism terminates
- A “good” substitution cannot be forbidden