

Designing an Automated Concurrent Tableau-Based Theorem Prover for First-Order Logic

Phd Defense

Julie Cailler

13 December 2023

Under the supervision of:

David Delahaye

Hinde Lilia Bouziane

Simon Robillard

MaREL Team
Laboratoire d'Informatique, de Robotique et de
Microélectronique de Montpellier
University of Montpellier



Bugs?

Tests

- Cheaper
- Faster
- Generate partial use cases and check if the system is working as expected



Formal Methods

- Expensive
- Time-consuming
- Use rigorous mathematical techniques to ensure that a system is working as expected



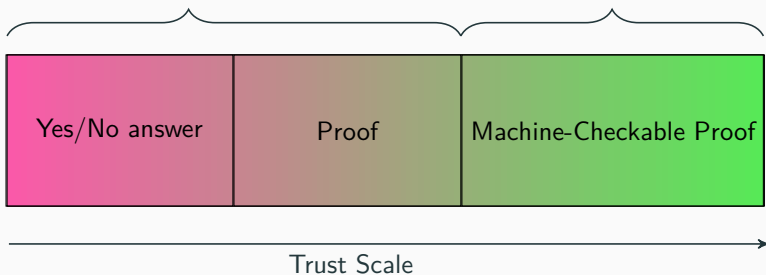
Proofs

Automated Theorem Proving

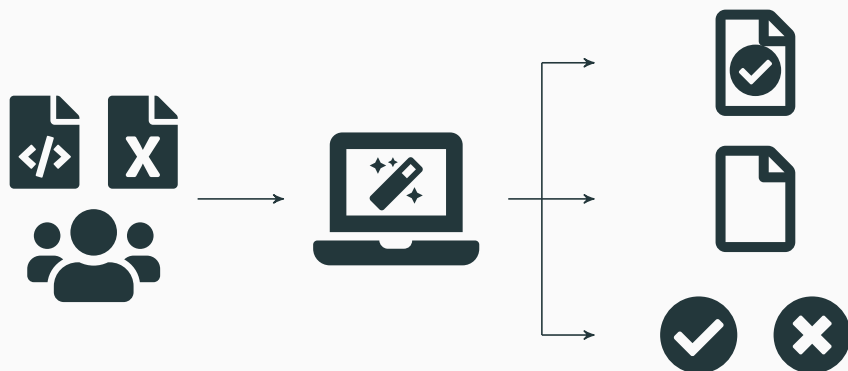
- Click-and-prove software
- Searching for a proof all by themselves
- Output a statement or a proof-like trace

Interactive Theorem Proving

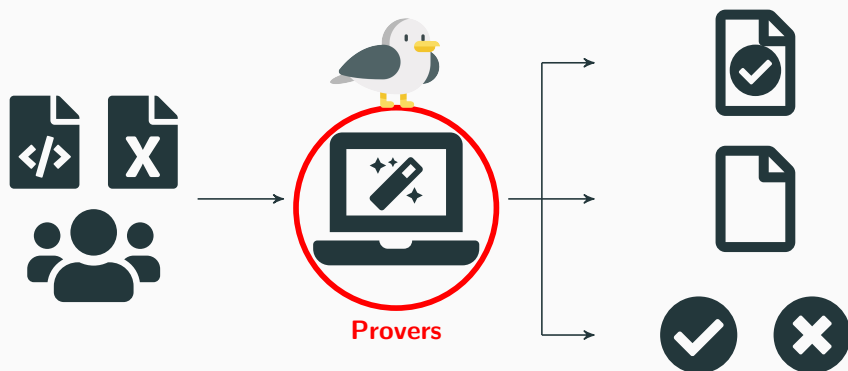
- Proof assistants
- Guide humans towards proof
- Proof are machine-checkable and certified



Big Picture



Big Picture



Yet Another Prover

How to...

- Perform an efficient and fair tableau-based proof-search procedure?
- Prove the completeness of the procedure?
- Make it suitable to reason on larger contexts?
- Provide a machine-checkable proof while using advanced proof-search strategies?

Yet Another Prover

How to...

- Perform an efficient and fair tableau-based proof-search procedure?
- Prove the completeness of the procedure?
- Make it suitable to reason on larger contexts?
- Provide a machine-checkable proof while using advanced proof-search strategies?

1. Preliminary Notions

1.1. Logic

1.2. Method of Analytic Tableaux

Logic

What is Logic?

- Study of correct reasoning
- Mathematical representation of the world
- Truth value of a statement

First-Order Logic (FOL)

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

Method of Analytic Tableaux

Principle

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

Origin & Strengths

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

$$\begin{array}{c}
 \frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\neg\exists} \\
 \frac{\quad}{P(a), \neg(P(a) \wedge P(b))} \alpha_{\neg\Rightarrow} \\
 \frac{\quad}{\neg P(a)} \beta_{\neg\wedge} \\
 \frac{\quad}{\odot} \odot
 \end{array}
 \quad
 \begin{array}{c}
 \frac{\quad}{\neg P(b)} \beta_{\neg\wedge} \\
 \frac{\quad}{\neg(P(b) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\neg\exists} \\
 \frac{\quad}{P(b), \neg(P(a) \wedge P(b))} \alpha_{\neg\Rightarrow} \\
 \frac{\quad}{\odot} \odot
 \end{array}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

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

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$Human(Socrates)$

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

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\textit{Human}(\textit{Socrates}) \quad \forall x. \neg \textit{Human}(x)}{\neg \textit{Human}(X)} \quad \gamma$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{Human(Socrates)}{\forall x. \neg Human(x)}}{\neg Human(\mathbf{Socrates})} \gamma_{\forall}}{\sigma = \{\mathbf{X} \mapsto Socrates\}} \odot_{\sigma}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(X) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\frac{\neg(P(X) \Rightarrow (P(a) \wedge P(b)))}{P(X), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}} \gamma_{\forall}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(X) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(X), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\neg P(a) \quad \neg P(b)} \beta_{\neg \wedge}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(X) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(X), \neg(P(a) \wedge P(b))} \alpha_{\Rightarrow}}{\neg P(a) \quad \neg P(b)} \beta_{\neg \wedge}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(X) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(X), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\neg P(a) \quad \neg P(b)} \beta_{\neg \wedge}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(X) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(X), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\neg P(a) \quad \neg P(b)} \beta_{\neg \wedge}}{\sigma = \{X \mapsto a\}} \odot_{\sigma}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(a), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\neg P(a) \quad \neg P(b)} \beta_{\neg \wedge}}{\sigma = \{X \mapsto a\}} \odot_{\sigma}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{\frac{P(a), \neg(P(a) \wedge P(b))}{\neg P(a)} \alpha_{\neg \Rightarrow}} \beta_{\neg \wedge}}{\frac{\neg P(a)}{\sigma = \{X \mapsto a\}} \odot_{\sigma}} \quad \frac{\neg P(b)}{\neg(P(X_2) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(a), \neg(P(a) \wedge P(b))} \alpha_{\Rightarrow}}{\neg P(a)} \beta_{\neg \wedge}}{\sigma = \{X \mapsto a\}} \odot_{\sigma} \quad \frac{\frac{\frac{\neg(P(X_2) \Rightarrow (P(a) \wedge P(b)))}{P(X_2), \neg(P(a) \wedge P(b))} \alpha_{\Rightarrow}}{\neg P(b)} \beta_{\neg \wedge}}{\neg(P(X_2) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}} \alpha_{\Rightarrow}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(a), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\neg P(a)} \beta_{\neg \wedge} \quad \frac{\frac{\frac{\neg P(b)}{\neg(P(X_2) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(X_2), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\sigma = \{X \mapsto a\}} \odot_{\sigma}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\begin{array}{c}
 \frac{\frac{\frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall}}{P(a), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\neg P(a)} \beta_{\neg \wedge} \\
 \frac{\sigma = \{X \mapsto a\}}{\neg P(a)} \odot_{\sigma}
 \end{array}
 \quad
 \begin{array}{c}
 \frac{\frac{\frac{\neg(P(X_2) \Rightarrow (P(a) \wedge P(b)))}{P(X_2), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow}}{\neg P(b)} \beta_{\neg \wedge}}{\sigma = \{X_2 \mapsto b\}} \odot_{\sigma}
 \end{array}$$

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions

$$\begin{array}{c}
 \frac{\neg(\exists x. P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))} \gamma_{\forall} \\
 \frac{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))}{P(a), \neg(P(a) \wedge P(b))} \alpha_{\neg \Rightarrow} \\
 \frac{P(a), \neg(P(a) \wedge P(b))}{\neg P(a)} \beta_{\neg \wedge} \\
 \frac{\neg P(a)}{\sigma = \{X \mapsto a\}} \odot_{\sigma}
 \end{array}
 \quad
 \begin{array}{c}
 \frac{\neg(P(b) \Rightarrow (P(a) \wedge P(b)))}{P(b), \neg(P(a) \wedge P(b))} \gamma_{\forall} \\
 \frac{P(b), \neg(P(a) \wedge P(b))}{\neg P(b)} \alpha_{\neg \Rightarrow} \\
 \frac{\neg P(b)}{\sigma = \{X_2 \mapsto b\}} \odot_{\sigma}
 \end{array}$$

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

2.1. Fairness Challenges in Tableaux

2.2. A Concurrent Proof-Search Procedure

Fairness in Tableaux

Fairness

A proof-search procedure is *fair* if and only if each formula on which a non- γ -rule can be applied occurs in a subsequent step, and every γ -rules will be computed an arbitrary number of times.

“At the present time, no strongly complete, destructive tableau proof procedure is known that works well in practice.”

— Reiner Hähnle, *Handbook of Automated Reasoning Vol.1*, 2001

Fairness Management

Unfairness Sources

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

State-of-the-Art Answers & Heuristics

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

Select Pair and Select Mode

$$\begin{aligned} & \neg P(a) \\ & \neg Q(b) \\ & \neg S(c) \\ & \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \end{aligned}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \\
 \hline
 P(X) \vee Q(X), \forall y. S(X)
 \end{array}
 \quad \mathcal{A}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \quad \gamma_{\forall} \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \\
 \hline
 P(X), \forall y. S(X) \qquad Q(X), \forall y. S(X) \quad \beta_{\Leftrightarrow}
 \end{array}$$

Select Pair and Select Mode

$$\frac{
 \frac{
 \frac{
 \neg P(a)
 }{
 \neg Q(b)
 }
 }{
 \neg S(c)
 }
 }{
 \frac{
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)
 }{
 P(X) \vee Q(X), \forall y. S(X)
 } \gamma_{\forall}
 }
 }{
 \frac{
 P(X), \forall y. S(X) \quad Q(X), \forall y. S(X)
 }{
 } \beta_{\Leftrightarrow}
 }$$

Select Pair and Select Mode

$$\frac{
 \frac{
 \frac{
 \neg P(a)
 }{
 \neg Q(b)
 }
 }{
 \neg S(c)
 }
 }{
 \frac{
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)
 }{
 P(X) \vee Q(X), \forall y. S(X)
 } \gamma_{\forall}
 }
 }{
 \frac{
 P(X), \forall y. S(X)
 }{
 \sigma = \{X \mapsto a\}
 } \odot_{\sigma}
 }
 }{
 Q(X), \forall y. S(X)
 } \beta_{\Leftrightarrow}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(a) \vee Q(a), \forall y. S(a)} \gamma_{\forall} \\
 \frac{P(a), \forall y. S(a)}{\sigma = \{X \mapsto a\}} \odot_{\sigma} \quad \frac{Q(a), \forall y. S(a)}{\beta_{\Leftrightarrow}}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(a) \vee Q(a), \forall y. S(a)} \gamma_{\forall} \\
 \frac{P(a), \forall y. S(a)}{\sigma = \{X \mapsto a\}} \odot_{\sigma} \quad \frac{Q(a), \forall y. S(a)}{S(a)} \gamma_{\forall} \quad \beta_{\Leftrightarrow}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(a) \vee Q(a), \forall y. S(a)} \gamma_{\forall} \\
 \\
 \frac{\frac{P(a), \forall y. S(a)}{\sigma = \{X \mapsto a\}} \odot_{\sigma} \quad \frac{\frac{Q(a), \forall y. S(a)}{S(a)} \gamma_{\forall}}{P(X_2) \vee Q(X_2), \forall y. S(X_2)} \beta_{\Leftrightarrow} \gamma_{\forall}}{}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(a) \vee Q(a), \forall y. S(a)} \gamma_{\forall} \\
 \\
 \frac{P(a), \forall y. S(a)}{\sigma = \{X \mapsto a\}} \odot_{\sigma} \quad \frac{\frac{Q(a), \forall y. S(a)}{S(a)} \gamma_{\forall}}{\frac{P(X_2) \vee Q(X_2), \forall y. S(X_2)}{P(X_2), \forall y. S(X_2) \quad Q(X_2), \forall y. S(X_2)} \beta_{\vee}} \beta_{\Leftrightarrow}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(a) \vee Q(a), \forall y. S(a)} \gamma_{\forall} \\
 \frac{\frac{P(a), \forall y. S(a)}{\sigma = \{X \mapsto a\}} \odot_{\sigma} \quad \frac{\frac{Q(a), \forall y. S(a)}{S(a)} \gamma_{\forall}}{P(X_2) \vee Q(X_2), \forall y. S(X_2)} \gamma_{\forall}}{\frac{P(X_2), \forall y. S(X_2) \quad Q(X_2), \forall y. S(X_2)}{\dots} \beta_{\vee}} \beta_{\Leftrightarrow}
 \end{array}$$

Select Pair and Select Mode

$$\begin{aligned} & \neg P(a) \\ & \neg Q(b) \\ & \neg S(c) \\ & \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \end{aligned}$$

Select Pair and Select Mode

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

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \quad \gamma_{\forall} \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \\
 \hline
 P(X), \forall y. S(X) \quad Q(X), \forall y. S(X) \quad \beta_{\Leftrightarrow}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \quad \gamma_{\forall} \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \\
 \hline
 \frac{P(X), \forall y. S(X) \quad \gamma_{\forall} \quad Q(X), \forall y. S(X) \quad \beta_{\Leftrightarrow}}{S(X)} \gamma_{\forall}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \gamma_{\forall} \\
 \hline
 \frac{P(X), \forall y. S(X)}{S(X)} \gamma_{\forall} \quad Q(X), \forall y. S(X) \quad \beta_{\Leftrightarrow} \\
 \hline
 \frac{S(X)}{\sigma = \{X \mapsto c\}} \odot_{\sigma}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(c) \vee Q(c), \forall y. S(c)} \gamma_{\forall} \\
 \frac{\frac{P(c), \forall y. S(c)}{S(c)} \gamma_{\forall} \quad Q(c), \forall y. S(c)}{\sigma = \{X \mapsto c\}} \beta_{\Leftrightarrow} \odot_{\sigma}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(c) \vee Q(c), \forall y. S(c)} \gamma_{\forall} \\
 \frac{\frac{P(c), \forall y. S(c)}{S(c)} \gamma_{\forall} \quad \frac{Q(c), \forall y. S(c)}{S(c)} \gamma_{\forall}}{\sigma = \{X \mapsto c\}} \beta_{\Leftrightarrow} \odot_{\sigma}
 \end{array}$$

Select Pair and Select Mode

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \boxed{\neg S(c)} \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(c) \vee Q(c), \forall y. S(c)} \gamma_{\forall} \\
 \frac{\frac{P(c), \forall y. S(c)}{S(c)} \gamma_{\forall} \quad \frac{Q(c), \forall y. S(c)}{S(c)} \gamma_{\forall}}{\sigma = \{X \mapsto c\}} \beta_{\Leftrightarrow} \quad \frac{\boxed{S(c)}}{\odot} \odot_{\sigma}
 \end{array}$$

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

New Challenges

- Free variable dependency
- Communication between branches

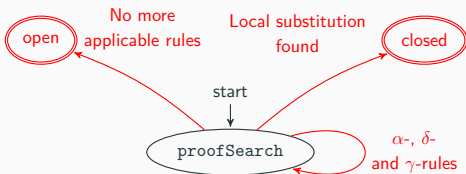
Procedures Interactions

PS

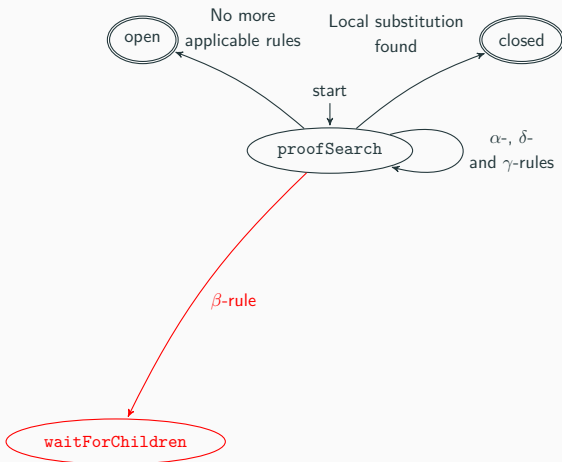
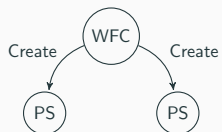


Procedures Interactions

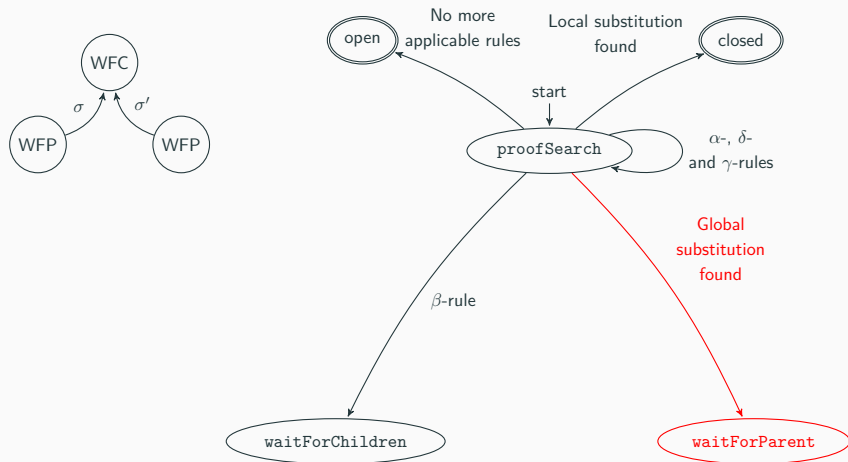
PS



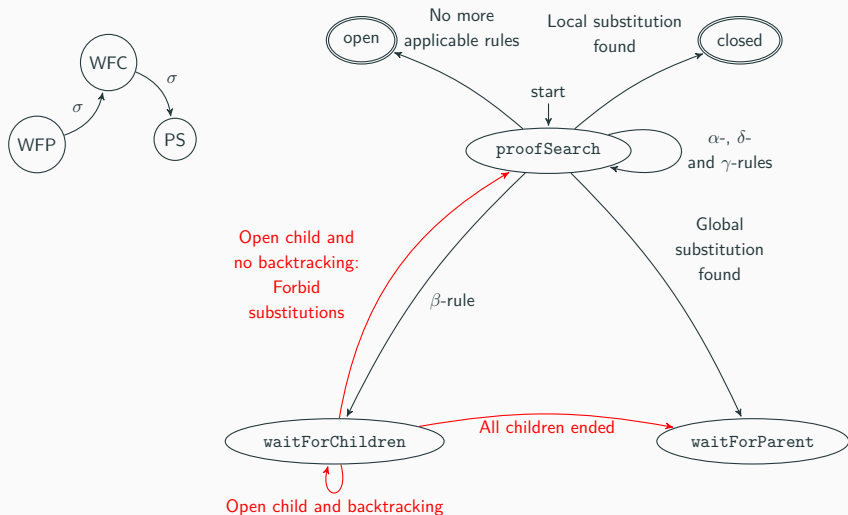
Procedures Interactions



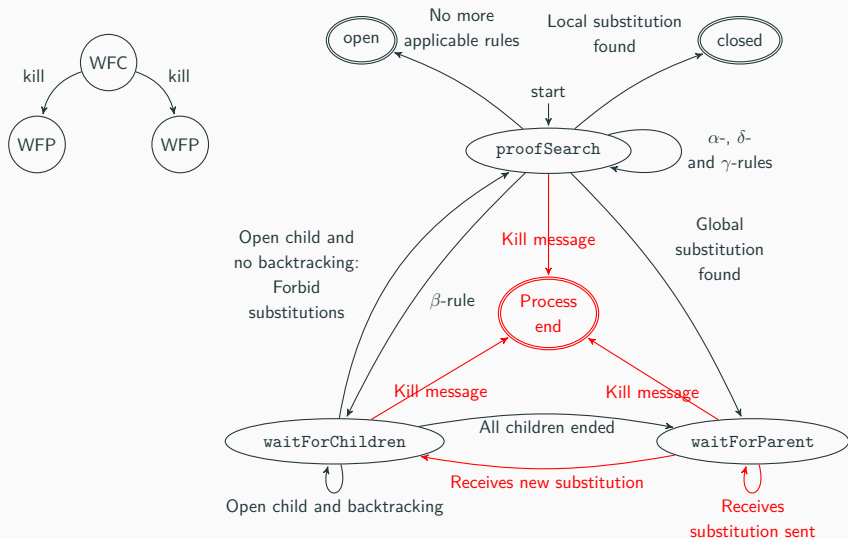
Procedures Interactions



Procedures Interactions



Procedures Interactions



Solving Fairness Issues with Concurrency

$$\begin{aligned} & \neg P(a) \\ & \neg Q(b) \\ & \neg S(c) \\ & \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \end{aligned}$$

Solving Fairness Issues with Concurrency

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

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \quad \gamma_{\forall} \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \\
 \hline
 P(X), \forall y. S(X) \quad Q(X), \forall y. S(X) \quad \beta_{\Leftrightarrow}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \gamma_{\forall} \\
 \frac{\frac{P(X), \forall y. S(X)}{\odot} \odot_{\sigma} \quad \frac{Q(X), \forall y. S(X)}{\odot} \odot_{\sigma}}{\beta_{\Leftrightarrow}}
 \end{array}$$

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

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \gamma_{\forall} \\
 \frac{\frac{P(X), \forall y. S(X)}{\odot_{\sigma}} \quad \frac{Q(X), \forall y. S(X)}{\odot_{\sigma}}}{\beta \Leftrightarrow}
 \end{array}$$

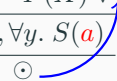
$\sigma = \{X \mapsto a\}$ $\sigma = \{X \mapsto b\}$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \quad \gamma_{\forall} \\
 \hline
 \frac{P(a), \forall y. S(a) \quad Q(a), \forall y. S(a)}{\quad} \quad \beta_{\Leftrightarrow} \\
 \hline
 \sigma = \{X \mapsto a\} \qquad \sigma = \{X \mapsto a\}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \quad \gamma_{\forall} \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \\
 \hline
 \frac{P(a), \forall y. S(a) \quad Q(a), \forall y. S(a)}{\quad} \beta_{\Leftrightarrow} \\
 \frac{\quad}{\quad} \odot_{\sigma}
 \end{array}$$



 Closed

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \quad \gamma_{\forall} \\
 \hline
 \frac{\frac{P(a), \forall y. S(a)}{\odot} \quad \odot_{\sigma} \quad \frac{Q(a), \forall y. S(a)}{S(a)} \quad \gamma_{\forall}}{\beta_{\Leftrightarrow}}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \quad \gamma_{\forall} \\
 \hline
 \frac{P(a), \forall y. S(a)}{\odot} \quad \odot_{\sigma} \quad \frac{Q(a), \forall y. S(a)}{\gamma_{\forall}} \quad \beta_{\Leftrightarrow} \\
 \hline
 \frac{S(a)}{\dots} \\
 \text{Open}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \quad \gamma_{\forall} \\
 \hline
 \frac{P(b), \forall y. S(b)}{\sigma = \{X \mapsto b\}} \quad \frac{Q(b), \forall y. S(b)}{\sigma = \{X \mapsto b\}} \quad \beta_{\Leftrightarrow}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \quad \gamma_{\forall} \\
 \hline
 P(b), \forall y. S(b) \quad \beta_{\Leftrightarrow} \\
 \hline
 Q(b), \forall y. S(b) \quad \odot_{\sigma} \\
 \hline
 \odot_{\sigma} \\
 \text{Closed}
 \end{array}$$

A blue arrow points from the \odot_{σ} symbol to the β_{\Leftrightarrow} symbol, indicating a transition or relationship between the two states.

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \quad \gamma_{\forall} \\
 \hline
 P(X) \vee Q(X), \forall y. S(X) \\
 \hline
 \frac{P(b), \forall y. S(b)}{S(b)} \gamma_{\forall} \quad \frac{Q(b), \forall y. S(b)}{\odot} \beta_{\Leftrightarrow} \odot_{\sigma}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(a) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \gamma_{\forall} \\
 \frac{P(b), \forall y. S(b)}{S(b)} \gamma_{\forall} \quad \frac{Q(b), \forall y. S(b)}{\odot} \beta_{\Leftrightarrow} \odot_{\sigma} \\
 \dots \\
 \text{Open}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \quad \gamma \forall \\
 \hline
 \frac{P(X), \forall y. S(X) \quad Q(X), \forall y. S(X)}{\beta \Leftrightarrow} \\
 \begin{array}{cc}
 \swarrow & \searrow \\
 X \notin \{a, b\} & X \notin \{a, b\}
 \end{array}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{P(X) \vee Q(X), \forall y. S(X)} \quad \gamma_{\forall} \\
 \frac{\frac{P(X), \forall y. S(X)}{S(X)} \quad \gamma_{\forall} \quad \frac{Q(X), \forall y. S(X)}{S(X)} \quad \gamma_{\forall}}{\quad} \beta_{\Leftrightarrow}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \boxed{\neg S(c)} \\
 \frac{\forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x)}{\quad} \gamma_{\forall} \\
 \frac{P(X) \vee Q(X), \forall y. S(X)}{\quad} \beta_{\Leftrightarrow} \\
 \frac{P(X), \forall y. S(X)}{\quad} \gamma_{\forall} \quad \frac{Q(X), \forall y. S(X)}{\quad} \gamma_{\forall} \\
 \frac{\boxed{S(X)}}{\quad} \odot_{\sigma} \quad \frac{\boxed{S(X)}}{\quad} \odot_{\sigma} \\
 \sigma = \{X \mapsto c\} \quad \sigma = \{X \mapsto c\}
 \end{array}$$

Solving Fairness Issues with Concurrency

$$\begin{array}{c}
 \neg P(a) \\
 \neg Q(b) \\
 \neg S(c) \\
 \hline
 \forall x. (P(x) \vee Q(x)) \wedge \forall y. S(x) \quad \gamma_{\forall} \\
 \hline
 P(c) \vee Q(c), \forall y. S(c) \\
 \hline
 \frac{P(c), \forall y. S(c)}{S(c)} \gamma_{\forall} \quad \frac{Q(c), \forall y. S(c)}{S(c)} \gamma_{\forall} \quad \beta_{\Leftrightarrow} \\
 \frac{S(c)}{\odot} \odot_{\sigma} \quad \frac{S(c)}{\odot} \odot_{\sigma} \\
 \sigma = \{X \mapsto c\} \quad \sigma = \{X \mapsto c\}
 \end{array}$$

Contributions

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

3. Goéland: Implementation, Experiments, and Analysis

- 3.1. The Goéland Automated Theorem Prover**
- 3.2. Theory Reasoning**
- 3.3. Experiments and Analysis**

Goéland Tool

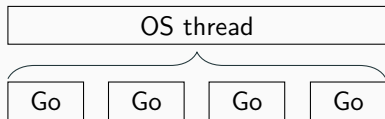
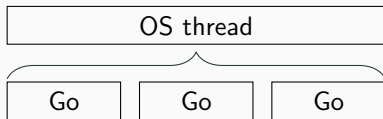
Functionnalités

- Concurrent proof-search procedure
- Equality reasoning
- Deduction modulo theory (+ polarized)
- Polymorphic types
- Alternative modes: incomplete, interactive,...

Goéland Tool

Implementation

- 30 000 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 axiom 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: $\forall x. P(x) \Leftrightarrow \forall y. Q(x, y) \wedge S(x, y)$

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

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)

Scale-Up Experimental Results

	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.

	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.

Analysis

- Promising results
- Less problems solved than other ATP
- Scaling issue
- Memory management
- Equality reasoning performances
- Good results with DMT

4. Toward Certification: an Output for Checkable Proofs

4.1. Skolemization and Translation

4.2. A Deskolemization Strategy

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

Pre-Inner Skolemization (δ^{++} -rule)

- Extension of δ^+ -rule
- Reuses the same Skolem symbol if they come from α -equivalent formulas

Example

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

(a) Outer Skolemization tableau.

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

(b) Inner Skolemization tableau.

Translation to Machine-Checkable Proofs

Gentzen-Schütte Calculus (GS3)

- Equivalent to tableaux
- Easily translatable to proof assistants
- Only supports outer skolemization

$$\frac{\frac{\frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y))}{\neg(D(X) \Rightarrow \forall y D(y))} \gamma_{\neg\exists}}{\frac{D(X), \neg(\forall y D(y))}{\neg D(f(X))} \delta_{\neg\forall}} \gamma_{\neg\exists}}{\frac{\neg(D(X_2) \Rightarrow \forall y D(y))}{D(X_2), \neg\forall y D(y)} \alpha_{\neg\Rightarrow}} \gamma_{\neg\exists}} \odot_{\sigma}$$

$$\sigma = \{X_2 \mapsto f(X)\}$$

(a) Outer Skolemization tableau proof.

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

(b) Equivalent GS3.

Translation in Inner Skolemization

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

(a) Inner Skolemization tableau proof.

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

(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 Notions

- Formulas that depend on a Skolem symbol
- Formulas that descend from 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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y))}{\neg(D(X) \Rightarrow \forall y D(y))} \gamma_{\neg\exists} \\
 \frac{\quad}{D(X), \neg(\forall y D(y))} \alpha_{\neg\Rightarrow} \\
 \frac{\quad}{\neg D(c)} \delta_{\neg\forall}^+ \\
 \frac{\quad}{\sigma = \{X \mapsto c\}} \odot_{\sigma}
 \end{array}$$

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)), \neg D(c) \vdash}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)) \vdash} \neg_{\forall} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), D(c), \neg(\forall y D(y)) \vdash} W \times 2 \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)) \vdash} \neg_{\Rightarrow} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y))} \neg_{\exists}
 \end{array}$$

Example

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

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

Example

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y))}{\neg(D(X) \Rightarrow \forall y D(y))} \gamma_{\neg\exists} \\
 \frac{\quad}{D(X), \neg(\forall y D(y))} \alpha_{\neg\Rightarrow} \\
 \frac{\quad}{\neg D(c)} \delta_{\neg\forall}^+ \\
 \frac{\quad}{\sigma = \{X \mapsto c\}} \odot_{\sigma}
 \end{array}$$

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)), \neg D(c) \vdash}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)) \vdash} \neg_{\forall} \\
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), D(c), \neg(\forall y D(y)) \vdash}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)) \vdash} W \times 2 \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y))} \neg_{\exists}
 \end{array}$$

Example

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y))}{\neg(D(X) \Rightarrow \forall y D(y))} \gamma_{\neg\exists} \\
 \frac{\quad}{D(X), \neg(\forall y D(y))} \alpha_{\neg\Rightarrow} \\
 \frac{\quad}{\neg D(c)} \delta_{\neg\forall}^+ \\
 \frac{\quad}{\sigma = \{X \mapsto c\}} \odot_{\sigma}
 \end{array}$$

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

Example

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

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

Example

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

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

Example

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y))}{\neg(D(X) \Rightarrow \forall y D(y))} \gamma_{\neg\exists} \\
 \frac{\quad}{D(X), \neg(\forall y D(y))} \alpha_{\neg\Rightarrow} \\
 \frac{\quad}{\neg D(c)} \delta_{\neg\forall}^+ \\
 \frac{\quad}{\sigma = \{X \mapsto c\}} \odot_{\sigma}
 \end{array}$$

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), D(c), \neg(\forall y D(y)), \neg D(c) \vdash}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), \neg(\forall y D(y)), \neg D(c) \vdash} \neg_{\Rightarrow} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)), \neg D(c) \vdash} \neg_{\exists} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)) \vdash} \neg_{\forall} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), D(c), \neg(\forall y D(y)) \vdash} W \times 2 \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)) \vdash} \neg_{\Rightarrow} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y))} \neg_{\exists}
 \end{array}$$

Example

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y))}{\neg(D(X) \Rightarrow \forall y D(y))} \gamma_{\neg\exists} \\
 \frac{\quad}{D(X), \neg(\forall y D(y))} \alpha_{\neg\Rightarrow} \\
 \frac{\quad}{\neg D(c)} \delta_{\neg\forall}^+ \\
 \frac{\quad}{\sigma = \{X \mapsto c\}} \odot_{\sigma}
 \end{array}$$

$$\begin{array}{c}
 \frac{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), D(c), \neg(\forall y D(y)), \neg D(c) \vdash}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), \neg(\forall y D(y)), \neg D(c) \vdash} \text{ax} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)), \neg D(c) \vdash} \neg_{\Rightarrow} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)), \neg D(c) \vdash} \neg_{\exists} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(\forall y D(y)) \vdash} \neg_{\forall} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)), D(c), \neg(\forall y D(y)) \vdash} \text{W} \times 2 \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y)), \neg(D(c) \Rightarrow \forall y D(y)) \vdash} \neg_{\Rightarrow} \\
 \frac{\quad}{\neg(\exists x. D(x) \Rightarrow \forall y D(y))} \neg_{\exists}
 \end{array}$$

Implementation

Implementation

- δ , δ^+ and δ^{++} Skolemization strategies
- GS3 proofs
- Deskolemization algorithms
- Coq & Lambdapi outputs

Evaluation Protocol

- Same setup as previous tests
- 3 Skolemization strategies + DMT
- Number of problems solved
- 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+ δ^{++}	274	100 %	10.6 %	10.3
Goéland+DMT	363	100 %	0 %	-
Goéland+DMT+ δ^+	375	100 %	4.5 %	3.9
Goéland+DMT+ δ^{++}	377	100 %	7.4 %	5.2

Contributions

- An optimization of the deskolemization algorithm for δ^+
- A deskolemization algorithm for δ^{++}
- Soundness proof for both translations
- Output of GS3 proof into Coq and Lambdapi
- Promising results
- 100% of the proofs are certified
- Far below the theoretical bound

Conclusion

Contributions

Fairness in Tableau-Based Proof Search

- Fairness between branches managed by concurrency
- Completeness of the procedure

Theory Reasoning in Tableaux

- Implementation of two background reasoners
- Study of parallelization points and interaction with the proof search

Proof Certification

- A sound deskolemization algorithm
- Output of the proofs into Coq & Lambdapi

Perspectives

Fairness in Tableau-Based Proof Search

- Improvement of the performances of Goéland
- Heuristics in formula computation order, closure management
- Simulate “intuition” with learning methods

Theory Reasoning in Tableaux

- Improvements of DMT (term rewriting, narrowing, manually designed rewrite rules)
- More experiments on polymorphic problems

Proof Certification

- Reduce the number of branches by the use of lemmas
- Framework for verification of tableau proofs

Thank you! 😊

- Johann Rosain (Code trees, DMT, polymorphism, Coq output, deskolemization)
- Nina Janeva (Benchmark)
- Cédric Berthet, Enzo Goulesque, Lorenzo Puccio, Margaux Renoir, Tom Simula (Arithmetic)
- Adrien Mecibah (Debugger)
- Matthieu Pierret (Interactive mode)
- Dylan Bettendroffer (Lambdapi output)
- Isaac Lluís (Arithmetic, memory-shared version, Lambdapi output)



...And Thomas!

First-Order Logic

Conventions

- Constant symbols: a, b, c
- Function symbols: f, f'
- Bound and free variables: x, y, X, X_2, Y
- Predicate symbols: P, Q, S
- Connectives: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
- Quantifiers: \exists, \forall

- *Socrates*
- *Human*(x)
- *Mortal*(x)
- All humans are mortals
- Socrates is a human
- Then Socrates is mortal

$(\forall x. \text{Human}(x) \Rightarrow \text{Mortal}(x)) \wedge \text{Human}(\text{Socrates}) \Rightarrow \text{Mortal}(\text{Socrates})$

Reasoning Methods in FOL

Resolution

- Breaks the initial formula into clauses
- Derivation step and saturation
- More efficient

CNF : $\{\neg A\}, \{A \vee A\}, \{\neg B \vee A\}$
 $\{\neg A\}$

$\{A \vee A\}$

$\{\neg B \vee A\}$

Tableaux

- Works with the unaltered original formula
- Reduces the goal into sub-goals
- Better interoperability

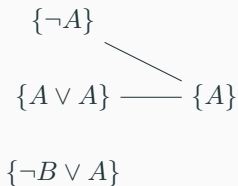
$$\frac{\frac{\frac{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)}{(A \Rightarrow B) \Rightarrow A, \neg A} \alpha_{\neg \Rightarrow}}{\neg(A \Rightarrow B)} \alpha_{\neg \Rightarrow}}{A, \neg B} \alpha_{\neg \Rightarrow}}{\odot} \odot \quad \frac{\beta_{\Rightarrow}}{\odot} \odot$$

Reasoning Methods in FOL

Resolution

- Breaks the initial formula into clauses
- Derivation step and saturation
- More efficient

CNF : $\{\neg A\}, \{A \vee A\}, \{\neg B \vee A\}$



Tableaux

- Works with the unaltered original formula
- Reduces the goal into sub-goals
- Better interoperability

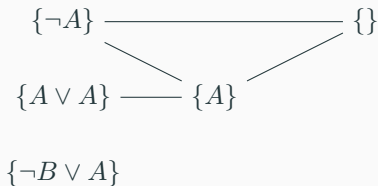
$$\frac{\frac{\frac{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)}{(A \Rightarrow B) \Rightarrow A, \neg A} \alpha_{\neg \Rightarrow}}{\neg(A \Rightarrow B)} \beta_{\Rightarrow}}{A, \neg B} \alpha_{\neg \Rightarrow}}{\odot} \odot$$

Reasoning Methods in FOL

Resolution

- Breaks the initial formula into clauses
- Derivation step and saturation
- More efficient

CNF : $\{\neg A\}, \{A \vee A\}, \{\neg B \vee A\}$



Tableaux

- Works with the unaltered original formula
- Reduces the goal into sub-goals
- Better interoperability

$$\frac{\frac{\frac{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)}{(A \Rightarrow B) \Rightarrow A, \neg A} \alpha_{\neg \Rightarrow}}{\neg(A \Rightarrow B)} \beta_{\Rightarrow}}{A, \neg B} \alpha_{\neg \Rightarrow}}{A, \neg B} \odot \odot$$

Select Branch

$$\frac{\frac{\frac{(P(a) \wedge \neg P(a)) \vee \perp}{P(a) \wedge P(a)} \alpha_{\wedge} \quad \frac{\perp}{P(a), \neg P(a)} \beta_{\vee}}{P(a), \neg P(a)} \odot}{\odot} \odot$$

(a) Proof of $(P(a) \wedge \neg P(a)) \vee \perp$.

$$\frac{\frac{\frac{(P(a) \wedge \neg P(a)) \vee \perp}{P(a) \wedge P(a)} \alpha_{\wedge} \quad \frac{\perp}{P(a), \neg P(a)} \beta_{\vee}}{P(a), \neg P(a)} \odot}{\odot} \dots$$

(b) Incompleteness caused by an unfair select branch.

Select Formula

$$\frac{\frac{P(a) \wedge \neg P(a)}{\forall x Q(X)} \alpha_{\wedge}}{\frac{P(a), \neg P(a)}{\odot}} \odot$$

(a) Proof of $P(a) \wedge \neg P(a), \forall x Q(X)$.

$$\frac{\frac{P(a) \wedge \neg P(a)}{\forall x Q(X)} \gamma_{\forall}}{\frac{Q(X)}{\gamma_{\forall}}} \gamma_{\forall}$$
$$\frac{\frac{Q(X')}{\gamma_{\forall}}}{\dots} \gamma_{\forall}$$

(b) Incompleteness caused by an unfair select formula.

Select Pair (Right Branch First)

$$\begin{array}{c} P(a) \\ \neg P(b) \\ \forall x. P(x) \Leftrightarrow (\forall y P(y)) \end{array}$$

Select Pair (Right Branch First)

$$\frac{\begin{array}{c} P(a) \\ \neg P(b) \\ \forall x. P(x) \Leftrightarrow (\forall y P(y)) \end{array}}{P(X) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}$$

Select Pair (Right Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)}}{\forall x. P(x) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{P(X) \Leftrightarrow (\forall y P(y))} \beta_{\Leftrightarrow}}{P(X), \forall y P(y) \quad \neg P(X), \neg(\forall y P(y))} \beta_{\Leftrightarrow}$$

Select Pair (Right Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)} \quad \forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(X) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(X), \forall y P(y) \quad \neg P(X), \neg(\forall y P(y))}{\sigma = \{X \mapsto a\}} \beta_{\Leftrightarrow} \odot_{\sigma}}$$

Select Pair (Right Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)}}{\forall x. P(x) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{P(a) \Leftrightarrow (\forall y P(y))} \beta_{\Leftrightarrow}}{\frac{P(a), \forall y P(y) \quad \neg P(a), \neg(\forall y P(y))}{\sigma = \{X \mapsto a\}} \odot_{\sigma}}$$

Select Pair (Right Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)}{\forall x. P(x) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{P(a) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(a), \forall y P(y)}{P(Y)} \gamma_{\forall} \quad \frac{\neg P(a), \neg(\forall y P(y))}{\sigma = \{X \mapsto a\}} \odot_{\sigma}} \beta_{\Leftrightarrow}$$

Select Pair (Right Branch First)

$$\begin{array}{c}
 P(a) \\
 \neg P(b) \\
 \frac{\forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(a) \Leftrightarrow (\forall y P(y))} \gamma_{\forall} \\
 \frac{P(a), \forall y P(y)}{P(Y)} \gamma_{\forall} \quad \frac{\neg P(a), \neg(\forall y P(y))}{\sigma = \{X \mapsto a\}} \beta_{\Leftrightarrow} \\
 \frac{P(Y)}{\sigma = \{Y \mapsto b\}} \odot_{\sigma} \quad \odot_{\sigma}
 \end{array}$$

Select Pair (Right Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)} \quad \forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(a) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(a), \forall y P(y)}{P(b)} \gamma_{\forall} \quad \frac{\neg P(a), \neg(\forall y P(y))}{\sigma = \{X \mapsto a\}} \beta_{\Leftrightarrow}} \odot_{\sigma}$$
$$\frac{\frac{P(b)}{\sigma = \{Y \mapsto b\}} \odot_{\sigma}}{\sigma = \{Y \mapsto b\}} \odot_{\sigma}$$

Select Pair (Left Branch First)

$$\begin{array}{l} P(a) \\ \neg P(b) \\ \forall x. P(x) \Leftrightarrow (\forall y P(y)) \end{array}$$

Select Pair (Left Branch First)

$$\frac{\begin{array}{c} P(a) \\ \neg P(b) \\ \forall x. P(x) \Leftrightarrow (\forall y P(y)) \end{array}}{P(X) \Leftrightarrow (\forall y P(y))} \quad \gamma_{\forall}$$

Select Pair (Left Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)}}{\forall x. P(x) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{P(X) \Leftrightarrow (\forall y P(y))} \beta_{\Leftrightarrow}$$

$$\frac{P(X), \forall y P(y)}{\neg P(X), \neg(\forall y P(y))} \beta_{\Leftrightarrow}$$

Select Pair (Left Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)} \quad \forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(X) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(X), \forall y P(y)}{\sigma = \{X \mapsto b\}} \odot_{\sigma}} \beta_{\Leftrightarrow}$$

Select Pair (Left Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)} \quad \forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(b) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(b), \forall y P(y)}{\sigma = \{X \mapsto b\}} \odot_{\sigma} \quad \neg P(b), \neg(\forall y P(y))} \beta_{\Leftrightarrow}$$

Select Pair (Left Branch First)

$$\frac{\frac{\frac{P(a)}{\neg P(b)} \quad \forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(b) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(b), \forall y P(y)}{\sigma = \{X \mapsto b\}} \odot_{\sigma}} \quad \frac{\frac{\neg P(b), \neg(\forall y P(y))}{\neg P(f(b))} \delta_{\neg\forall}}{\beta_{\Leftrightarrow}}$$

Select Pair (Left Branch First)

$$\begin{array}{c}
 P(a) \\
 \neg P(b) \\
 \hline
 \forall x. P(x) \Leftrightarrow (\forall y P(y)) \\
 \hline
 P(b) \Leftrightarrow (\forall y P(y)) \quad \gamma_{\forall} \\
 \hline
 \frac{P(b), \forall y P(y)}{\sigma = \{X \mapsto b\}} \odot_{\sigma} \qquad \frac{\neg P(b), \neg(\forall y P(y))}{\neg P(f(b))} \delta_{\neg_{\forall}} \quad \beta_{\Leftrightarrow} \\
 \hline
 P(X_2) \Leftrightarrow (\forall y P(y)) \quad \gamma_{\forall}
 \end{array}$$

Select Pair (Left Branch First)

$$\begin{array}{c}
 \frac{
 \frac{
 \frac{
 P(a) \\
 \neg P(b) \\
 \forall x. P(x) \Leftrightarrow (\forall y P(y))
 }{
 P(b) \Leftrightarrow (\forall y P(y))
 } \gamma_{\forall}
 }{
 P(b), \forall y P(y)
 } \odot_{\sigma}
 }{
 \sigma = \{X \mapsto b\}
 } \\
 \frac{
 \frac{
 \frac{
 \neg P(b), \neg(\forall y P(y)) \\
 \neg P(f(b))
 }{
 P(X_2) \Leftrightarrow (\forall y P(y))
 } \gamma_{\forall}
 }{
 \neg P(X_2), \neg(\forall y P(y))
 } \delta_{\neg_{\forall}}
 }{
 P(X_2), \forall y P(y) \quad \neg P(X_2), \neg(\forall y P(y))
 } \beta_{\Leftrightarrow}
 }{
 } \beta_{\Leftrightarrow}
 \end{array}$$

Select Pair (Left Branch First)

$$\begin{array}{c}
 \frac{P(a)}{\neg P(b)} \\
 \frac{\forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(b) \Leftrightarrow (\forall y P(y))} \gamma_{\forall} \\
 \frac{P(b), \forall y P(y)}{\sigma = \{X \mapsto b\}} \odot_{\sigma} \quad \frac{\neg P(b), \neg(\forall y P(y))}{\neg P(f(b))} \delta_{\neg\forall} \quad \beta_{\Leftrightarrow} \\
 \frac{\quad}{P(X_2) \Leftrightarrow (\forall y P(y))} \gamma_{\forall} \\
 \frac{P(X_2), \forall y P(y)}{\sigma = \{X_2 \mapsto b\}} \odot_{\sigma} \quad \frac{\neg P(X_2), \neg(\forall y P(y))}{\sigma' = \{X_2 \mapsto f(b)\}} \beta_{\Leftrightarrow}
 \end{array}$$

Select Pair (Left Branch First)

$$\begin{array}{c}
 P(a) \\
 \neg P(b) \\
 \frac{\forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(b) \Leftrightarrow (\forall y P(y))} \gamma_{\forall} \\
 \frac{P(b), \forall y P(y)}{\sigma = \{X \mapsto b\}} \odot_{\sigma} \quad \frac{\frac{\frac{\neg P(b), \neg(\forall y P(y))}{\neg P(f(b))} \delta_{\neg_{\forall}}}{P(b) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(b), \forall y P(y)}{\sigma = \{X_2 \mapsto b\}} \odot_{\sigma} \quad \neg P(b), \neg(\forall y P(y))} \beta_{\Leftrightarrow} \\
 \sigma' = \{X_2 \mapsto f(b)\}
 \end{array}$$

Select Pair (Left Branch First)

$$\begin{array}{c}
 \frac{
 \frac{
 \frac{
 \frac{
 P(a) \\
 \neg P(b) \\
 \forall x. P(x) \Leftrightarrow (\forall y P(y))
 }{
 P(b) \Leftrightarrow (\forall y P(y))
 }{\gamma_{\forall}}
 }{
 P(b), \forall y P(y)
 }{\odot_{\sigma}}
 }{
 \sigma = \{X \mapsto b\}
 }
 }{
 \frac{
 \frac{
 \frac{
 \neg P(b), \neg(\forall y P(y)) \\
 \neg P(f(b))
 }{
 P(b) \Leftrightarrow (\forall y P(y))
 }{\gamma_{\forall}}
 }{
 \neg P(b), \neg(\forall y P(y))
 }{\delta_{\neg\forall}}
 }{
 \neg P(b), \neg(\forall y P(y))
 }{\beta_{\Leftrightarrow}}
 }{
 \frac{
 \frac{
 P(b), \forall y P(y) \\
 \sigma = \{X_2 \mapsto b\}
 }{\odot_{\sigma}}
 }{
 \sigma' = \{X_2 \mapsto f(b)\}
 }
 }{
 \frac{
 \frac{
 \neg P(b), \neg(\forall y P(y)) \\
 \neg P(f'(b))
 }{
 \neg P(b), \neg(\forall y P(y))
 }{\delta_{\neg\forall}}
 }{
 \neg P(b), \neg(\forall y P(y))
 }{\beta_{\Leftrightarrow}}
 }
 }
 \end{array}$$

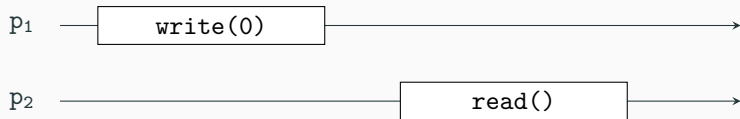
Select Pair (Left Branch First)

$$\begin{array}{c}
 \frac{P(a)}{\quad} \\
 \frac{\neg P(b)}{\quad} \\
 \frac{\forall x. P(x) \Leftrightarrow (\forall y P(y))}{P(b) \Leftrightarrow (\forall y P(y))} \gamma_{\forall} \\
 \frac{P(b), \forall y P(y)}{\sigma = \{X \mapsto b\}} \odot_{\sigma} \quad \frac{\frac{\frac{\neg P(b), \neg(\forall y P(y))}{\neg P(f(b))} \beta_{\Leftrightarrow} \quad \delta_{\neg\forall}}{P(b) \Leftrightarrow (\forall y P(y))} \gamma_{\forall}}{\frac{P(b), \forall y P(y)}{\sigma = \{X_2 \mapsto b\}} \odot_{\sigma} \quad \frac{\frac{\neg P(b), \neg(\forall y P(y))}{\neg P(f'(b))} \beta_{\Leftrightarrow} \quad \delta_{\neg\forall}}{\dots} \gamma_{\forall}}{\sigma' = \{X_2 \mapsto f(b)\}} \beta_{\Leftrightarrow}
 \end{array}$$

Sequential and Concurrent Executions

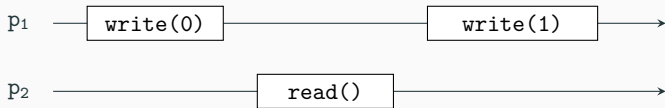


(a) Sequential execution of two operations on a resource R by the process p_1 .

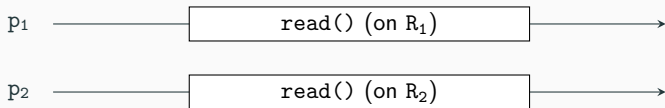


(b) Concurrent execution of two operations on a shared resource R: `write(0)` by p_1 and `read()` by p_2 .

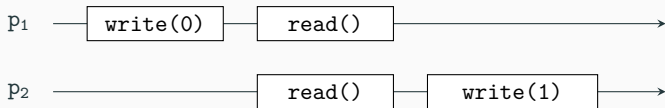
Parallelism and Concurrency



(a) *Concurrent but not parallel.*



(b) *Parallel but not concurrent.*



(c) *Concurrent and parallel.*

Interactions with the Proof-Search Procedure

Equality Reasoning

- Capture equality predicate \approx
- Extract terms that have to be equals
- BSE calculus
- New closure rule: $\neg(X \approx X)$

Integration

- Triggered when a predicate or an equality is generated
- Backtrack if the chosen solution does not fit with other branches
- Parallelization if multiple rules are applicable

Rigid E-unification Problem

A rigid E-unification problem

$$\langle E, s, t \rangle$$

consists of a finite set E of equalities of the form $(l \approx r)$ and two terms s and t such that $r, l, s, t \in \mathcal{T}$.

Constraint

An (ordering) constraint is a (finite) set of expressions of the form $s \simeq t$ or $s \succ t$ where s and t are terms. A substitution σ is a solution to a constraint \mathcal{C} if and only if :

- $\sigma(s) = \sigma(t)$ for all $s \simeq t \in \mathcal{C}$, i.e., σ is a unifier for s and t .
- $\sigma(s) > \sigma(t)$ for all $s \succ t \in \mathcal{C}$, where $>$ is an arbitrary but fixed term reduction ordering.
- σ instantiates all variables occurring in \mathcal{C} with ground terms.

Basic Rigid Superposition Rules

Right Basic Rigid Superposition Rule

Let $l \approx r$ or $r \approx l$ be an equality of E and l' is sub-term of s or t . Thus, the application of the right rigid basic superposition (*rbrs*) rule results in one of the following, regarding the term on which it is applied:

- s become $s[l' \mapsto r]$ and the constraints $l \succ r, s \succ t, l \simeq l'$ are added to C
- t become $t[l' \mapsto r]$ and the constraints $l \succ r, t \succ s, l \simeq l'$ are added to C

$$\frac{\langle E \cup \{l \approx r\}, s, t \rangle \cdot C}{\langle E \cup \{l \approx r\}, s[l' \mapsto r], t \rangle \cdot C \cup \{l \succ r, s \succ t, l \simeq l'\}} \text{rbrs}$$

Basic Rigid Superposition Rules

Left Basic Rigid Superposition Rule

Let $l \approx r$ or $r \approx l$ and $u \approx v$ or $v \approx u$ be two equalities of E . Let l' be a sub-term of u . Thus, the application of the left rigid basic superposition (*lbrs*) rule results in $u \approx v$ becoming $u_{[l' \mapsto r]} \approx v$ and the constraints $l \succ r$, $u \succ v$ and $l \simeq l'$ are added to C .

$$\frac{\langle E \cup \{l \approx r, u \approx v\}, s, t \rangle \cdot C}{\langle E \cup \{l \approx r, u_{[l' \mapsto r]} \approx v\}, s, t \rangle \cdot C \cup \{l \succ r, u \succ v, l \simeq l'\}} \textit{lbrs}$$

Example using Equality Reasoning

$$\begin{array}{l} a \approx b \\ a \approx c \\ \neg P(c, c) \\ \forall x. P(c, c) \vee \neg(x \approx c) \end{array}$$

Example using Equality Reasoning

$$\frac{\begin{array}{l} a \approx b \\ a \approx c \\ \neg P(a, b) \end{array}}{\forall x. P(c, c) \vee \neg(x \approx c)} \quad \mathcal{A}$$

$$P(c, c) \vee \neg(X \approx c)$$

Example using Equality Reasoning

$$\frac{\begin{array}{c} a \approx b \\ a \approx c \\ \neg P(c, c) \end{array}}{\forall x. P(c, c) \vee \neg(x \approx c)} \gamma_{\forall}$$
$$\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)} \beta_{\forall}$$

Example using Equality Reasoning

$$a \approx b$$

$$a \approx c$$

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

$$\frac{\forall x. P(c, c) \vee \neg(x \approx c)}{P(c, c) \vee \neg(X \approx c)} \gamma_{\forall}$$

$$\frac{P(c, c) \quad \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)} \beta_{\forall}$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c}}{\neg P(a, b)} \quad \forall x. P(c, c) \vee \neg(x \approx c)}{\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)}} \gamma_{\forall} \beta_{\forall}$$

$$\langle \{a \approx b, a \approx c\}, a, c \rangle \cdot \emptyset$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c}}{\neg P(a, b)} \quad \forall x. P(c, c) \vee \neg(x \approx c)}{P(c, c) \vee \neg(X \approx c)} \gamma_{\forall} \quad \beta_{\forall}$$
$$\frac{P(c, c) \quad \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)}$$

$$\frac{\langle \{a \approx b, a \approx c\}, a, c \rangle \cdot \emptyset}{\langle \{a \approx b, a \approx c\}, c, c \rangle \cdot \{a \succ c, a \simeq a\}} rbrs$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c}}{\neg P(a, b)} \quad \forall x. P(c, c) \vee \neg(x \approx c)}{P(c, c) \vee \neg(X \approx c)} \gamma_{\forall} \quad \beta_{\forall}$$
$$\frac{P(c, c) \quad \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)}$$

$$\frac{\langle \{a \approx b, a \approx c\}, a, c \rangle \cdot \emptyset}{\langle \{a \approx b, a \approx c\}, c, c \rangle \cdot \{a \succ c, a \simeq a\}} rbrs$$

Example using Equality Reasoning

$$a \approx b$$

$$a \approx c$$

$$\neg P(c, b)$$

$$\frac{\forall x. P(c, c) \vee \neg(x \approx c)}{P(c, c) \vee \neg(X \approx c)} \gamma_{\forall}$$

$$\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)} \beta_{\forall}$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c} \quad \neg P(c, b)}{\forall x. P(c, c) \vee \neg(x \approx c)} \gamma_{\forall}}{\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)} \beta_{\forall}}$$

$$\langle \{a \approx b, a \approx c\}, b, c \rangle \cdot \emptyset$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c} \quad \neg P(c, b)}{\forall x. P(c, c) \vee \neg(x \approx c)} \quad \gamma_{\forall}}{\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)} \quad \beta_{\forall}}$$

$$\frac{\langle \{a \approx b, a \approx c\}, b, c \rangle \cdot \emptyset}{\langle \{a \approx b, a \approx c\}, a, c \rangle \cdot \{b \succ a, b \simeq b\}} \quad rbrs$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c} \quad \neg P(c, b)}{\forall x. P(c, c) \vee \neg(x \approx c)} \gamma_{\forall}}{\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)} \beta_{\forall}}$$

$$\frac{\langle \{a \approx b, a \approx c\}, b, c \rangle \cdot \emptyset}{\langle \{a \approx b, a \approx c\}, a, c \rangle \cdot \{b \succ a, b \simeq b\}} rbrs$$

Example using Equality Reasoning

$$a \approx b$$

$$a \approx c$$

$$\neg P(c, b)$$

$$\frac{\forall x. P(c, c) \vee \neg(x \approx c)}{P(c, c) \vee \neg(X \approx c)} \gamma_{\forall}$$

$$\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c) \quad \neg(X \approx c)} \beta_{\forall}$$

$$\langle \{a \approx b, a \approx c\}, b, c \rangle \cdot \emptyset$$

$$\frac{\langle \{a \approx b, a \approx c\}, b, c \rangle \cdot \emptyset}{\langle \{a \approx b, a \approx c\}, a, c \rangle \cdot \{b \succ a, b \simeq b\}} rbrs$$

$$\frac{\langle \{a \approx b, a \approx c\}, a, c \rangle \cdot \{b \succ a, b \simeq b\}}{\langle \{a \approx b, a \approx c\}, c, c \rangle \cdot \{a \succ c, a \simeq a, b \succ a, b \simeq b\}} rbrs$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c}}{\neg P(c, c)} \quad \forall x. P(c, c) \vee \neg(x \approx c)}{\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c)} \quad \neg(X \approx c)} \quad \begin{array}{l} \gamma_V \\ \beta_V \end{array} \quad \odot$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c}}{\neg P(c, c)}}{\frac{\forall x. P(c, c) \vee \neg(x \approx c)}{P(c, c) \vee \neg(c \approx c)} \gamma_{\forall}} \beta_{\forall} \frac{P(c, c)}{\neg(X \approx c)} \odot$$

$$\neg(X \approx c)$$

Example using Equality Reasoning

$$\frac{\frac{\frac{a \approx b}{a \approx c} \quad \neg P(c, c)}{\forall x. P(c, c) \vee \neg(x \approx c)} \gamma_{\forall}}{\frac{P(c, c) \vee \neg(X \approx c)}{P(c, c)} \beta_{\forall}} \beta_{\forall}$$
$$\frac{\frac{P(c, c)}{\odot} \quad \frac{\neg(\mathbf{c} \approx \mathbf{c})}{\odot}}{\odot} \odot$$

$$\frac{\neg(X \approx c)}{\{X \mapsto c\}} \odot$$

Reasoning Modulo Theory

Simple Set Theory

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

$$A_1 \wedge A_2 \wedge \neg C$$

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

Reasoning Modulo Theory

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

α_{\wedge}
 $\delta_{\neg \forall}$
 $\delta_{\neg \forall}$
 β_{\Leftrightarrow}
 σ
 $\delta_{\neg \forall}$
 \odot

Reasoning Modulo Theory

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

Deduction Modulo Theory (DMT)

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

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \rightarrow A \subseteq B \wedge B \subseteq A$$

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

\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

Proof Tree and Segments

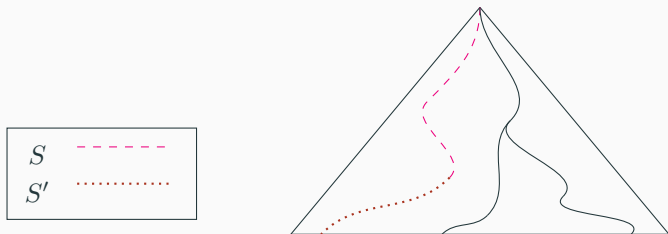


Figure 8: S is an initial segment, S' is a branch, and $S \sqsubseteq S'$.

Mapping

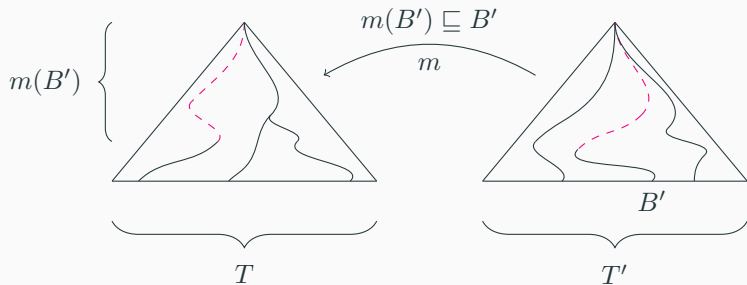


Figure 9: The branch B' is mapped to the initial segment $m(B')$, which means B' contains at least all the formulas of $m(B')$.

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 in 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