Design of Tableau-Based Automated Theorem Provers and Production of Machine-Chekable Proofs

Julie Cailler

Chair of Theoretical Computer Science
University of Regensburg
Germany

Universität Regensburg

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
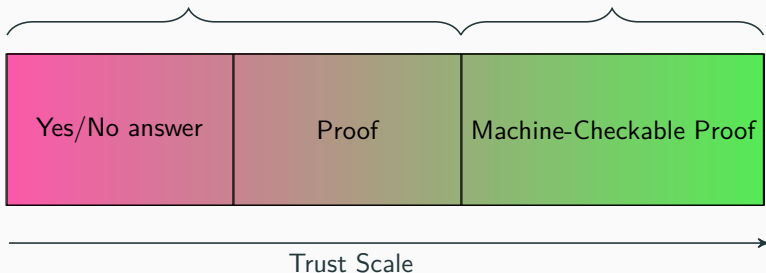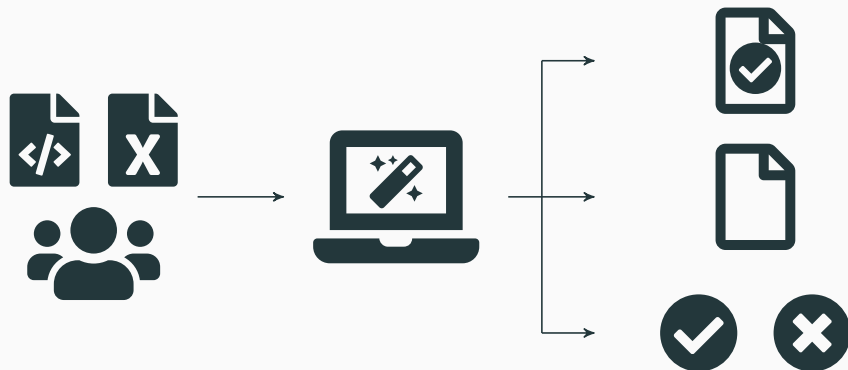
Proofs

Automated Theorem Proving

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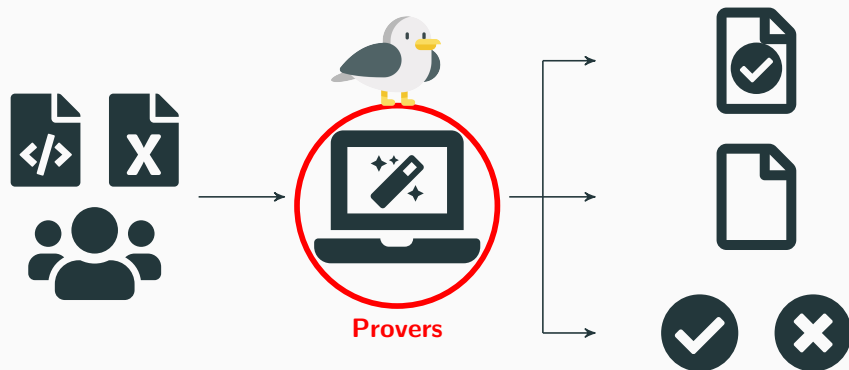
Interactive Theorem Proving

- Proof assistants
- Guide humans towards proofs
- Proofs are machine-checkable and certified

| Yes/No answer | Proof | Machine-Checkable Proof |

Trust Scale

Big Picture

Big Picture

Provers

1. Preliminary Notions

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

$$\cfrac{\cfrac{\cfrac{\neg(\exists x.\ P(x) \Rightarrow (P(a) \wedge P(b)))}{\neg(P(a) \Rightarrow (P(a) \wedge P(b)))}\ \gamma_{\neg\exists}}{P(a), \neg(P(a) \wedge P(b))}\ \alpha_{\neg\Rightarrow}}{\cfrac{\neg P(a)}{\odot}\ \odot \qquad \cfrac{\cfrac{\cfrac{\neg P(b)}{\neg(P(b) \Rightarrow (P(a) \wedge P(b)))}\ \gamma_{\neg\exists}}{P(b), \neg(P(a) \wedge P(b))}\ \alpha_{\neg\Rightarrow}}{\odot}\ \odot}\ \beta_{\neg\wedge}$$

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 (local & global)

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

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions (local & global)

$$\frac{Human(Socrates)}{\neg Human(X)} \gamma_\forall$$

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 (local & global)

$$\cfrac{\cfrac{\begin{array}{c} Human(Socrates) \\ \forall x. \neg Human(x) \end{array}}{\neg Human(\textcolor{red}{Socrates})} \gamma_\forall}{\sigma = \{\textcolor{red}{X} \mapsto Socrates\}} \odot_\sigma$$

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 (local & global)

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

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 (local & global)

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

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 (local & global)

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

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 (local & global)

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

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 (local & global)

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

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 (local & global)

$$\cfrac{\cfrac{\cfrac{\neg(\exists x.\ P(x) \Rightarrow (P(a) \land P(b)))}{\neg(P(X) \Rightarrow (P(a) \land P(b)))}\ \gamma_\forall}{P(X), \neg(P(a) \land P(b))}\ \alpha_{\neg\Rightarrow}}{\neg P(a) \qquad\qquad\qquad \neg P(b)}\ \beta_{\neg\land}$$

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 (local & global)

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

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 (local & global)

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

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 (local & global)

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

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions (local & global)

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

Tableau-Based Proof-Search Procedure

Rules

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

Tableaux in AR

- Free variables
- Substitutions (local & global)

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

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 (local & global)

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

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 (local & global)

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

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

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

Fariness 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

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

Select Pair and Select Mode

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

Select Pair and Select Mode

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

Select Pair and Select Mode

$$\cfrac{\cfrac{\neg P(a)}{\cfrac{\neg Q(b)}{\cfrac{\neg S(c)}{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(X) \lor Q(X), \forall y.\ S(X)}\ \gamma_\forall}}}}{P(X), \forall y.\ S(X) \qquad\qquad Q(X), \forall y.\ S(X)}\ \beta_\Leftrightarrow$$

Select Pair and Select Mode

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

Select Pair and Select Mode

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$

$$\cfrac{\cfrac{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(a) \lor Q(a), \forall y.\ S(a)}\ \gamma_\forall}{\cfrac{P(a), \forall y.\ S(a)}{\sigma = \{X \mapsto a\}}\ \odot_\sigma \qquad Q(a), \forall y.\ S(a)}}{}\ \beta_\Leftrightarrow$$

Select Pair and Select Mode

$$\cfrac{\cfrac{\cfrac{\cfrac{\neg P(a)}{\neg Q(b)} \atop \cfrac{\neg S(c)}{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}}{P(a) \lor Q(a), \forall y.\ S(a)} \gamma_\forall}{\cfrac{P(a), \forall y.\ S(a)}{\sigma = \{X \mapsto a\}} \odot_\sigma \qquad \cfrac{Q(a), \boxed{\forall y.\ S(a)}}{S(a)} \gamma_\forall}{\ } \beta_\Leftrightarrow}$$

Select Pair and Select Mode

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$

$$\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(a) \lor Q(a), \forall y.\ S(a)}\ \gamma_\forall$$

$$\cfrac{\cfrac{P(a), \forall y.\ S(a)}{\sigma = \{X \mapsto a\}}\ \odot_\sigma \qquad \cfrac{\cfrac{Q(a), \forall y.\ S(a)}{\cfrac{S(a)}{P(X_2) \lor Q(X_2), \forall y.\ S(X_2)}\ \gamma_\forall}\ \gamma_\forall}{}}{}\ \beta_\Leftrightarrow$$

Select Pair and Select Mode

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(a) \lor Q(a), \forall y.\ S(a)}\ \gamma_\forall$$

$$\cfrac{P(a), \forall y.\ S(a)}{\sigma = \{X \mapsto a\}}\ \odot_\sigma \qquad \cfrac{\cfrac{Q(a), \forall y.\ S(a)}{\cfrac{S(a)}{\cfrac{P(X_2) \lor Q(X_2), \forall y.\ S(X_2)}{P(X_2), \forall y.\ S(X_2) \qquad Q(X_2), \forall y.\ S(X_2)}\ \beta_\lor}\ \gamma_\forall}\ \gamma_\forall}\ \beta_\Leftrightarrow$$

Select Pair and Select Mode

$$\cfrac{\cfrac{\cfrac{\cfrac{\neg P(a)}{\neg Q(b)}}{\cfrac{\neg S(c)}{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(a) \lor Q(a), \forall y.\ S(a)}\ \gamma_\forall}}}{\cfrac{P(a), \forall y.\ S(a)}{\sigma = \{X \mapsto a\}}\ \odot_\sigma \qquad \cfrac{\cfrac{Q(a), \forall y.\ S(a)}{S(a)}\ \gamma_\forall}{\cfrac{P(X_2) \lor Q(X_2), \forall y.\ S(X_2)}{\cfrac{P(X_2), \forall y.\ S(X_2) \qquad Q(X_2), \forall y.\ S(X_2)}{\cdots \qquad\qquad \cdots}\ \beta_\lor}\ \gamma_\forall}}\ \beta_\Leftrightarrow}$$

Select Pair and Select Mode

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\forall x.\ (P(x) \vee Q(x)) \wedge \forall y.\ S(x)$$

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

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

Select Pair and Select Mode

$$\cfrac{\cfrac{\cfrac{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(X) \lor Q(X), \forall y.\ S(X)}\ \gamma_\forall}{\cfrac{P(X), \forall y.\ S(X)}{S(X)}\ \gamma_\forall \qquad Q(X), \forall y.\ S(X)}\ \beta_\Leftrightarrow}{}}{}$$

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$

Select Pair and Select Mode

$$\neg P(a)$$
$$\neg Q(b)$$
$$\boxed{\neg S(c)}$$

$$\cfrac{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(X) \lor Q(X), \forall y.\ S(X)}\ \gamma_\forall}{\cfrac{P(X), \forall y.\ S(X)}{\cfrac{\boxed{S(X)}}{\sigma = \{X \mapsto c\}}\ \odot_\sigma}\ \gamma_\forall \qquad Q(X), \forall y.\ S(X)}\ \beta_\Leftrightarrow$$

Select Pair and Select Mode

$$\cfrac{\cfrac{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(c) \lor Q(c), \forall y.\ S(c)}\ \gamma_\forall}{\cfrac{P(c), \forall y.\ S(c)}{\cfrac{S(c)}{\sigma = \{X \mapsto c\}}\ \odot_\sigma}\ \gamma_\forall \qquad Q(c), \forall y.\ S(c)}}{\quad} \beta_\Leftrightarrow$$

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$

Select Pair and Select Mode

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{\cfrac{P(c) \lor Q(c), \forall y.\ S(c)}{\cfrac{P(c), \forall y.\ S(c)}{\cfrac{S(c)}{\sigma = \{X \mapsto c\}}\ \odot_\sigma}\ \gamma_\forall \qquad \cfrac{Q(c), \forall y.\ S(c)}{S(c)}\ \gamma_\forall}\ \beta_\Leftrightarrow}\ \gamma_\forall$$

Select Pair and Select Mode

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$

$$\cfrac{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(c) \lor Q(c), \forall y.\ S(c)}\ \gamma_\forall}{\cfrac{\cfrac{P(c), \forall y.\ S(c)}{\cfrac{S(c)}{\sigma = \{X \mapsto c\}}\ \odot_\sigma}\ \gamma_\forall \qquad \cfrac{Q(c), \forall y.\ S(c)}{\cfrac{S(c)}{\odot}\ \odot_\sigma}\ \gamma_\forall}{}\ \beta_\Leftrightarrow}$$

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
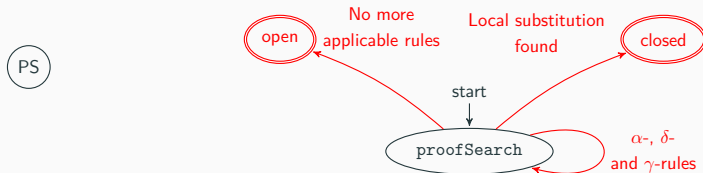
New Challenges

- Free variable dependency
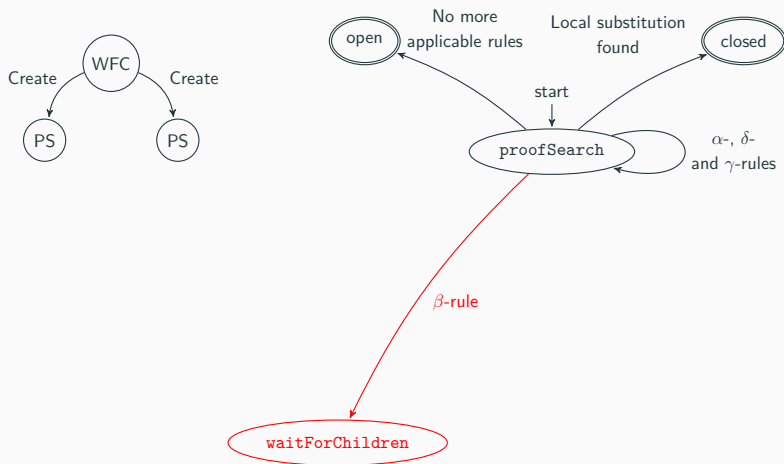- Communication between branches
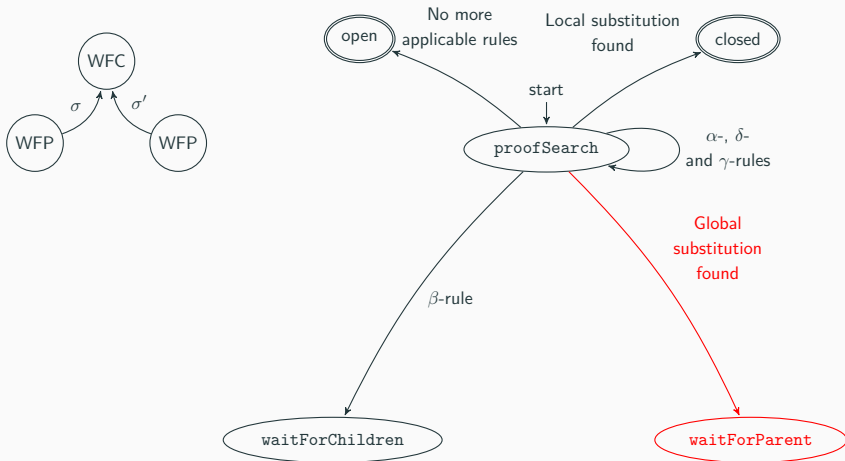
Procedures Interactions
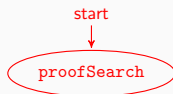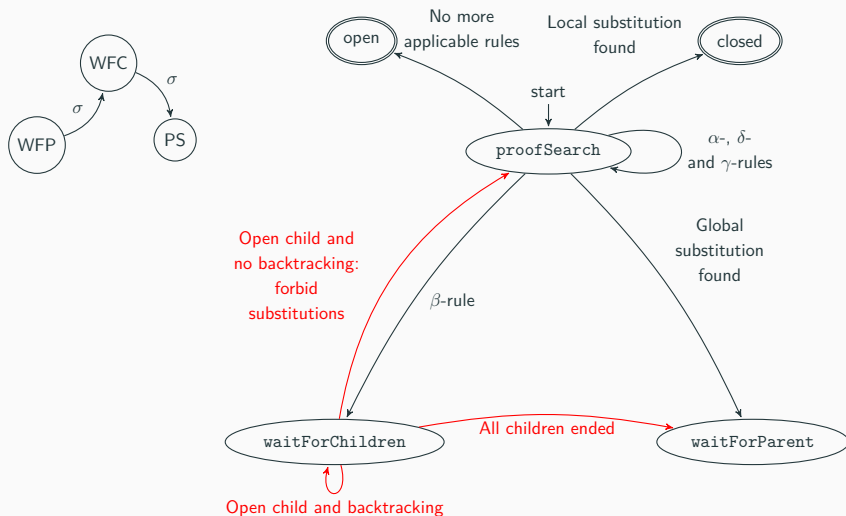
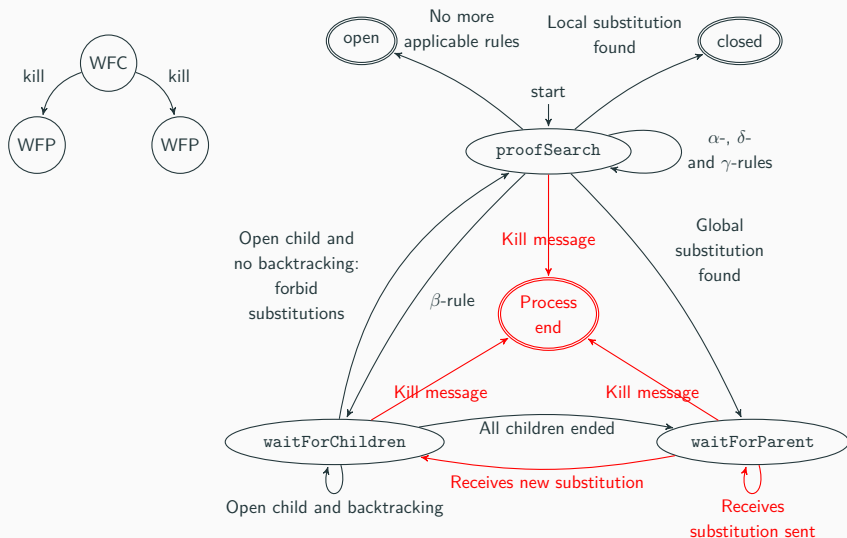# Procedures Interactions

Procedures Interactions

Procedures Interactions

Procedures Interactions

Procedures Interactions

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\forall x.\ (P(x) \vee Q(x)) \wedge \forall y.\ S(x)$$

Solving Fairness Issues with Concurrency

$$\frac{\neg P(a) \\ \neg Q(b) \\ \neg S(c) \\ \forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(X) \lor Q(X), \forall y.\ S(X)}\ \gamma_\forall$$

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\cfrac{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(X) \lor Q(X), \forall y.\ S(X)}\ \gamma_\forall}{P(X), \forall y.\ S(X) \qquad Q(X), \forall y.\ S(X)}\ \beta_\Leftrightarrow$$

Solving Fairness Issues with Concurrency

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

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

Solving Fairness Issues with Concurrency

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

$$\cfrac{\cfrac{P(X), \forall y.\ S(X)}{\odot}}{\qquad}\ \cfrac{Q(X), \forall y.\ S(X)}{\odot}\ \beta_\Leftrightarrow$$

$$\odot_\sigma \qquad \qquad \odot_\sigma$$

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

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\cfrac{\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(X) \lor Q(X),\ \forall y.\ S(X)}\ \gamma_\forall}{P(a),\ \forall y.\ S(a) \qquad Q(a),\ \forall y.\ S(a)}\ \beta_\Leftrightarrow$$

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

Solving Fairness Issues with Concurrency

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

$$\frac{P(a), \forall y.\ S(a) \qquad\qquad Q(a), \forall y.\ S(a)}{}\ \beta_\Leftrightarrow$$

$$\frac{}{\odot}\ \odot_\sigma$$

Closed

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\frac{\forall x. \ (P(x) \lor Q(x)) \land \forall y. \ S(x)}{P(X) \lor Q(X), \forall y. \ S(X)} \ \gamma_\forall$$

$$\frac{\dfrac{P(a), \forall y. \ S(a)}{\odot} \quad \odot_\sigma \qquad \dfrac{Q(a), \boxed{\forall y. \ S(a)}}{S(a)} \ \gamma_\forall}{} \ \beta_\Leftrightarrow$$

Solving Fairness Issues with Concurrency

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

$$\cfrac{\cfrac{P(a), \forall y.\ S(a)}{\odot}\ \odot_\sigma \qquad \cfrac{Q(a), \forall y.\ S(a)}{\cfrac{S(a)}{\cdots}\ \gamma_\forall}}{}\ \beta_\Leftrightarrow$$

Open

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\frac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(X) \lor Q(X), \forall y.\ S(X)}\ \gamma_\forall$$

$$\frac{}{P(b), \forall y.\ S(b) \qquad\qquad Q(b), \forall y.\ S(b)}\ \beta_\Leftrightarrow$$

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

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)$$
$$\frac{}{P(X) \lor Q(X), \forall y.\ S(X)} \gamma_\forall$$

$$\frac{P(b), \forall y.\ S(b) \qquad\qquad Q(b), \forall y.\ S(b)}{} \beta_\Leftrightarrow$$

$$\odot \qquad \odot_\sigma$$

Closed

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\cfrac{\cfrac{\cfrac{\forall x. \ (P(x) \lor Q(x)) \land \forall y. \ S(x)}{P(X) \lor Q(X), \forall y. \ S(X)} \ \gamma_\forall}{\cfrac{P(b), \forall y. \ S(b)}{S(b)} \ \gamma_\forall \qquad \cfrac{Q(b), \forall y. \ S(b)}{\odot} \ \odot} \ \beta_\Leftrightarrow}{} \ \odot_\sigma$$

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\boxed{\neg Q(a)}$$
$$\neg S(c)$$

$$\dfrac{\forall x.\ (P(x) \vee Q(x)) \wedge \forall y.\ S(x)}{P(X) \vee Q(X), \forall y.\ S(X)}\ \gamma_\forall$$

$$\dfrac{\dfrac{P(b), \forall y.\ S(b)}{S(b)}\ \gamma_\forall \qquad \dfrac{Q(b), \forall y.\ S(b)}{\odot}\ \odot_\sigma}{}\ \beta_\Leftrightarrow$$

$$\cdots$$

Open

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$

$$\cfrac{\cfrac{\forall x.\ (P(x) \vee Q(x)) \wedge \forall y.\ S(x)}{P(X) \vee Q(X), \forall y.\ S(X)}\ \gamma_\forall}{\cfrac{P(X), \forall y.\ S(X)}{S(X)}\ \gamma_\forall \qquad \cfrac{Q(X), \forall y.\ S(X)}{S(X)}\ \gamma_\forall}\ \beta_\Leftrightarrow$$

Solving Fairness Issues with Concurrency

Solving Fairness Issues with Concurrency

$$\neg P(a)$$
$$\neg Q(b)$$
$$\neg S(c)$$
$$\cfrac{\forall x.\ (P(x) \lor Q(x)) \land \forall y.\ S(x)}{P(c) \lor Q(c), \forall y.\ S(c)}\ \gamma_\forall$$

$$\cfrac{\cfrac{P(c), \forall y.\ S(c)}{\cfrac{S(c)}{\odot}\ \odot_\sigma}\ \gamma_\forall \qquad \cfrac{Q(c), \forall y.\ S(c)}{\cfrac{S(c)}{\odot}\ \odot_\sigma}\ \gamma_\forall}{}\ \beta_\Leftrightarrow$$

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

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

Goéland Tool

Functionnalities

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

Goéland Tool

Implementation

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

OS thread			OS thread			
Go	Go	Go	Go	Go	Go	Go
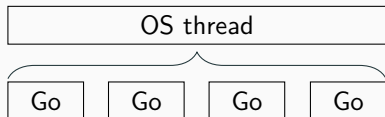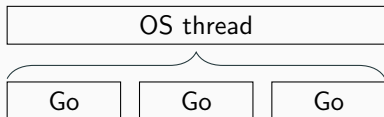
Theory Reasoning

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

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

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

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

(a) Outer Skolemization tableau.

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

(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

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

(a) Outer Skolemization tableau proof.

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

(b) Equivalent GS3.

Outer Skolemisation

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

(a) Inner Skolemization tableau proof.

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

(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 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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

$$\frac{\dfrac{\dfrac{\dfrac{\rule{3cm}{0.4pt}}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)), \neg D(c) \vdash}\ \neg\exists}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(\forall y\ D(y)) \vdash}\ \neg\forall}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)), D(c), \neg(\forall y\ D(y)) \vdash}\ \mathsf{W} \times 2}{\dfrac{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y)), \neg(D(c) \Rightarrow \forall y\ D(y)) \vdash}{\neg(\exists x.\ D(x) \Rightarrow \forall y\ D(y))}\ \neg\exists}\ \neg\Rightarrow$$

Example

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

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

Example

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

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

Example

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

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

Example

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

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

Example

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

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

with the **ax** rule applied at the top.

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 generic 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
- Modular and generic prover

Theory Reasoning

- Improvements of DMT (term rewriting, narrowing, manually designed rewrite rules)
- More experiments on polymorphic problems
- SMT solvers: string equations, quantum circuits

Proof Certification

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

Thank you! ☺

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

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

Reasoning Methods in FOL

Resolution

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

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

$\quad \{\neg A\}$

$\quad \{A \vee A\}$

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

Tableaux

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

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

Reasoning Methods in FOL

Resolution

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

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

$$\{\neg A\}$$

$$\{A \vee A\} \longrightarrow \{A\}$$

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

Tableaux

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

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

Reasoning Methods in FOL

Resolution

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

Tableaux

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

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

$$\{\neg A\} \underline{\hspace{4cm}} \{\}$$

$$\{A \vee A\} \underline{\hspace{1cm}} \{A\}$$
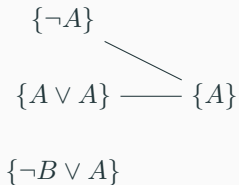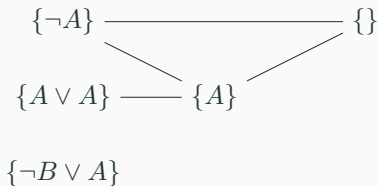
$$\{\neg B \vee A\}$$

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

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

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

$$\dfrac{\dfrac{(P(a) \wedge \neg P(a)) \vee \bot}{\dfrac{P(a) \wedge P(a)}{\dfrac{P(a), \neg P(a)}{\odot} \odot} \alpha_\wedge} \quad \dfrac{\bot}{\cdots} \beta_\vee}{}$$

(b) Incompleteness caused by an unfair *select branch*.

$$\frac{\dfrac{\begin{array}{c} P(a) \wedge \neg P(a) \\ \hline \forall x \ Q(X) \end{array}}{P(a), \neg P(a)} \ \alpha_\wedge}{\odot} \ \odot$$

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

$$\frac{\dfrac{\dfrac{\begin{array}{c} P(a) \wedge \neg P(a) \\ \hline \forall x \ Q(X) \end{array}}{Q(X)} \ \gamma_\forall}{Q(X')} \ \gamma_\forall}{\cdots} \ \gamma_\forall$$

(b) Incompleteness caused by an unfair *select formula*.

Select Pair (Right Branch First)

$$P(a)$$
$$\neg P(b)$$
$$\forall x.\ P(x) \Leftrightarrow (\forall y\ P(y))$$

Select Pair (Right Branch First)

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

Select Pair (Right Branch First)

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

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

Select Pair (Right Branch First)

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

$$\frac{P(a), \forall y\ P(y) \qquad \dfrac{\neg P(a), \neg(\forall y\ P(y))}{\sigma = \{X \mapsto a\}}\ \odot_\sigma}{}\ \beta_\Leftrightarrow$$

Select Pair (Right Branch First)

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

Select Pair (Right Branch First)

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

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

Select Pair (Right Branch First)

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

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

Select Pair (Left Branch First)

$$P(a)$$
$$\neg P(b)$$
$$\forall x.\ P(x) \Leftrightarrow (\forall y\ P(y))$$

Select Pair (Left Branch First)

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

Select Pair (Left Branch First)

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

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

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

Select Pair (Left Branch First)

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

$$\frac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma \qquad\qquad \neg P(b), \neg(\forall y\ P(y))}\ \beta_\Leftrightarrow$$

$$P(a)$$
$$\neg P(b)$$
$$\cfrac{\forall x. \; P(x) \Leftrightarrow (\forall y \; P(y))}{P(b) \Leftrightarrow (\forall y \; P(y))} \; \gamma_\forall$$

$$\cfrac{\cfrac{P(b), \forall y \; P(y)}{\sigma = \{X \mapsto b\}} \; \odot_\sigma \qquad\qquad \cfrac{\neg P(b), \boxed{\neg(\forall y \; P(y))}}{\neg P(f(b))} \; \delta_{\neg\forall}}{} \; \beta_\Leftrightarrow$$

Select Pair (Left Branch First)

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

$$\frac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma \qquad\qquad \frac{\dfrac{\neg P(b), \neg(\forall y\ P(y))}{\dfrac{\neg P(f(b))}{P(X_2) \Leftrightarrow (\forall y\ P(y))}\ \delta_{\neg\forall}}\ \gamma_\forall}{}\ \beta_\Leftrightarrow$$

Select Pair (Left Branch First)

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

$$\cfrac{\cfrac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma \qquad \cfrac{\cfrac{\cfrac{\neg P(b), \neg(\forall y\ P(y))}{\neg P(f(b))}\ \delta_{\neg\forall}}{P(X_2) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall}{P(X_2), \forall y\ P(y) \qquad \neg P(X_2), \neg(\forall y\ P(y))}\ \beta_\Leftrightarrow}{\ }\ \beta_\Leftrightarrow$$

Select Pair (Left Branch First)

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

$$\cfrac{\forall x.\ P(x) \Leftrightarrow (\forall y\ P(y))}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall$$

$$\cfrac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma$$

$$\cfrac{\cfrac{\cfrac{\neg P(b), \neg(\forall y\ P(y))}{\neg P(f(b))}\ \delta_{\neg\forall}}{P(X_2) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall}{\cfrac{P(X_2), \forall y\ P(y)}{\sigma = \{X_2 \mapsto b\}}\ \odot_\sigma \qquad \neg P(X_2), \neg(\forall y\ P(y))}\ \beta_\Leftrightarrow$$

$$\sigma' = \{X_2 \mapsto f(b)\}$$

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

$$\cfrac{\forall x.\ P(x) \Leftrightarrow (\forall y\ P(y))}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall$$

$$\cfrac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma$$

$$\cfrac{\cfrac{\cfrac{\neg P(b), \neg(\forall y\ P(y))}{\neg P(f(b))}\ \delta_{\neg\forall}}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall}{\cfrac{P(b), \forall y\ P(y)}{\sigma = \{X_2 \mapsto b\}}\ \odot_\sigma \qquad \neg P(b), \neg(\forall y\ P(y))}\ \beta_\Leftrightarrow$$

$$\sigma' = \{X_2 \mapsto f(b)\}$$

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

$$\cfrac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma$$

$$\cfrac{\cfrac{\neg P(b), \neg(\forall y\ P(y))}{\neg P(f(b))}\ \delta_{\neg\forall}}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall$$

$$\cfrac{P(b), \forall y\ P(y)}{\sigma = \{X_2 \mapsto b\}}\ \odot_\sigma \qquad \cfrac{\neg P(b), \neg(\forall y\ P(y))}{\neg P(f'(b))}\ \delta_{\neg\forall}$$
$$\sigma' = \{X_2 \mapsto f(b)\}$$

Select Pair (Left Branch First)

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

$$\frac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma$$

$$\frac{\neg P(b), \neg(\forall y\ P(y))}{\frac{\neg P(f(b))}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall}\ \delta_{\neg\forall}$$
$$\beta_\Leftrightarrow$$

$$\frac{P(b), \forall y\ P(y)}{\sigma = \{X_2 \mapsto b\}}\ \odot_\sigma \qquad \frac{\neg P(b), \neg(\forall y\ P(y))}{\frac{\neg P(f'(b))}{\cdots}\ \gamma_\forall}\ \delta_{\neg\forall}$$
$$\beta_\Leftrightarrow$$
$$\sigma' = \{X_2 \mapsto f(b)\}$$

Sequential and Concurrent Executions

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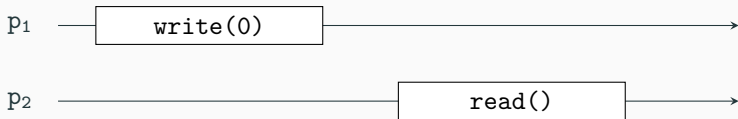
(b) Concurrent execution of two operations on a shared resource R: write(0) by p_1 and read() by p_2.

Parallelism and Concurrency
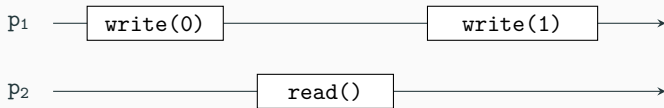
(a) *Concurrent* but not *parallel*.
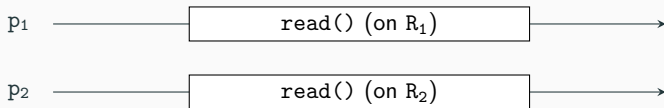
(b) *Parallel* but not *concurrent*.
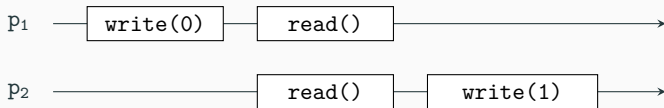
(c) *Concurrent* and *parallel*.

Equality Reasoning

- Capture equality predicate $\approx$
- Extract terms that have to be equals
- $\mathcal{BSE}$ 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

$\mathcal{BSE}$-**Calculus**

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 $r, l, s, t \in \mathscr{T}$.

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 an 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

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

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.

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

Example using Equality Reasoning

$$a \approx b$$
$$a \approx c$$
$$\neg P(c, c)$$
$$\forall x. \ P(c, c) \vee \neg(x \approx c)$$

Example using Equality Reasoning

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

Example using Equality Reasoning

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

Example using Equality Reasoning

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

Example using Equality Reasoning

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

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

Example using Equality Reasoning

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

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

Example using Equality Reasoning

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

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

Example using Equality Reasoning

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

$$\cfrac{\cfrac{\forall x.\ P(c,c) \vee \neg(x \approx c)}{\cfrac{P(c,c) \vee \neg(X \approx c)}{\boldsymbol{P(c,c)} \qquad \neg(X \approx c)}\ \beta_\vee}\ \gamma_\forall}{}$$

Example using Equality Reasoning

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

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

Example using Equality Reasoning

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

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

Example using Equality Reasoning

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

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

Example using Equality Reasoning

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

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

Example using Equality Reasoning

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

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

$$\odot$$

Example using Equality Reasoning

$$a \approx b$$
$$a \approx c$$
$$\neg P(c,c)$$
$$\cfrac{\cfrac{\forall x.\ P(c,c) \vee \neg(x \approx c)}{\cfrac{P(c,c) \vee \neg(\textcolor{red}{c} \approx c)}{\cfrac{P(c,c)}{\odot}\ \odot \qquad \neg(\boldsymbol{X \approx c})}\ \beta_\vee}\ \gamma_\forall}{}$$

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

Example using Equality Reasoning

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

$$\cfrac{\forall x.\ P(c, c) \vee \neg(x \approx c)}{\cfrac{P(c, c) \vee \neg(X \approx c)}{\cfrac{P(c, c)}{\odot}\ \odot \qquad \cfrac{\neg(\textcolor{red}{c \approx c})}{\odot}\ \odot}\ \beta_\vee}\ \gamma_\forall$$

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

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: $\forall a.\ a \subseteq a$

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

$$(\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b)$$
$$\wedge\ (\forall a, b.\ a = b \Leftrightarrow a \subseteq b \wedge b \subseteq a)$$
$$\wedge\ \neg(\forall a.\ a \subseteq a)$$

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

Reasoning Modulo Theory

$$\frac{(\forall a,b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b) \wedge (\forall a,b.\ a = b \Leftrightarrow a \subseteq b \wedge b \subseteq a) \wedge \neg(\forall a.\ a \subseteq a)}{\forall a,b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b,\ \forall a,b.\ a = b \Leftrightarrow a \subseteq b \wedge b \subseteq a,}\ \alpha_\wedge$$

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

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

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

$$\frac{\neg(s \in a \Rightarrow s \in a)}{\neg(s \in a),\ (s \in a)}\ \delta_{\neg\forall}$$

$$\frac{\neg(s \in a),\ (s \in a)}{\odot}\ \alpha_{\neg\Rightarrow}$$

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

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

$$A = B \to A \subseteq B \land B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \to A \subseteq B \land B \subseteq A$$

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

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

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

$$A = B \to A \subseteq B \land B \subseteq A$$

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

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

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

$$A = B \to A \subseteq B \land B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \to A \subseteq B \land B \subseteq A$$

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

Deduction Modulo Theory (DMT)

Rewrite Rules

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

$$A = B \to A \subseteq B \land B \subseteq A$$

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

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

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** $(+9)$

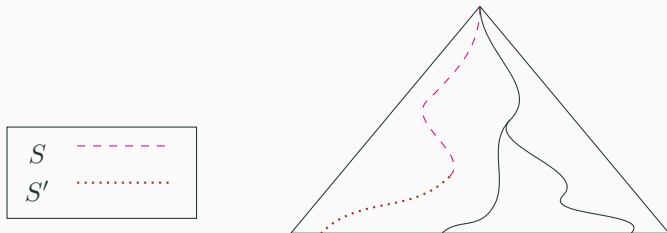**Table 2:** Scale-up experimental results of Goéland+DMT.

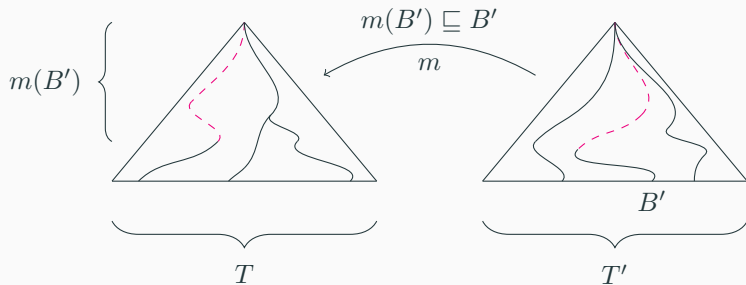**Figure 8:** S is an initial segment, S' is a branch, and $S \sqsubseteq S'$.

Mapping

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

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