Formal Methods

The Art of Using Logic to Build Safer Systems

Julie Cailler

May 25, 2023

MaREL Team, LIRMM, University of Montpellier, CNRS, France

What are Formal Methods?

Definition & Goal

Definition

In computer science, formal methods are mathematically rigorous techniques for the specification, development, analysis, and verification of software and hardware systems.

In a nutshell

- Prevent bugs
- Safer software
- Like the tests, but better
- Money and time consuming

Bugs

- Ariane 5 — ESA
- 1996
- Explosion 36,7 second after launch
- Integer overflow
- US$370 million

- Pentium FDIV — Intel
- 1994
- Recall the processors
- Error in the floating point — returns the wrong value for some calculations
- US$475 million

Verified Systems

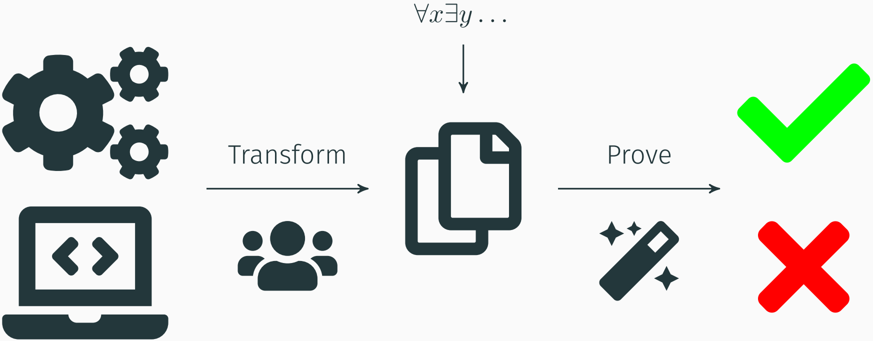
- Metro line 14
- 1998
- Fully automated
- Use of the B method — Set theory
- Simens

- JavaCard
- Run Java-based application on smart cards
- Certified architecture using Coq
- Thales (Gemalto)

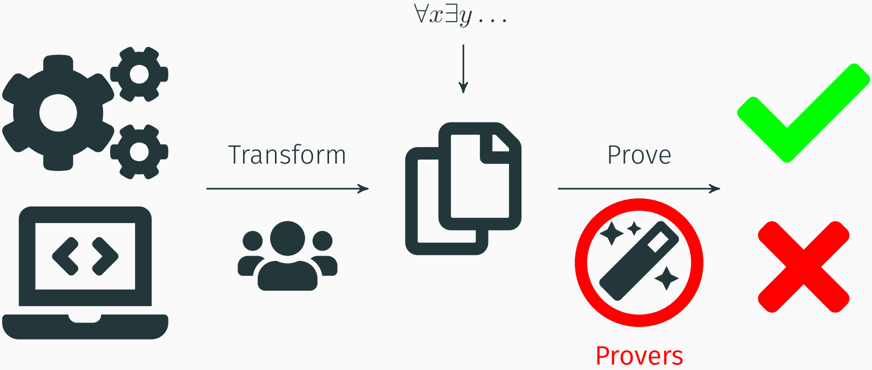
- CompCert
- Certified compiler for the C language
- Correspondence source code – compiled code
- Developed and certified correct in Coq
- INRIA & AbsInt

How to Make a Proof?

From Program to Proof



From Program to Proof



ITP and ATP

Interactive Theorem Proving

- Proof assistant
- Guides humans towards proof
- Proof are certified correct

Automated Theorem Proving

- Click-and-proof software
- Searching for a proof all by themselves
- Output a proof or the status of the formula

Vampire E LeoIII
Princess IProver
cvc5

Method of Analytics Tableaux

Principle

- A set of axioms and one conjecture
- Refutation : proof that the negation of the conjecture is unsatisfiable
- Apply rules : $\odot \prec \alpha \prec \delta \prec \beta \prec \gamma$
- Goal: close all the branches

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

$\odot$-rules

- Closes a branch
- Special symbols $\top$ and $\bot$
- Contradiction between two unifiable terms

$$\frac{\bot}{\odot}\ \odot_{\bot} \qquad \frac{\neg\top}{\odot}\ \odot_{\neg\top}$$

$$\frac{P, \neg P}{\odot}\ \odot \qquad \frac{P, \neg Q}{\sigma}\ \odot_{\sigma}$$

$$s.t.\ \sigma(P) = \sigma(Q)$$

α-rules

- Breaks the connector

$$\frac{\neg\neg P}{P}\,\alpha_{\neg\neg} \qquad \frac{\neg(P \vee Q)}{\neg P, \neg Q}\,\alpha_{\neg\vee}$$

$$\frac{P \wedge Q}{P, Q}\,\alpha_{\wedge} \qquad \frac{\neg(P \Rightarrow Q)}{P, \neg Q}\,\alpha_{\neg\Rightarrow}$$

β-rules

- Creates (at least) two branches

$$\frac{P \lor Q}{P \qquad Q}\ \beta_{\lor}$$

$$\frac{\neg(P \land Q)}{\neg P \qquad \neg Q}\ \beta_{\neg\land}$$

$$\frac{P \Rightarrow Q}{\neg P \qquad Q}\ \beta_{\Rightarrow}$$

$$\frac{P \Leftrightarrow Q}{P, Q \qquad \neg P, \neg Q}\ \beta_{\Leftrightarrow}$$

$$\frac{\neg(P \Leftrightarrow Q)}{\neg P, Q \qquad P, \neg Q}\ \beta_{\Leftrightarrow}$$

γ-rules

- x is universally quantified variable, X is a metavariable (or free variable)
- Used as a placeholder, waiting for an instantiation

$$\frac{\forall x\ P(x)}{P[x := X]}\ \gamma_{\forall M} \qquad \frac{\neg\exists x\ P(x)}{\neg P[x := X]}\ \gamma_{\neg\exists M}$$

δ-rules

- x is an existentially quantified variable
- f is a new Skolem term: constant or function symbol with the branch's metavariables $\vec{y}$ in parameter ($f(X, Y)$, $f(X)$, ...)

$$\frac{\exists x\ P(x)}{P[x := f(\vec{y})]}\ \delta_{\exists} \qquad \frac{\neg\forall x\ P}{\neg P[x := f(\vec{y})]}\ \delta_{\neg\forall}$$

A Concurrent Proof-Search Procedure

Context

Method of analytic tableaux

- Gives a proof
- Uses free variables
- Usually managed sequentially

Fair proof search is difficult!

- Shared free variables
- Find a substitution for the whole tree
- Completeness issues: branch selection, free variables reintroduction

Motivating Example

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

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

Motivating Example

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

$$\dfrac{P(a), \neg P(b), \boldsymbol{\forall x \; (P(x) \Leftrightarrow (\forall y \; P(y)))}}{P(X) \Leftrightarrow (\forall y \; P(y))} \; \gamma\forall$$

Motivating Example

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

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

Motivating Example

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

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

Motivating Example

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

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

Motivating Example

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

$$\dfrac{\dfrac{P(a), \neg \boldsymbol{P(b)}, \forall x \; (P(x) \Leftrightarrow (\forall y \; P(y)))}{P(\textcolor{red}{a}) \Leftrightarrow (\forall y \; P(y))}\;\gamma_\forall}{\dfrac{\dfrac{P(\textcolor{red}{a}), \forall y \; P(y)}{\boldsymbol{P(\textcolor{red}{b})}}\;\gamma_\forall}{\boldsymbol{\sigma = \{Y \mapsto b\}}}\;\odot_\sigma \qquad \dfrac{\neg P(\textcolor{red}{a}), \neg(\forall y \; P(y))}{\sigma = \{X \mapsto a\}}\;\odot_\sigma}\;\beta_\Leftrightarrow$$

Motivating Example (Other Branch)

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

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

Motivating Example (Other Branch)

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

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

Motivating Example (Other Branch)

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

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

Motivating Example (Other Branch)

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

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

Motivating Example (Other Branch)

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(\color{red}{b}\color{black}) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall}{\dfrac{P(\color{red}{b}\color{black}), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma \qquad \dfrac{\neg P(\color{red}{b}\color{black}), \boldsymbol{\neg(\forall y\ P(y))}}{\neg P(sko)}\ \delta_{\neg\forall}}\ \beta_\Leftrightarrow$$

Motivating Example (Other Branch)

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

$$\dfrac{\dfrac{P(a), \neg P(b), \boldsymbol{\forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}}{P(\color{red}{b}\color{black}) \Leftrightarrow (\forall y\ P(y))}\ \gamma_{\forall}}{\dfrac{P(\color{red}{b}\color{black}), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_{\sigma} \qquad \dfrac{\dfrac{\neg P(\color{red}{b}\color{black}), \neg(\forall y\ P(y))}{\neg P(sko)}\ \delta_{\neg\forall}}{P(X_2) \Leftrightarrow (\forall y\ P(y))}\ reintroduction}\ \beta_{\Leftrightarrow}$$

Motivating Example (Other Branch)

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(\color{red}{b}\color{black}) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall}{\dfrac{P(\color{red}{b}\color{black}), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma \qquad \dfrac{\dfrac{\dfrac{\neg P(\color{red}{b}\color{black}), \neg(\forall y\ P(y))}{\neg P(sko)}\ \delta_{\neg\forall}}{\boldsymbol{P(X_2) \Leftrightarrow (\forall y\ P(y))}}\ reintroduction}{P(X_2), \forall y\ P(y) \qquad \neg P(X_2), \neg(\forall y\ P(y))}\ \beta_\Leftrightarrow}\ \beta_\Leftrightarrow$$

Motivating Example (Other Branch)

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

$$
\dfrac{\dfrac{P(a), \neg \boldsymbol{P(b)}, \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_{\forall}}{\dfrac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_{\sigma} \qquad \dfrac{\dfrac{\dfrac{\neg P(b), \neg(\forall y\ P(y))}{\boldsymbol{\neg P(sko)}}\ \delta_{\neg\forall}}{P(b) \Leftrightarrow (\forall y\ P(y))}\ reintroduction}{\dfrac{\boldsymbol{P(b)}, \forall y\ P(y)}{\begin{array}{c}\boldsymbol{\sigma = \{X_2 \mapsto b\}} \\ \boldsymbol{\sigma' = \{X_2 \mapsto sko\}}\end{array}}\ \odot_{\sigma} \qquad \neg P(b), \neg(\forall y\ P(y))}\ \beta_{\Leftrightarrow}}\ \beta_{\Leftrightarrow}
$$

Motivating Example (Other Branch)

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

$$\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_{\forall}$$

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

$$\dfrac{\neg P(sko)}{P(b) \Leftrightarrow (\forall y\ P(y))}\ reintroduction$$

$$\dfrac{P(b) \Leftrightarrow (\forall y\ P(y))}{\dfrac{P(b), \forall y\ P(y)}{\sigma = \{X_2 \mapsto b\}}\ \odot_{\sigma} \qquad \dfrac{\neg P(b), \boldsymbol{\neg(\forall y\ P(y))}}{\neg P(sko_2)}\ \delta_{\neg\forall}}\ \beta_{\Leftrightarrow}$$

$$\sigma' = \{X_2 \mapsto sko\}$$

Motivating Example (Other Branch)

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(b) \Leftrightarrow (\forall y\ P(y))}\ \gamma_\forall}{\dfrac{P(b), \forall y\ P(y)}{\sigma = \{X \mapsto b\}}\ \odot_\sigma \qquad \dfrac{\neg P(b), \neg(\forall y\ P(y))}{\dfrac{\neg P(sko)}{\dfrac{P(b) \Leftrightarrow (\forall y\ P(y))}{\dfrac{P(b), \forall y\ P(y)}{\sigma = \{X_2 \mapsto b\}}\ \odot_\sigma \quad \dfrac{\neg P(b), \neg(\forall y\ P(y))}{\dfrac{\neg P(sko_2)}{\dots}\ reintroduction}\ \delta_{\neg\forall}}\ \beta_\Leftrightarrow}\ reintroduction}\ \delta_{\neg\forall}}\ \beta_\Leftrightarrow$$

$$\sigma' = \{X_2 \mapsto sko\}$$

Exploring Branches in Parallel?

Approach

- Each branch searches for a local solution
- Manages multiple solutions
- No more branch selection fairness problem

New Challenges

- Free variable dependency
- Communication between branches

Technical Point

- Backtracking on solutions
- Reintroduction fairness problem: iterative deepening

Comeback to Example

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

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

Comeback to Example

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

$$\frac{P(a), \neg P(b), \boldsymbol{\forall x \ (P(x) \Leftrightarrow (\forall y \ P(y)))}}{P(X) \Leftrightarrow (\forall y \ P(y))} \ \gamma\forall M$$

Comeback to Example

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

$$\cfrac{\cfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{\boldsymbol{P(X) \Leftrightarrow (\forall y\ P(y))}}\ \gamma\forall M}{P(X), \forall y\ P(y) \qquad \neg P(X), \neg(\forall y\ P(y))}\ \beta \Leftrightarrow$$

Comeback to Example

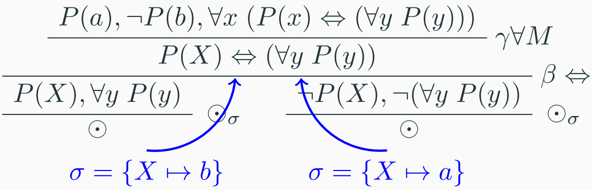
$$P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))$$

$$\dfrac{\dfrac{\dfrac{\boldsymbol{P(a)}, \neg \boldsymbol{P(b)}, \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(X) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M}{\dfrac{\boldsymbol{P(X)}, \forall y\ P(y)}{\odot}\ \odot_\sigma \qquad \dfrac{\neg \boldsymbol{P(X)}, \neg(\forall y\ P(Y))}{\odot}\ \odot_\sigma}\ \beta\Leftrightarrow}{}$$

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

Comeback to Example

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



Comeback to Example

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(X) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M}{\dfrac{P(b), \forall y\ P(y)}{} \qquad \dfrac{\neg P(b), \neg(\forall y\ P(y))}{}}\ \beta\Leftrightarrow$$

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

Comeback to Example

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

$$
\begin{array}{c}
P(a), \neg \boldsymbol{P(b)}, \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y))) \\
\hline
P(X) \Leftrightarrow (\forall y\ P(y))
\end{array}
\ \gamma\forall M
$$

$$
\begin{array}{c|c}
\begin{array}{c}
\boldsymbol{P(b)}, \forall y\ P(y) \\
\hline
\odot
\end{array}
\quad \odot_\sigma
&
\begin{array}{c}
\neg P(b), \neg(\forall y\ P(y)) \\
\hline
\end{array}
\end{array}
\ \beta\Leftrightarrow
$$

Closed

Comeback to Example

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(X) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M}{\dfrac{P(b), \forall y\ P(y)}{\odot}\ \odot_\sigma \qquad \dfrac{\neg P(b), \neg(\forall y\ P(y))}{P(sko)}\ \delta_{\neg\forall}}\ \beta\Leftrightarrow$$

Comeback to Example

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(X) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M}{\dfrac{P(b), \forall y\ P(y)}{\odot}\ \odot_\sigma \qquad \dfrac{\neg P(b), \neg(\forall y\ P(y))}{\dfrac{P(sko)}{\cdots}}\ \delta_{\neg\forall}}\ \beta \Leftrightarrow$$

Open

Comeback to Example

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(X) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M}{\dfrac{P(a), \forall y\ P(y)}{} \qquad \dfrac{\neg P(a), \neg(\forall y\ P(y))}{}}\ \beta\Leftrightarrow$$

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

Comeback to Example

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

$$\dfrac{\dfrac{\boldsymbol{P(a)}, \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(X) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M}{\dfrac{P(\color{red}{a}), \forall y\ P(y)}{} \qquad \dfrac{\neg \boldsymbol{P(\color{red}{a})}, \neg(\forall y\ P(y))}{\odot}\ \odot_\sigma}\ \beta\Leftrightarrow$$

Closed

Comeback to Example

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

$$\dfrac{\dfrac{P(a), \neg P(b), \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(X) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M}{\dfrac{P(\textcolor{red}{a}), \forall \boldsymbol{y}\ \boldsymbol{P(y)}}{P(Y)}\ \gamma\forall \qquad \dfrac{\neg P(\textcolor{red}{a}), \neg(\forall y\ P(y))}{\odot}\ \odot_\sigma}\ \beta\Leftrightarrow$$

Comeback to Example

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

$$\dfrac{P(a), \neg \boldsymbol{P(b)}, \forall x\ (P(x) \Leftrightarrow (\forall y\ P(y)))}{P(a) \Leftrightarrow (\forall y\ P(y))}\ \gamma\forall M$$

$$\dfrac{P(a) \Leftrightarrow (\forall y\ P(y))}{P(a), \forall y\ P(y) \quad\quad \neg P(a), \neg(\forall y\ P(y))}\ \beta \Leftrightarrow$$

$$\dfrac{P(a), \forall y\ P(y)}{\boldsymbol{P(b)}}\ \gamma\forall \quad\quad \dfrac{\neg P(a), \neg(\forall y\ P(y))}{\odot}\ \odot_\sigma$$

$$\dfrac{\boldsymbol{P(b)}}{\odot}\ \odot_\sigma$$

closed $(Y \mapsto b)$

Reasoning within Theories

Reasoning Modulo Theory

Example

- Axiom: $\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b$
- Axiom: $\forall a, b.\ a = b \Leftrightarrow a \subseteq b \wedge b \subseteq a$
- Conjecture: $\forall a.\ a \subseteq a$

In the method of analytics tableaux

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

Reasoning Modulo Theory

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

$$\dfrac{\forall a, b.\ a \subseteq b \Leftrightarrow \forall x.\ x \in a \Rightarrow x \in b, \forall a, b.\ a = b \Leftrightarrow a \subseteq b \land b \subseteq a, \neg(\forall a.\ a \subseteq a)}{\neg(a \subseteq a)}\ \delta_{\neg\forall}$$

$$\dfrac{\dfrac{\neg(a \subseteq a)}{(\forall b.\ A \subseteq b \Leftrightarrow \forall x.\ x \in A \Rightarrow x \in b)}\ \gamma_{\forall M}}{(A \subseteq B \Leftrightarrow \forall x.\ x \in A \Rightarrow x \in B)}\ \gamma_{\forall M}$$

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

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

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

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

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

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

Deduction Modulo Theory (DMT)

Rewrite rules

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

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

Deduction Modulo Theory (DMT)

Rewrite rules

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

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

Deduction Modulo Theory (DMT)

Rewrite rules

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

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

Deduction Modulo Theory (DMT)

Rewrite rules

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

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

Deduction Modulo Theory (DMT)

Benefits

- Avoid combinatorial explosion
- “Useless” axioms aren’t tiggered
- Shorter proof
- Not limited to one theory
- Good properties for an ATP!

Implementation and Results

Goéland Tool

Functionnalities

- Concurrent proof search algorithm
- Equality
- Deduction modulo theory (DMT)
- Polymorphic types
- Coq output
- Arithmetic (with simplex and branch and bound, not linked yet)

Prize

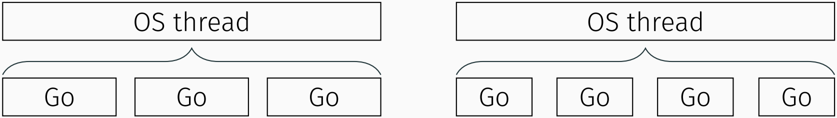
Best Newcomer — CASC2022

Goéland Tool

Implementation

- 30 000 lines of code
- Go programming language
- Designed for concurrency
- Goroutines: N:M lightweight threads

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



Experimentals Results on TPTP

	SYN (263 problems)		SET (464 problems)	
Goéland	199		229	
GoélandDMT	199	$(+0, -0)$	272	$(+66, -23)$
Zenon	256	$(+60, -3)$	150	$(+74, -153)$
Princess	195	$(+1, -5)$	258	$(+132, -103)$
LeoIII	195	$(+1, -5)$	177	$(+93, -145)$
E	261	$(+62, -0)$	363	$(+184, -50)$
Vampire	262	$(+63, -0)$	321	$(+167, -75)$

Experimentals Results on TPTP

	SYN (263 problems)		SET (464 problems)	
Goéland	199		229	
GoélandDMT	199	$(+0, -0)$	272	$(+66, -23)$
Zenon	256	$(+60, -3)$	150	$(+74, -153)$
Princess	195	$(+1, -5)$	258	$(+132, -103)$
LeoIII	195	$(+1, -5)$	177	$(+93, -145)$
E	261	$(+62, -0)$	363	$(+184, -50)$
Vampire	262	$(+63, -0)$	321	$(+167, -75)$

Experimentals Results on TPTP

	SYN (263 problems)		SET (464 problems)	
Goéland	199		229	
GoélandDMT	199	$(+0, -0)$	272	$(+66, -23)$
Zenon	256	$(+60, -3)$	150	$(+74, -153)$
Princess	195	$(+1, -5)$	258	$(+132, -103)$
LeoIII	195	$(+1, -5)$	177	$(+93, -145)$
E	261	$(+62, -0)$	363	$(+184, -50)$
Vampire	262	$(+63, -0)$	321	$(+167, -75)$

Conclusion

Goéland and ATP

- Fairness between branches managed by concurrency
- Promising results for a very new prover, especially with DMT
- Combination is the key (Core solver, SMT, extension for a given theories)

Formal Methods

- Formal methods are the only way to ensure that something works perfectly
- ...but it requires a lot of time and money
- Good balance between tests and proofs

Thank you! ☺

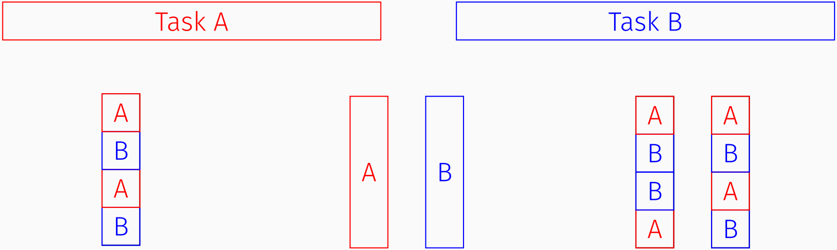
Concurrency vs. parallelism

Concurrency

Concurrency is about an application making progress on more than one task at the same time.

Parallelism

Parallelism is about tasks which can be processed in parallel, for instance on multiple CPUs at the exact same time.

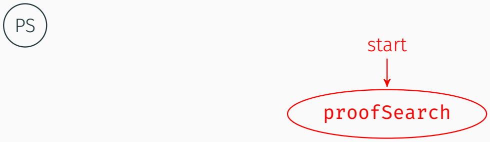


Concurrent but not parallel

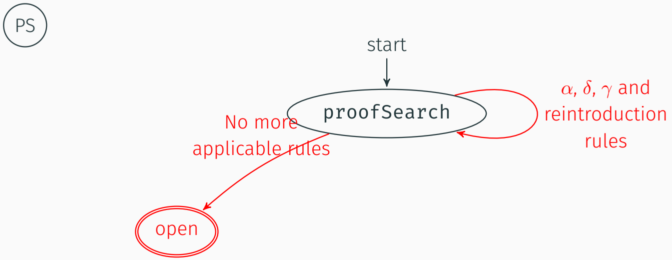
Parallel but not concurrent

parallel and concurrent

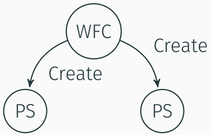
Procedures interactions

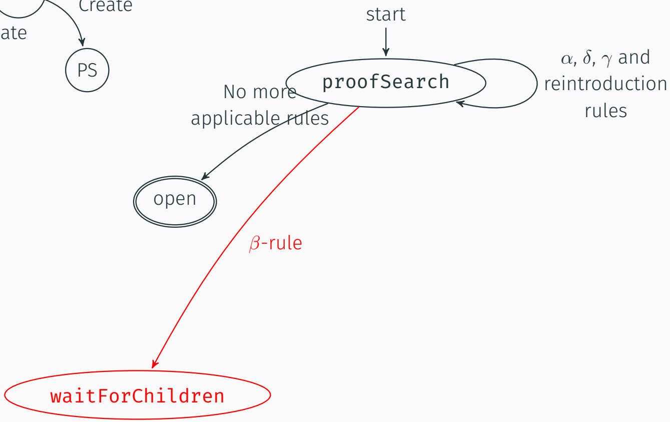


Procedures interactions

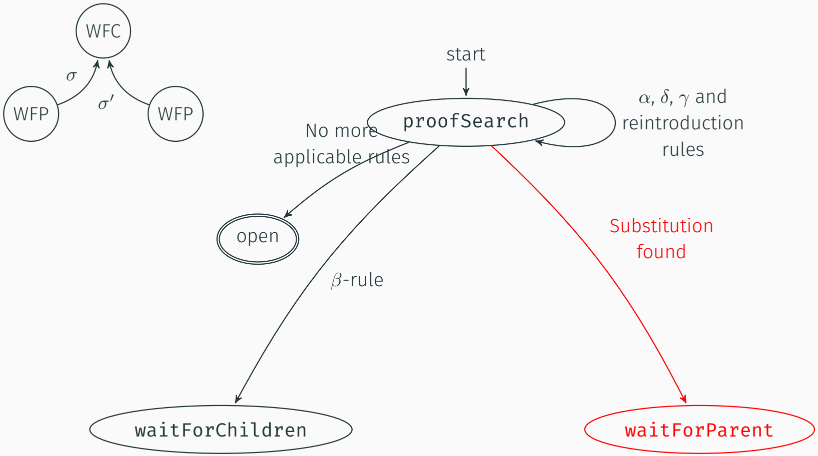


Procedures interactions

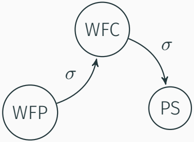


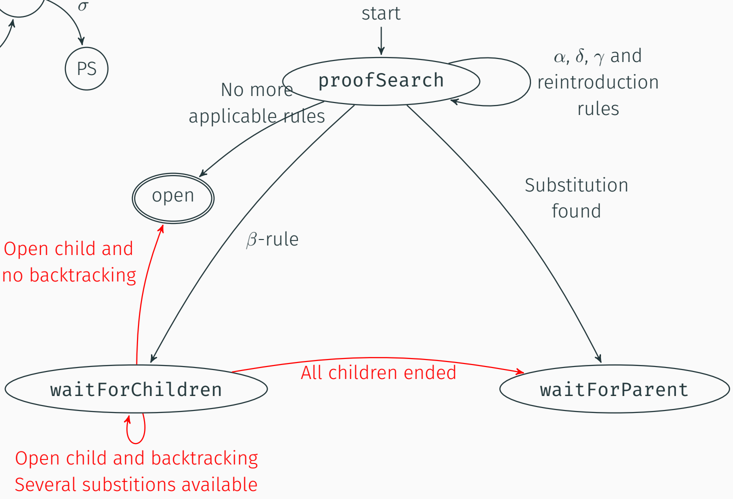


Procedures interactions

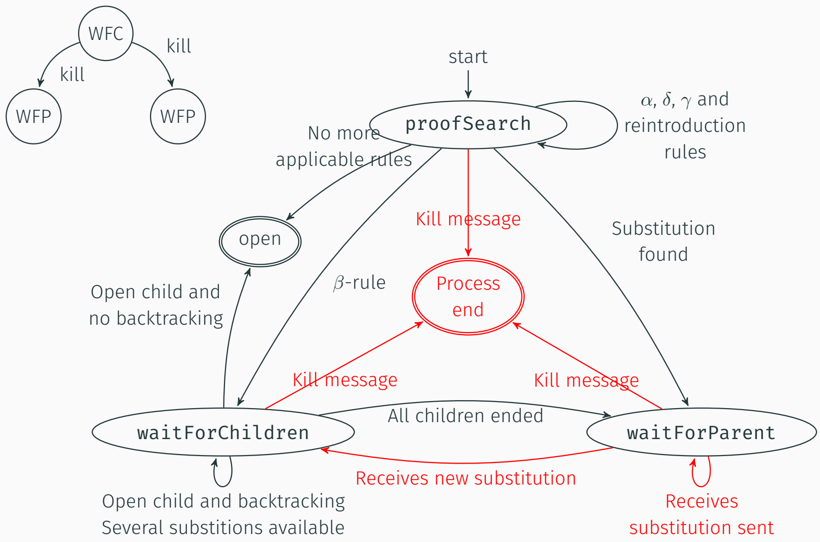


Procedures interactions





Procedures interactions



Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\frac{\neg P(b), \neg Q(a), \neg R(c), \boldsymbol{\forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}}{P(X) \vee Q(X), \partial R(X)}\ \gamma\forall M$$

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \lor Q(x)) \land (\partial R(x)))$$

$$\dfrac{\dfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \lor Q(x)) \land (\partial R(x)))}{\boldsymbol{P(X)} \lor \boldsymbol{Q(X)}, \partial R(X)}\ \gamma\forall M}{P(X), \partial R(X) \qquad Q(X), \partial R(X)}\ \beta \Leftrightarrow$$

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\boldsymbol{\neg P(b)}, \boldsymbol{\neg Q(a)}, \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{\dfrac{P(X) \vee Q(X), \partial R(X)}{\dfrac{\boldsymbol{P(X)}, \partial R(X)}{\odot}\ \odot_\sigma \qquad \dfrac{\boldsymbol{Q(X)}, \partial R(X)}{\odot}\ \odot_\sigma}\ \beta\Leftrightarrow}\ \gamma\forall M$$

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

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{\dfrac{P(X) \vee Q(X), \partial R(X)}{\dfrac{P(X), \partial R(X)}{\odot}\ \odot_\sigma \qquad \dfrac{Q(X), \partial R(X)}{\odot}\ \odot_\sigma}\ \beta \Leftrightarrow}\ \gamma\forall M$$

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

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x \; ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\cfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x \; ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{\cfrac{P(X) \vee Q(X), \partial R(X)}{\cfrac{P(b), \partial R(b)}{} \qquad \cfrac{Q(b), \partial R(b)}{}} \; \beta \Leftrightarrow} \; \gamma \forall M$$

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

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\dfrac{\boldsymbol{\neg P(b)}, \neg Q(a), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{P(X) \vee Q(X), \partial R(X)}\ \gamma\forall M}{\dfrac{\boldsymbol{P(b)}, \partial R(b)}{\odot}\ \odot_\sigma \qquad \dfrac{Q(b), \partial R(b)}{}}\ \beta \Leftrightarrow$$

Closed

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{\dfrac{P(X) \vee Q(X), \partial R(X)}{\dfrac{P(b), \partial R(b)}{\odot}\ \odot_\sigma \qquad \dfrac{Q(b), \boldsymbol{\partial R(X)}}{R(b)}\ \partial}\ \beta \Leftrightarrow}\ \gamma\forall M$$

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x \; ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x \; ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{P(X) \vee Q(X), \partial R(X)} \; \gamma\forall M$$

$$\dfrac{P(X) \vee Q(X), \partial R(X)}{\dfrac{P({\color{red}b}), \partial R({\color{red}b})}{\odot} \; \odot_\sigma \qquad \dfrac{Q({\color{red}b}), \partial R({\color{red}b})}{\dfrac{R({\color{red}b})}{\cdots}} \; \partial} \; \beta \Leftrightarrow$$

Open

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \lor Q(x)) \land (\partial R(x)))$$

$$\dfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \lor Q(x)) \land (\partial R(x)))}{\dfrac{P(X) \lor Q(X), \partial R(X)}{\dfrac{P(a), \partial R(a)}{} \qquad \dfrac{Q(a), \partial R(a)}{}}\ \beta \Leftrightarrow}\ \gamma\forall M$$

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

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\neg P(b), \boldsymbol{\neg Q(a)}, \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{P(X) \vee Q(X), \partial R(X)}\ \gamma\forall M$$

$$\dfrac{P(X) \vee Q(X), \partial R(X)}{P(a), \partial R(a) \qquad \boldsymbol{Q(a)}, \partial R(a)}\ \beta \Leftrightarrow$$

$$\dfrac{\boldsymbol{Q(a)}, \partial R(a)}{\odot}\ \odot_\sigma$$

Closed

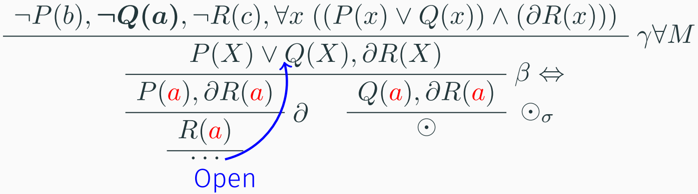
Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\cfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{\cfrac{P(X) \vee Q(X), \partial R(X)}{\cfrac{P(\color{red}{a}), \boldsymbol{\partial R(\color{red}{a})}}{R(\color{red}{a})}\ \partial \qquad \cfrac{Q(\color{red}{a}), \partial R(\color{red}{a})}{\odot}\ \odot_\sigma}\ \beta \Leftrightarrow}\ \gamma\forall M$$

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$



Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{\dfrac{P(X) \vee Q(X), \partial R(X)}{\dfrac{P(X), \partial R(X)}{} \qquad \dfrac{Q(X), \partial R(X)}{}}\ \beta \Leftrightarrow}\ \gamma\forall M$$

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

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \lor Q(x)) \land (\partial R(x)))$$

$$\cfrac{\neg P(b), \neg Q(a), \neg R(c), \forall x\ ((P(x) \lor Q(x)) \land (\partial R(x)))}{\cfrac{P(X) \lor Q(X), \partial R(X)}{\cfrac{P(X), \boldsymbol{\partial R(X)}}{R(X)}\ \partial \qquad \cfrac{Q(X), \boldsymbol{\partial R(X)}}{R(X)}\ \partial}\ \beta \Leftrightarrow}\ \gamma\forall M$$

Example with the Proof Resuming

$$\neg P(b), \neg Q(b), \neg R(c), \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))$$

$$\dfrac{\neg P(b), \neg Q(a), \boldsymbol{\neg R(c)}, \forall x\ ((P(x) \vee Q(x)) \wedge (\partial R(x)))}{P(X) \vee Q(X), \partial R(X)}\ \gamma\forall M$$

$$\dfrac{P(X) \vee Q(X), \partial R(X)}{P(X), \partial R(X) \qquad\qquad Q(X), \partial R(X)}\ \beta \Leftrightarrow$$

$$\dfrac{P(X), \partial R(X)}{\dfrac{\boldsymbol{R(X)}}{\odot}\ \odot_\sigma}\ \partial \qquad\qquad \dfrac{Q(X), \partial R(X)}{\dfrac{\boldsymbol{R(X)}}{\odot}\ \odot_\sigma}\ \partial$$

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