

# Comparison of two theorem provers: Isabelle & Coq

A. Yushkovskiy   S. Tripakis

Department of Computer Science  
School of Science  
**Aalto University**

CS-E4000: Seminar in Computer Science  
autumn 2017

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# Outline

## Foundations of Formal Approach

- A Formal System

- Properties of a Formal System

- Classical and Intuitionistic Logics

## Two Theorem Provers

- Isabelle

- Coq

## Comparison of the Theorem Provers

- Common Features

- Major Differences

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# Elements of a Formal System

- ▶ A formula (judgement, statement)  $\phi \in \Phi$ :

$$\begin{aligned}\phi &:= p \mid q \mid \dots \\ &\mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \neg \phi_1 \mid \phi_1 \rightarrow \phi_2 \\ &\mid \textit{true} \mid \textit{false} \\ &\mid \dots\end{aligned}$$

- ▶ Propositional variables: —  $p, q, \dots \in V$
- ▶ An axiom —  $\phi_A \in A$
- ▶ An inference rule  $\tau$  — a transition function  $\tau : \Phi \rightarrow \Phi$
- ▶ A formula  $\phi$  provable from  $\Phi$  —  $\Phi \vdash \phi$
- ▶ A tautology  $\top$  —  $\vdash \phi$
- ▶ A contradiction  $\perp$  —  $\vdash \neg \phi$

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle  
Coq

Comparison of the  
Theorem Provers

Common Features  
Major Differences

Summary

# Definition of the Formal System

A *formal system* is a quadruple  $\Gamma = \langle A, V, \Omega, R \rangle$ , where

- ▶  $A$  – set of axioms
- ▶  $V$  – set of propositional variables
- ▶  $\Omega$  – set of logical operators
- ▶  $R$  – set of inference rules

A *formal proof* of the formula  $\phi$  is a finite sequence of judgements

$$\psi_1 \xrightarrow{\tau_1} \psi_2 \xrightarrow{\tau_2} \dots \xrightarrow{\tau_n} \psi_n$$

where each  $\psi_i$  is either an axiom  $\phi_{A_i}$ , or a formula inferred from the set of previously derived formulas according the rules of inference.

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# Properties of a Formal System

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

A formal system  $\Gamma$  is called:

- ▶ *consistent*, if  $\nexists \phi \in \Gamma : \Gamma \vdash \phi \wedge \Gamma \vdash \neg \phi \Leftrightarrow \Gamma \not\vdash \perp$ ;
- ▶ *complete*, if  $\forall \phi \in U : A \vdash \phi \vee A \vdash \neg \phi$ ;
- ▶ *independent*, if  $\nexists a \in A : A \vdash a$ .

# Classical Logic

## Example: The Hilbert System

Set of axioms:

$$A \rightarrow (B \rightarrow A) \quad (\text{A1})$$

$$(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) \quad (\text{A2})$$

Single inference rule:

$$\llbracket A, A \rightarrow B \rrbracket \longrightarrow B \quad (\text{MP})$$

Some tautologies:

$$A \vee \neg A \quad (\text{EM})$$

$$\neg\neg(A \vee \neg A) \quad (\text{nnEM})$$

$$A \rightarrow \neg\neg A \quad (\text{DNi})$$

$$\neg\neg A \rightarrow A \quad (\text{DNe})$$

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# Isabelle: First Acquaintance

- ▶ a generic proof assistant
- ▶ a successor of HOL theorem prover //TODO: cite
- ▶ created in 1986 by
  - ▶ Larry Paulson @ University of Cambridge, and
  - ▶ Tobias Nipkow @ Technische Universität München
- ▶ based on classical higher-order logic
- ▶ uses powerful functional language HOL
- ▶ has large collection of formalised theories //TODO: HOL, ZF, CCL, ...

## Example 1: Definition of basic datatypes

```
datatype bool =  
  True | False
```

```
datatype nat =  
  zero ("0") | Suc nat
```

## Example 2: ???

???

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

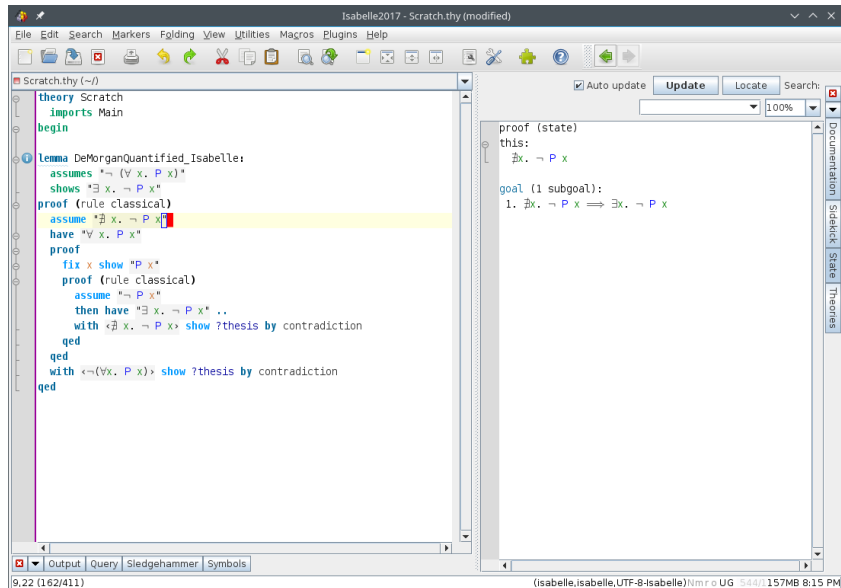
Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# Isabelle: Native GUI



Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary



# Coq: First Acquaintance

- ▶ a formal proof management system
- ▶ created at INRIA (Paris, France) in 1984
- ▶ based on Calculus of Inductive Constructions theory (an implementation of intuitionistic logic)
- ▶ uses powerful functional language `Gallina`
- ▶ has large collection of formalised theories //TODO
- ▶ widely used in software verification (proof code extraction)

## Example 3: Definition of basic datatypes

```
Inductive False : Prop := .
```

```
Inductive True : Prop := I : True.
```

```
Inductive nat : Type :=  
  | O : nat  
  | S : nat -> nat.
```

## Example 4: ???

???

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# The Coq theorem prover

The screenshot shows the CoqIDE interface with a menu bar (File, Edit, View, Navigation, Try Tactics, Templates, Queries, Tools, Compile, Windows, Help) and a toolbar with icons for saving, opening, undo, redo, and other editing functions. The main editor displays a Coq script for proving De Morgan's law. The script is as follows:

```
Theorem DeMorganPropositional_Coq:
  forall P Q : Prop, ~(P /\ Q) <-> ~P /\ ~Q.
Proof.
  (* 'tauto' automatically proves the equation *)
  intros P Q. unfold iff.
  split.
  - intros H_not_or. unfold not. constructor.
    + intro H_P. apply H_not_or. left. apply H_P.
    + intro H_Q. apply H_not_or. right. apply H_Q.
  - intros H_and_not H_or.
    destruct H_and_not as [H_not_P H_not_Q].
    destruct H_or as [H_P | H_Q].
    + apply H_not_P. assumption.
    + apply H_not_Q. assumption.
Qed.
```

On the right side of the interface, there is a goal panel showing the current subgoal:

```
| subgoal
P, Q : Prop
H_not_or : ~ (P /\ Q)
H_Q : Q
----- (1/1)
P /\ Q
```

At the bottom of the interface, there is a status bar that reads "Ready, proving DeMorganPropositional\_Coq" and "Line: 9 Char: 33 Coq is ready 0 / 0".

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

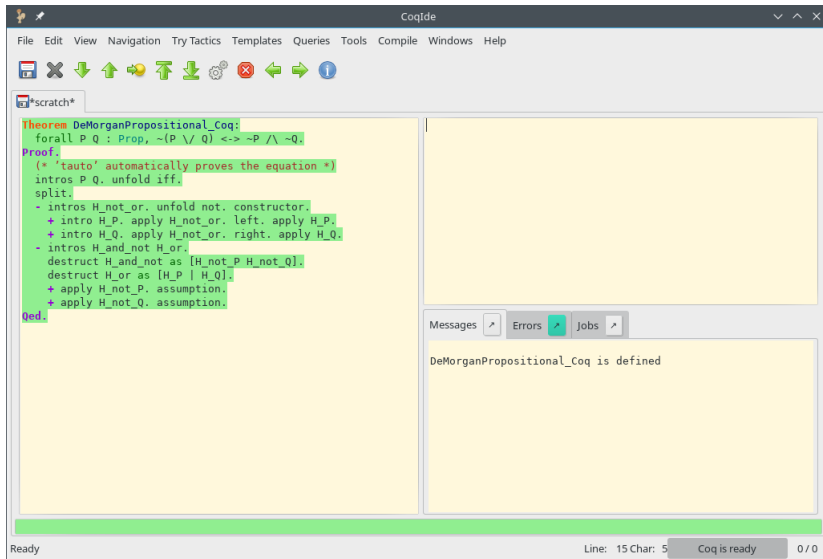
Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# The Coq theorem prover



Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary

# Summary

- ▶ The **first main message** of your talk in one or two lines.
- ▶ The **second main message** of your talk in one or two lines.
- ▶ Perhaps a **third message**, but not more than that.
- ▶ Outlook
  - ▶ Something you haven't solved.
  - ▶ Something else you haven't solved.

Comparison of two  
theorem provers:  
Isabelle & Coq

A. Yushkovskiy,  
S. Tripakis

Foundations of  
Formal Approach

A Formal System

Properties of a Formal  
System

Classical and Intuitionistic  
Logics

Two Theorem  
Provers

Isabelle

Coq

Comparison of the  
Theorem Provers

Common Features

Major Differences

Summary