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

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

Elements of a Formal System

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

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

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

Definition of the Formal System

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

- A – set of axioms
- V – set of propositional variables
- Ω – set of logical operators
- R – set of inference rules

A *formal proof* of the formula ϕ is a finite sequence of judgements

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

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

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

A formal system Γ is called:

- *consistent*, if $\nexists \phi \in \Gamma : \ \Gamma \vdash \phi \land \Gamma \vdash \neg\phi \ \Leftrightarrow \ \Gamma \nvdash \bot$;
- *complete*, if $\forall \phi \in U : \ A \vdash \phi \lor A \vdash \neg\phi$;
- *independent*, if $\nexists a \in A : \ A \vdash a$.

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

Classical Logic

Example: The Hilbert System

Set of axioms:

$$A \to (B \to A) \tag{A1}$$

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)) \tag{A2}$$

Single inference rule:

$$[\![A, A \to B]\!] \longrightarrow B \tag{MP}$$

Some tautologies:

$$A \vee \neg A \tag{EM}$$

$$\neg\neg(A \vee \neg A) \tag{nnEM}$$

$$A \to \neg\neg A \tag{DNi}$$

$$\neg\neg A \to A \tag{DNe}$$

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, ...

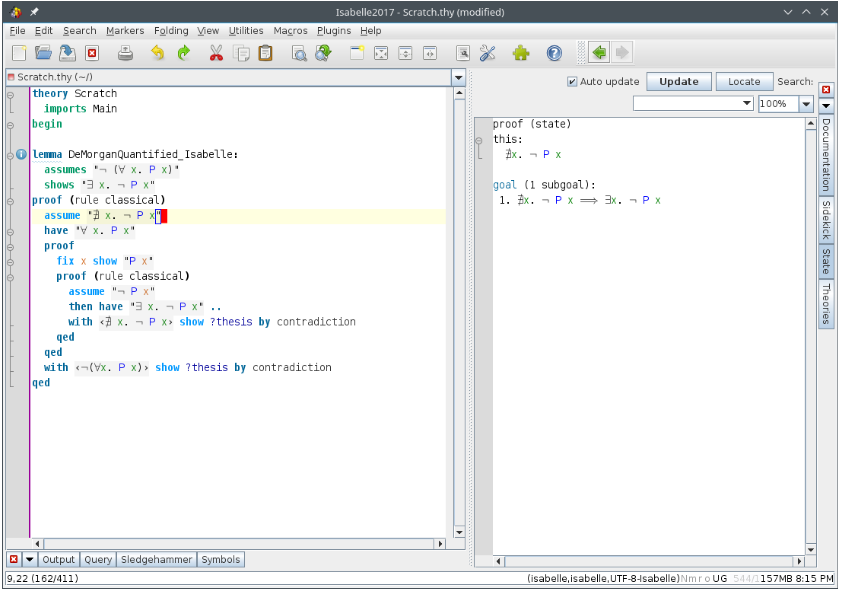
Example 1: Definition of basic datatypes

```
datatype bool =
  True | False

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

Example 2: ???

```
???
```

Isabelle: Native GUI



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

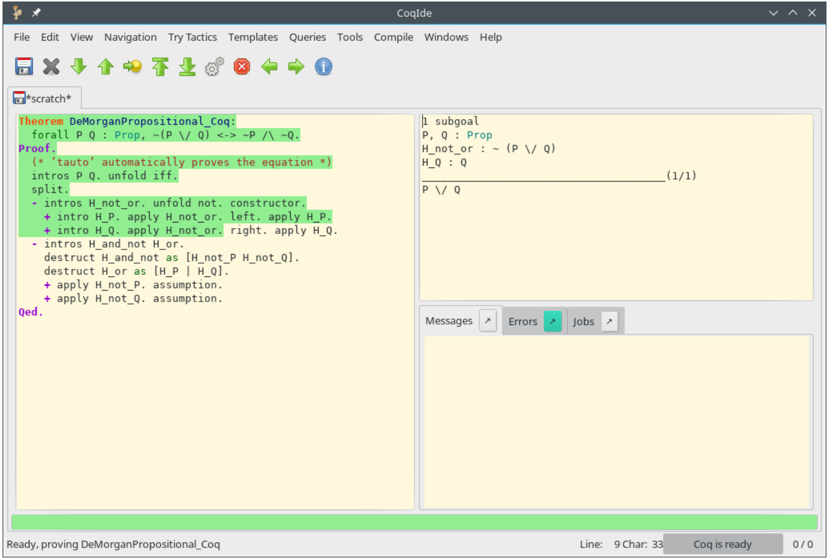
```
Inductive False : Prop := .

Inductive True : Prop := I : True.

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

Example 4: ???

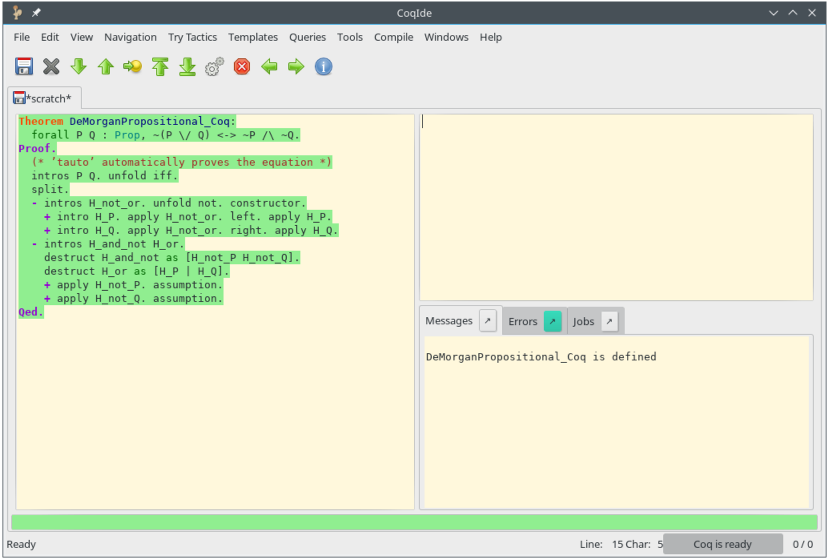
```
???
```


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 Coq theorem prover



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.

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