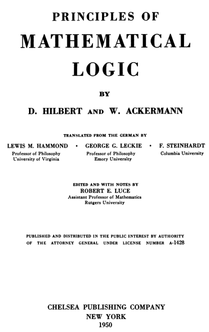
Comparison of two theorem provers: Isabelle & Coq

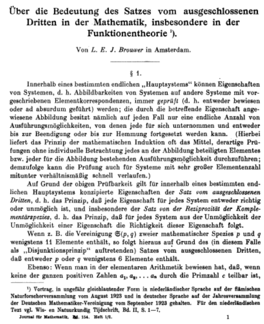
A. Yushkovskiy S. Tripakis

Department of Computer Science
School of Science
Aalto University

CS-E4000: Seminar in Computer Science
autumn 2017

Introduction


PRINCIPLES OF
MATHEMATICAL
LOGIC
BY
D. HILBERT AND W. ACKERMANN
TRANSLATED FROM THE GERMAN BY
LEWIS M. HAMMOND · GEORGE G. LECKIE · F. STEINHARDT
Professor of Philosophy, University of Virginia · Professor of Philosophy, Emory University · Columbia University
EDITED AND WITH NOTES BY
ROBERT E. LUCE
Assistant Professor of Mathematics
Rutgers University
PUBLISHED AND DISTRIBUTED IN THE PUBLIC INTEREST BY AUTHORITY OF THE ATTORNEY GENERAL UNDER LICENSE NUMBER A-1428
CHELSEA PUBLISHING COMPANY
NEW YORK
1950


Über die Bedeutung des Satzes vom ausgeschlossenen Dritten in der Mathematik, insbesondere in der Funktionentheorie [1]).

Von *L. E. J. Brouwer* in Amsterdam.

§ 1.

Innerhalb eines bestimmten endlichen „Hauptsystems" können Eigenschaften von Systemen, d. h. Abbildbarkeiten von Systemen auf andere Systeme mit vorgeschriebenen Elementkorrespondenzen, immer *geprüft* (d. h. entweder bewiesen oder ad absurdum geführt) werden; die durch die betreffende Eigenschaft angewiesene Abbildung besitzt nämlich auf jeden Fall nur eine endliche Anzahl von Ausführungsmöglichkeiten, von denen jede für sich unternommen und entweder bis zur Beendigung oder bis zur Hemmung fortgesetzt werden kann. (Hierbei liefert das Prinzip der mathematischen Induktion oft das Mittel, derartige Prüfungen ohne individuelle Betrachtung jedes an der Abbildung beteiligten Elementes bzw. jeder für die Abbildung bestehenden Ausführungsmöglichkeit durchzuführen; demzufolge kann die Prüfung auch für Systeme mit sehr großer Elementenzahl mitunter verhältnismäßig schnell verlaufen.)

Auf Grund der obigen Prüfbarkeit gilt für innerhalb eines bestimmten endlichen Hauptsystems konzipierte Eigenschaften der *Satz vom ausgeschlossenen Dritten*, d. h. das Prinzip, daß jede Eigenschaft für jedes System entweder richtig oder unmöglich ist, und insbesondere der *Satz von der Reziprozität der Komplementärspezies*, d. h. das Prinzip, daß für jedes System aus der Unmöglichkeit der Unmöglichkeit einer Eigenschaft die Richtigkeit dieser Eigenschaft folgt.

Wenn z. B. die Vereinigung $\mathfrak{S}(p, q)$ zweier mathematischer Spezies p und q wenigstens 11 Elemente enthält, so folgt hieraus auf Grund des (in diesem Falle als „Disjunktionsprinzip" auftretenden) Satzes vom ausgeschlossenen Dritten, daß entweder p oder q wenigstens 6 Elemente enthält.

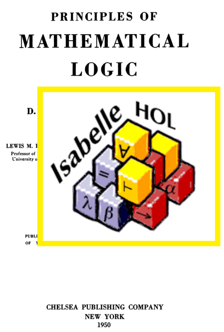
Ebenso: Wenn man in der elementaren Arithmetik bewiesen hat, daß, wenn keine der ganzen positiven Zahlen $a_1, a_2, \dots a_n$ durch die Primzahl c teilbar ist,

[1]) Vortrag, in ungefähr gleichlautender Form in niederländischer Sprache auf der flämischen Naturforscherversammlung vom August 1923 und in deutscher Sprache auf der Jahresversammlung der Deutschen Mathematiker-Vereinigung vom September 1923 gehalten. Für den niederländischen Text vgl. Wis- en Natuurkundig Tijdschrift, Bd. II, S. 1—7.

Journal für Mathematik. Bd. 154. Heft 1/2. 1

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Introduction



Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Outline

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Elements of a Formal System

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

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

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

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

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.

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Classical Logic

example: The Hilbert System

Set of axioms:

$$A \to (B \to A) \qquad \text{(A1)}$$
$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)) \qquad \text{(A2)}$$
$$A \vee \neg A \qquad \text{(EM)}$$

Single inference rule (*Modus Ponens*)

$$[\![A, A \to B]\!] \longrightarrow B \qquad \text{(MP)}$$

Some provable tautologies:

$\neg\neg(A \vee \neg A)$	(nnEM)	$\neg(A \wedge B) \to \neg A \vee \neg B$	(DMdi)
$A \to \neg\neg A$	(DNi)	$\neg(A \vee B) \to \neg A \wedge \neg B$	(DMci)
$\neg\neg A \to A$	(DNe)	$\neg A \wedge \neg B \to \neg(A \vee B)$	(DMce)
$((A \to B) \to A) \to B$	(PL)	$\neg A \vee \neg B \to \neg(A \wedge B)$	(DMde)

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Intuitionistic Logic

a.k.a. Constructive Logic

Set of axioms:

$$A \to (B \to A) \qquad \text{(A1)}$$
$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)) \qquad \text{(A2)}$$
$$\cancel{A \vee \neg A} \qquad \text{(EM)}$$

Single inference rule (*Modus Ponens*)

$$[\![A, A \to B]\!] \longrightarrow B \qquad \text{(MP)}$$

Some provable tautologies:

$\neg\neg(A \vee \neg A)$	(nnEM)	$\cancel{\neg(A \wedge B) \to \neg A \vee \neg B}$	(DMdi)
$\cancel{A \to \neg\neg A}$	(DNi)	$\neg(A \vee B) \to \neg A \wedge \neg B$	(DMci)
$\neg\neg A \to A$	(DNe)	$\neg A \wedge \neg B \to \neg(A \vee B)$	(DMce)
$\cancel{((A \to B) \to A) \to B}$	(PL)	$\neg A \vee \neg B \to \neg(A \wedge B)$	(DMde)

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Isabelle: first acquaintance

- a generic proof assistant
- based on classical higher-order logic
- created in 1986 by
  - Larry Paulson @ University of Cambridge, and
  - Tobias Nipkow @ Technische Universität München
- uses powerful functional language `HOL`
- the proof system core *Isabelle* is extended by various theories: Isabelle/HOL, Isabelle/ZF, Isabelle/CCL, etc.

Example 1: Definition of basic datatypes

```
datatype bool =
  True | False

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

Example 2: Definition of addition over `nat`

```
fun add :: "nat ⇒ nat ⇒ nat"
  where
    "add 0 n = n" |
    "add (Suc m) n = Suc(add m n)"
```

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Coq: first acquaintance

- a formal proof management system
- based intuitionistic logic (Calculus of Inductive Constructions)
- created at INRIA (Paris, France) in 1984
- uses powerful functional language `Gallina`
- has large collection of formalised theories
- 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: Definition of addition over `nat`

```
Fixpoint add (n m: nat) : nat :=
  match n with
    | O ⇒ m
    | S n′ ⇒ S (n′ + m)
  end
where "n + m" :=
  (add n m) : nat_scope.
```

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Comparison

Major similarities:

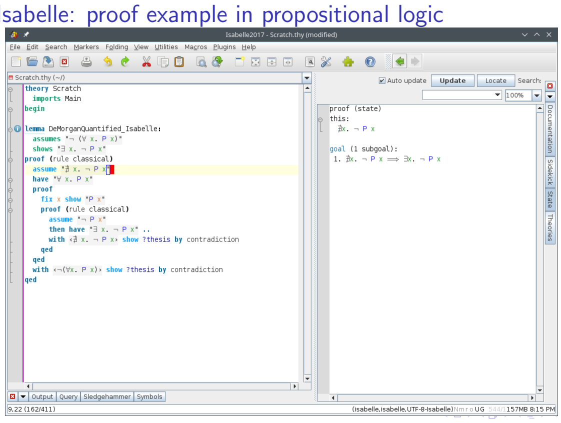
- both work in a similar way of *verifying* the proof or *assisting* in creation of the new one
- *premises* $\xrightarrow{tactics}$ *goals* (forward proof)
- *goals* $\xrightarrow{tactics}$ *premises* (backward proof)
- both have large amount of libraries with formalised theories
- both dispose the set of highly automated tactics
- both are being actively developed these days

Major differences:

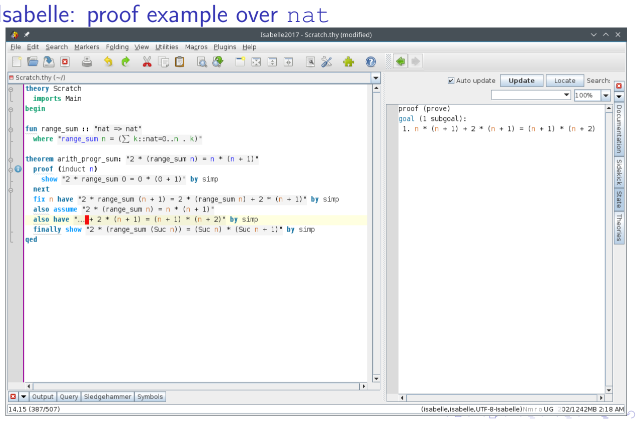
- based on different logics ⇒
  - unprovable statements and invalid proofs in Coq
  - sometimes more complex proof in Coq
  - *constructive* proof in Coq

Comparison of two theorem provers: Isabelle & Coq
A. Yushkovskiy, S. Tripakis
Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

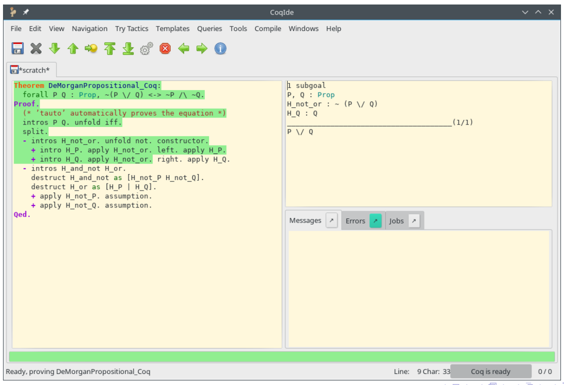
Isabelle: proof example in propositional logic



Isabelle: proof example over nat



Coq: proof example in propositional logic

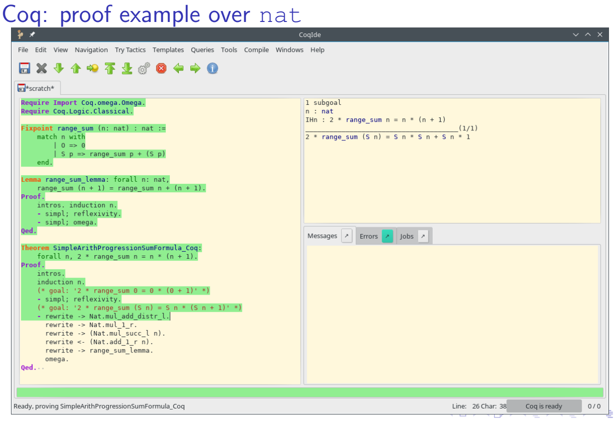


Comparison of two theorem provers: Isabelle & Coq

A. Yushkovskiy, S. Tripakis

Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Coq: proof example over nat

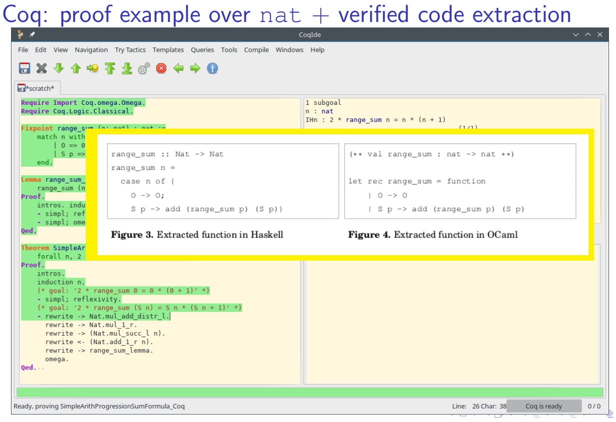


Comparison of two theorem provers: Isabelle & Coq

A. Yushkovskiy, S. Tripakis

Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Coq: proof example over nat + verified code extraction



Comparison of two theorem provers: Isabelle & Coq

A. Yushkovskiy, S. Tripakis

Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary

Summary

- Two widespread theorem provers were considered: Isabelle and Coq
- The key difference between them lie in differences between logical theories they based on
- Nonetheless, they both may be used to solve applied problems, such as software testing and verification

Comparison of two theorem provers: Isabelle & Coq

A. Yushkovskiy, S. Tripakis

Foundations of Formal Approach
A formal system
Classical and Intuitionistic logics
Two Theorem Provers
Isabelle
Coq
Comparison of the theorem provers
Comparison
Proof examples
Summary