# 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

# Outline

# Definition of the Formal System

- // TODO
- My second point.

# Properties of a Formal System

A formal system $\Gamma = < A, V, \Omega, R >$ is called:

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

# Classical and Intuitionistic Logics

// Classical: set of axioms
// Intuitionistic: same, but without EM

# 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: ???

```
???
```

# 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: ???

```
???
```

# Blocks

### Block Title
You can also highlight sections of your presentation in a block, with it's own title

### Theorem
*There are separate environments for theorems, examples, definitions and proofs.*

### Example
Here is an example of an example block.

# 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.

# For Further Reading I


A. Author.
*Handbook of Everything*.
Some Press, 1990.

S. Someone.
On this and that.
*Journal of This and That*, 2(1):50–100, 2000.