NICTA

NICTA

COMP 4161 NICTA Advanced Course

Advanced Topics in Software Verification

Simon Winwood, Toby Murray, June Andronick, Gerwin Klein



Slide 1

Content

- → Intro & motivation, getting started with Isabelle
- → Foundations & Principles
 - Lambda Calculus
 - Higher Order Logic, natural deduction
 - Term rewriting
- → Proof & Specification Techniques
 - Inductively defined sets, rule induction
 - Datatypes, recursion, induction
 - Well founded recursion, Calculational reasoning
 - Hoare logic, proofs about programs
 - Locales, Presentation





→ Sets in Isabelle

- ➔ Inductive Definitions
- → Rule induction
- → Fixpoints

Slide 3

Exercises



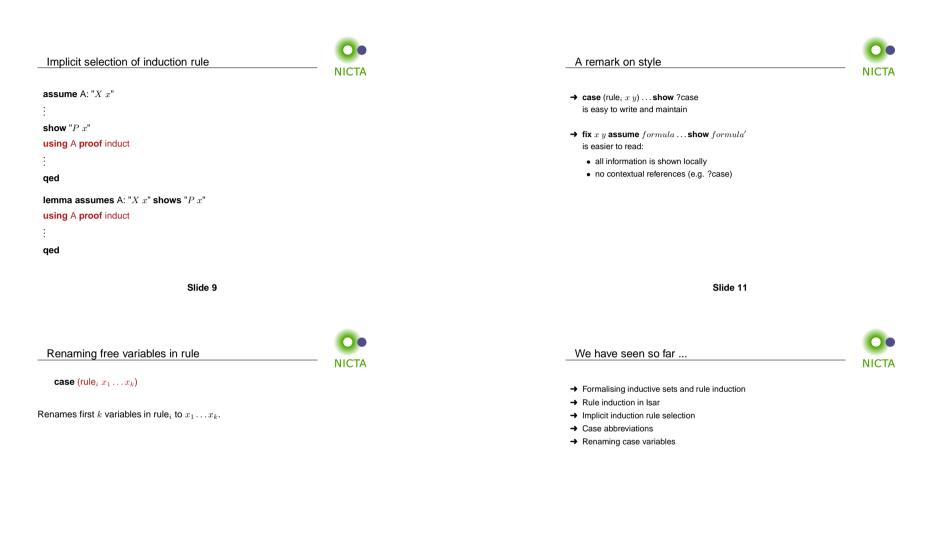
Formalize the last lecture in Isabelle:

- → Define closed $f A :: (\alpha \text{ set} \Rightarrow \alpha \text{ set}) \Rightarrow \alpha \text{ set} \Rightarrow \text{bool}$
- → Show closed $f A \land$ closed $f B \Longrightarrow$ closed $f (A \cap B)$ if f is monotone (mono is predefined)
- → Define **Ifpt** *f* as the intersection of all *f*-closed sets
- \rightarrow Show that lfpt f is a fixpoint of f if f is monotone
- \rightarrow Show that lfpt *f* is the least fixpoint of *f*
- → Declare a constant $R :: (\alpha \text{ set } \times \alpha)$ set
- → Define \hat{R} :: α set $\Rightarrow \alpha$ set in terms of R
- → Show soundness of rule induction using R and lfpt \hat{R}

Slide 2

Slide 4







Slide 12