ę	0	•
N	IC.	ТА

NICTA

COMP 4161 NICTA Advanced Course

Advanced Topics in Software Verification

Toby Murray, June Andronick, Gerwin Klein

$\lambda^{\rightarrow} {}_{\rm and \; {\rm HOL}}$

Slide 1

Last time...

- → Simply typed lambda calculus: λ^{\rightarrow}
- → Typing rules for λ^{\rightarrow} , type variables, type contexts
- → β -reduction in λ^{\rightarrow} satisfies subject reduction
- → β -reduction in λ^{\rightarrow} always terminates
- → Types and terms in Isabelle

Oraclest	
Content	NICTA
→ Intro & motivation, getting started	[1]
➔ Foundations & Principles	
 Lambda Calculus, natural deduction 	[1,2
Higher Order Logic	[3 ^a
Term rewriting	[4
 Proof & Specification Techniques 	
 Inductively defined sets, rule induction 	[5
 Datatypes, recursion, induction 	[6, 7
 Hoare logic, proofs about programs, C verification 	[8 ^b ,9
(mid-semester break)	
 Writing Automated Proof Methods 	[10
 Isar, codegen, typeclasses, locales 	[11 ^c ,12

^a a1 due; ^ba2 due; ^ca3 due

Slide 3



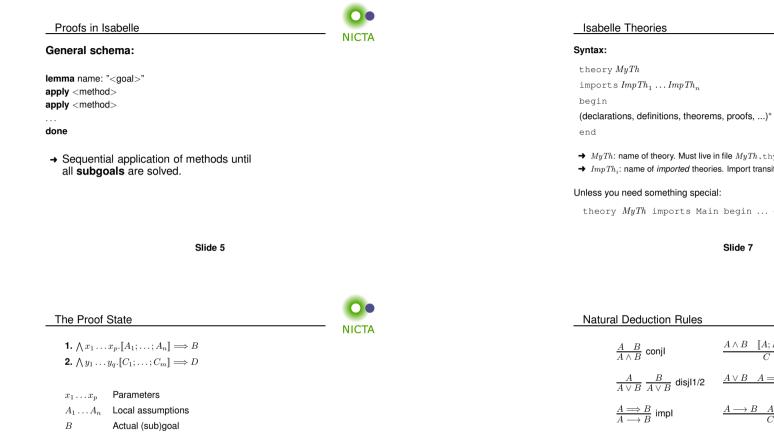
PREVIEW: PROOFS IN ISABELLE

Slide 4

Slide 2

Copyright NICTA 2014, provided under Creative Commons Attribution License

1





 \rightarrow MyTh: name of theory. Must live in file MyTh.thy

→ $ImpTh_i$: name of *imported* theories. Import transitive.

theory MyTh imports Main begin ... end

Slide 7

Natural Deduction Rules		0
	$A \land P \llbracket A, P \rrbracket \longrightarrow C$	NICTA
$rac{A}{A \wedge B}$ conjl	$\frac{A \land B \llbracket A; B \rrbracket \Longrightarrow C}{C} \text{ conjE}$	
$rac{A}{A \lor B} rac{B}{A \lor B}$ disjl1/2	$ \begin{array}{ccc} \underline{A \lor B} & \underline{A \Longrightarrow C} & \underline{B \Longrightarrow C} \\ \hline C & \end{array} \text{disjE} $	
$\frac{A \Longrightarrow B}{A \longrightarrow B} \text{ impl}$	$\frac{A \longrightarrow B A B \Longrightarrow C}{C} \text{ impE}$	

For each connective (\land , \lor , etc): introduction and elimination rules

Slide 8

