Content	
	NICTA
	Rough timeline
→ Intro & motivation, getting started	[1]
→ Foundations & Principles	
 Lambda Calculus, natural deduction 	[2,3,4 ^a]
Higher Order Logic	[5,6 ^b ,7
Term rewriting	[8,9,10 ^c
 Proof & Specification Techniques 	
• Isar	[11,12 ^d
 Inductively defined sets, rule induction 	[13 ^e ,15
 Datatypes, recursion, induction 	[16,17 ^f ,18,19
 Calculational reasoning, mathematics style proofs 	[20
 Hoare logic, proofs about programs 	[21 ^g ,22,23

^a a1 out; ^ba1 due; ^ca2 out; ^da2 due; ^esession break; ^fa3 out; ^ga3 due

Slide 3



PREVIEW: PROOFS IN ISABELLE

Slide 4

- NICTA

COMP 4161 NICTA Advanced Course

Advanced Topics in Software Verification

Gerwin Klein, June Andronick, Toby Murray

 $\lambda^{
ightarrow}$ and HOL

Slide 1

Eversions from last time	0•
Exercises from last time	NICTA
	NICIA

- → Construct a type derivation tree for the term $\lambda x y z. z x (y x)$
- → Find a unifier (substitution) such that $\lambda x \ y \ z$. ?*F* $y \ z = \lambda x \ y \ z$. 2 (?*G* $x \ y$)

Slide 2

1

Proofs in Isabelle

NICTA

NICTA

General schema:

lemma name: "<goal>"
apply <method>
apply <method>

The Proof State

B

1. $\bigwedge x_1 \dots x_p \cdot \llbracket A_1; \dots; A_n \rrbracket \Longrightarrow B$ **2.** $\bigwedge y_1 \dots y_q \cdot \llbracket C_1; \dots; C_m \rrbracket \Longrightarrow D$

Actual (sub)goal

 $x_1 \dots x_p$ Parameters $A_1 \dots A_n$ Local assumptions

done

→ Sequential application of methods until all **subgoals** are solved.

Isabelle Theories



Syntax:

theory MyTh imports $ImpTh_1\ldots ImpTh_n$ begin (declarations, definitions, theorems, proofs, ...)* end

→ MyTh: name of theory. Must live in file MyTh.thy

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

Unless you need something special:

theory MyTh imports Main begin ... end

Slide 7

Natural Deduction Rules		NICTA
$rac{A B}{A \wedge B}$ conjl	$\frac{A \wedge B [\![A;B]\!] \Longrightarrow C}{C} \operatorname{conjE}$	
$\frac{A}{A \lor B} \frac{B}{A \lor B}$ disjl1/2	$\frac{A \lor B A \Longrightarrow C B \Longrightarrow C}{C} \text{ disjE}$	
$\frac{A \Longrightarrow B}{A \longrightarrow B} \text{ impl}$	$\frac{A \longrightarrow B A B \Longrightarrow C}{C} \text{ impE}$	

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

Slide 5

Slide 8

NICTA

apply assumption

NICTA

proves

1. $\llbracket B_1; \ldots; B_m \rrbracket \Longrightarrow C$

by unifying C with one of the B_i

Proof by assumption

There may be more than one matching B_i and multiple unifiers.

Backtracking!

Explicit backtracking command: back

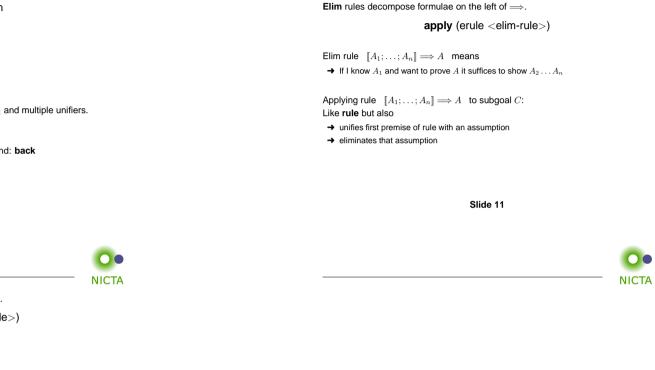
Slide 9

Intro rules	
Intro rules decompose formulae to the right of \Longrightarrow .	itien,
apply (rule <intro-rule>)</intro-rule>	
Intro rule $[\![A_1;\ldots;A_n]\!] \Longrightarrow A$ means \rightarrow To prove A it suffices to show $A_1 \ldots A_n$	

Applying rule $[\![A_1; \ldots; A_n]\!] \Longrightarrow A$ to subgoal C:

 \rightarrow unify A and C

→ replace C with n new subgoals $A_1 \dots A_n$



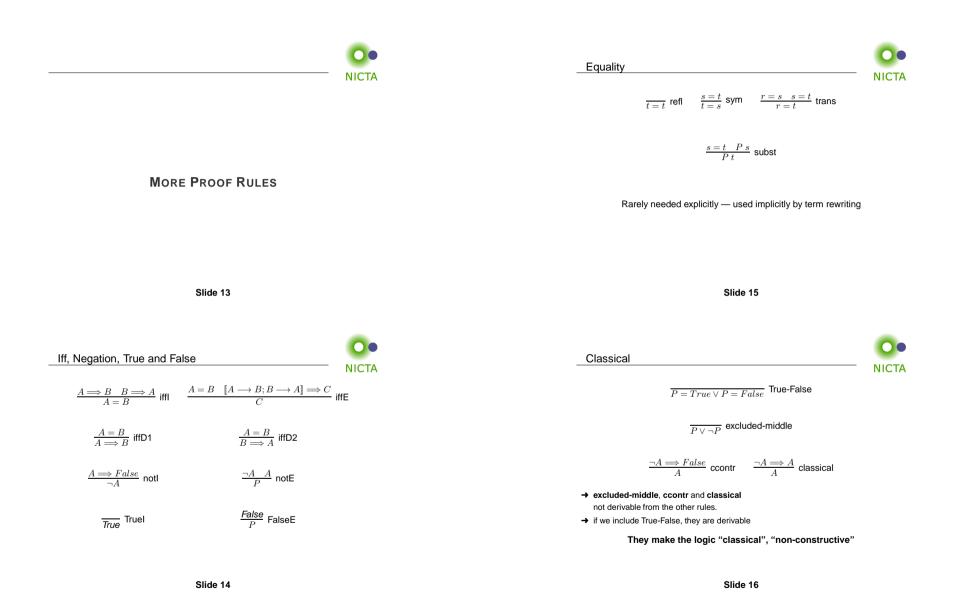
Elim rules

DЕМО

Slide 12

Slide 10

5







- → Redo the demo alone + exercises
- → Assignement 1 is out today!
- → Reminder: DO NOT CHEAT
 - Assignments and exams are take-home. This does NOT mean you can work in groups. Each submission is personal.
 - For more info, see Plagiarism Policy

Slide 21