

# COMP 4161 NICTA Advanced Course

# Advanced Topics in Software Verification

Gerwin Klein, June Andronick, Toby Murray

# Isar

Slide 1

	0.
Content	NICTA
	Rough timeline
→ Intro & motivation, getting started	[1]
→ Foundations & Principles	
<ul> <li>Lambda Calculus, natural deduction</li> </ul>	[2,3,4 <sup>a</sup> ]
Higher Order Logic	[5,6 <sup>b</sup> ,7]
Term rewriting	[8,9,10 <sup>c</sup> ]
➔ Proof & Specification Techniques	
• Isar	[11,12 <sup>d</sup> ]
<ul> <li>Inductively defined sets, rule induction</li> </ul>	[13 <sup>e</sup> ,15]
<ul> <li>Datatypes, recursion, induction</li> </ul>	[16,17 <sup>f</sup> ,18,19]
<ul> <li>Calculational reasoning, mathematics style proofs</li> </ul>	[20]
<ul> <li>Hoare logic, proofs about programs</li> </ul>	[21 <sup>g</sup> ,22,23]



ISAR

# A LANGUAGE FOR STRUCTURED PROOFS

Slide 3

Isar					NICT
		apply scripts		What about	
	→	unreadable	→	Elegance?	
	→	hard to maintain	→	Explaining deeper insights?	
	→	do not scale	→	Large developments?	
	No structure.			Isar!	

<sup>a</sup> a1 out; <sup>b</sup> a1 due; <sup>c</sup> a2 out; <sup>d</sup> a2 due; <sup>e</sup> session break; <sup>f</sup> a3 out; <sup>g</sup> a3 due

Slide 2

Slide 4



NICTA

NICTA

proof [method] statement\* ged

Slide 6

3

Slide 8

# The Three Modes of Isar

→ [prove]:

goal has been stated, proof needs to follow.

 → [state]: proof block has openend or subgoal has been proved, new *from* statement, goal statement or assumptions can follow.
 → [chain]:

from statement has been made, goal statement needs to follow.

lemma " $[A; B] \implies A \land B$ " [prove] proof (rule conjl) [state] assume A: "A" [state] from A [chain] show "A" [prove] by assumption [state] next [state] ...

Slide 9

NICTA

NICTA

Have			

Can be used to make intermediate steps.

#### Example:

```
lemma "(x :: nat) + 1 = 1 + x"
proof -
have A: "x + 1 = Suc x" by simp
have B: "1 + x = Suc x" by simp
```

show "x + 1 = 1 + x" by (simp only: A B)

# qed



NICTA

**D**емо

Slide 11

# Backward and Forward

## Backward reasoning: ... have " $A \land B$ " proof

- → proof picks an intro rule automatically
- → conclusion of rule must unify with  $A \land B$

#### Forward reasoning: ....

#### assume AB: " $A \land B$ "

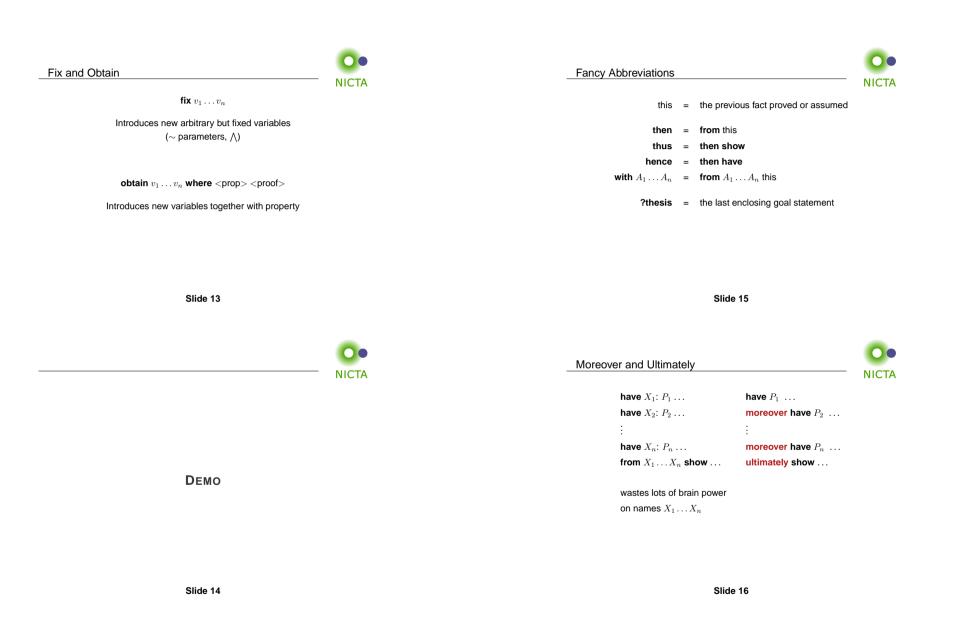
- from AB have "..." proof
- → now proof picks an elim rule automatically
- → triggered by from
- → first assumption of rule must unify with AB

### General case: from $A_1 \dots A_n$ have R proof

- $\rightarrow$  first *n* assumptions of rule must unify with  $A_1 \dots A_n$
- $\rightarrow$  conclusion of rule must unify with R

Slide 10

Slide 12



```
General Case Distinctionsshow formulaproof -have P_1 \lor P_2 \lor P_3 < proof >moreover { assume P_1 \dots have ?thesis < proof >}moreover { assume P_2 \dots have ?thesis < proof >}ultimately show ?thesis by blastqed{ ... } is a proof block similar to proof ... qed{ assume P_1 \dots have P < proof > }stands for P_1 \implies PSlide 17
```

Mixing proof styles	<b>O</b> • NICTA
from have apply - make incoming facts assumptions apply ( )	
: apply ( ) done	

