COMP 4161

NICTA Advanced Course

Advanced Topics in Software Verification

Gerwin Klein, June Andronick, Toby Murray

Slide 1

Content

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; [b] a1 due; [c] a2 out; [d] a2 due; [e] session break; [f] a3 out; [g] a3 due

Slide 2

DATATYPES IN ISAR

Slide 3

Datatype case distinction

proof (cases $term$)
  case Constructor$_1$
  $\vdots$
next
$\vdots$
next
  case (Constructor$_k$ $\vec{x}$)
  $\cdots\ \vec{x}\ \cdots$
qed

case (Constructor$_i$ $\vec{x}$) $\equiv$

fix $\vec{x}$ **assume** Constructor$_i$: "$term =$ Constructor$_i$ $\vec{x}$"

Slide 4

Structural induction for type nat

NICTA

show $P\ n$
proof (induct n)
  case 0 $\equiv$ **let** $?case$ = $P\ 0$
  $\ldots$
  show $?case$
next
  case (Suc n) $\equiv$ **fix** n **assume** Suc: $P\ n$
  $\ldots$ **let** $?case$ = P (Suc n)
  $\cdots\ n\ \cdots$
  show $?case$
qed

Slide 5

Structural induction with $\Longrightarrow$ and $\bigwedge$

NICTA

show "$\bigwedge x.\ A\ n \Longrightarrow P\ n$"
proof (induct n)
  case 0 $\equiv$ **fix** x **assume** 0: "$A\ 0$"
  $\ldots$ **let** $?case$ = "$P\ 0$"
  show $?case$
next
  case (Suc n) $\equiv$ **fix** n and x
  $\ldots$ **assume** Suc: "$\bigwedge x.\ A\ n \Longrightarrow P\ n$"
  $\cdots\ n\ \cdots$ "A (Suc n)"
  $\ldots$ **let** $?case$ = "P (Suc n)"
  show $?case$
qed

Slide 6

NICTA

DEMO: DATATYPES IN ISAR

Slide 7

NICTA

DEMO: REGULAR EXPRESSIONS

Slide 8

We have seen today ...

NICTA

- ➜ Datatypes in Isar
- ➜ Defining regular wxpressions as a data type
- ➜ Playing with recursion and induction

Slide 9