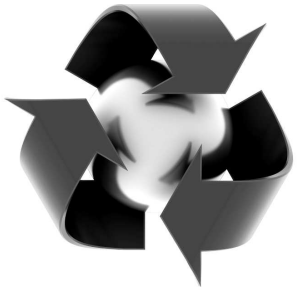
NICTA

COMP 4161

NICTA Advanced Course

Advanced Topics in Software Verification

Gerwin Klein, June Andronick, Toby Murray



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

Datatypes in Isar

Datatype case distinction

NICTA

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

case (Constructor$_i$ $\vec{x}$) $\equiv$
fix $\vec{x}$ **assume** Constructor$_i$: "$term$ = Constructor$_i$ $\vec{x}$"

Structural induction for type nat

show $P\ n$

proof (induct n)

  case 0 $\equiv$ **let** $?case = P\ 0$

  ...

  show $?case$

next

  case (Suc n) $\equiv$ **fix** n **assume** Suc: $P\ n$

  ... **let** $?case = P\ (\text{Suc}\ n)$

  $\cdots\ n\ \cdots$

  show $?case$

qed

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

NICTA

Demo: Datatypes in Isar

NICTA

Demo: Regular Expressions

We have seen today ...

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