COMP 4161
NICTA Advanced Course

Advanced Topics in Software Verification

Gerwin Klein, June Andronick, Toby Murray
Rough timeline

Intro & motivation, getting started [1]

Foundations & Principles
- Lambda Calculus, natural deduction [2,3,4]
- Higher Order Logic [5,6,7]
- Term rewriting [8,9,10]

Proof & Specification Techniques
- Isar [11,12]
- Inductively defined sets, rule induction [13,15]
- Datatypes, recursion, induction [16,17,18,19]
- Calculational reasoning, mathematics style proofs [20]
- Hoare logic, proofs about programs [21,22,23]

a1 out; a1 due; a2 out; a2 due; session break; a3 out; a3 due
DATATYPES IN ISAR
Datatype case distinction

proof (cases term)
  case Constructor_1
    · · ·
  next
    · · ·
  next
    case (Constructor_k \vec{x})
    · · · \vec{x} · · ·
qed

\begin{align*}
\text{case } (\text{Constructor}_i \vec{x}) \quad &\equiv \\
\text{fix } \vec{x} \text{ assume Constructor}_i : "term = \text{Constructor}_i \vec{x}\"
\end{align*}
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 $?case = P \, (\text{Suc} \, n)$

  ... $n$ ...

  show $?case$

qed
 Structural induction with $\implies$ and $\land$

show "$\land x. A\ n \implies P\ n$"

proof (induct $n$)
  case 0
    ... show ?case

next
case (Suc $n$)
  ... $n$ ...
  ... show ?case

qed
DEMO: DATATYPES IN ISAR
DEMO: REGULAR EXPRESSIONS
We have seen today ...

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