NICTA

COMP 4161

NICTA Advanced Course

Advanced Topics in Software Verification

Gerwin Klein
Formal Methods

wf_rec

Content

Datatypes in Isar

proof (cases $term$)

case Constructor_1

⋮

next

⋮

next

case (Constructor_k $\vec{x}$)

$\ldots\ \vec{x}\ \ldots$

qed

case (Constructor_i $\vec{x}$) $\equiv$

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

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)

  $\ldots\ n\ \ldots$

  show $?case$

qed

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: "$\bigwedge x.\ A\ n \Longrightarrow P\ n$"
  $\cdots\ n\ \cdots$ "A (Suc n)"
  . . . **let** $?case$ = "P (Suc n)"
  show $?case$
qed

DEMO