COMP340-08B Reasoning About Programs

14. Proof by Induction

Robi Malik

THE UNIVERSITY OF WAIKATO
DEPARTMENT OF COMPUTER SCIENCE
TARI ROROHIKO

Principle of Induction

$$(p(0) \wedge \forall x\ (\mathrm{nat}(x) \wedge p(x) \rightarrow p(s(x))) \rightarrow \forall x\ (\mathrm{nat}(x) \rightarrow p(x))$$

To prove a property **P** of all natural numbers:

Inductive base. Prove that 0 satisfies **P**.

Inductive hypothesis. Assume that some number n satisfies **P**.

Inductive step. Using the inductive hypothesis, prove that $n+1$ satisfies **P**.

About the RISC Proof Navigator

- Type `ProofNavigator` to start
- Homepage and download
  `http://www.risc-uni-linz.ac.at/research/formal/software/ProofNavigator`
- Local copies of documentation on the COMP340-08B homepage in Moodle:
  - → Online manual available from `Help` menu or from the homepage
  - → Read the tutorial (section 3.1 of the manual)

Example

Proving

(Claim) $\forall x{:}\mathbb{N}\ \ x + 0 = x$

from the axioms

(A1) $\forall x{:}\mathbb{N}\ \ 0 + x = x$

(A2) $\forall x{:}\mathbb{N}, y{:}\mathbb{N}\ \ s(x) + y = s(x + y)$

Inductive base.
$0 + 0 = 0$ by axiom (A1)

Inductive hypothesis.
$n + 0 = n$ for some $n \in \mathbb{N}$

Inductive step.
$s(n) + 0 = s(n + 0) = s(n)$ □

By Axiom (A2)

By Inductive hypothesis

Example Proofs with ProofNavigator

Definition

$\mathrm{divides}(x, y) \equiv \exists n{:}\mathbb{N}\ n \cdot x = y$

Theorems to prove

(DIV_0) $\forall x{:}\mathbb{N}\ \ \mathrm{divides}(x, 0)$

(DIV_{self}) $\forall x{:}\mathbb{N}\ \ \mathrm{divides}(x, x)$

(DIV_1) $\forall x{:}\mathbb{N}\ \ \mathrm{divides}(1, x)$

```
expand divides;
scatter;
instantiate 0 in h36;
instantiate x_0 in gwo;
```

```
scatter;
expand divides;
instantiate 1 in gpq;
lemma MULT_1a;
auto xdm;
```


Reading on Induction

Huth & Ryan:
Section 1.4.2
pp. 40–45.

To be Proven by Induction

$\forall x{:}\mathbb{N}\ \ x + 0 = x$

$\forall x{:}\mathbb{N}, y{:}\mathbb{N}, z{:}\mathbb{N}\ \ (x + y) + z = x + (y + z)$

$\forall x{:}\mathbb{N}, y{:}\mathbb{N}\ \ x + y = y + x$

$\forall x{:}\mathbb{N}\ \ x \cdot 0 = 0$

$\forall x{:}\mathbb{N}\ \ x \cdot 1 = x$

$\forall x{:}\mathbb{N}, y{:}\mathbb{N}, z{:}\mathbb{N}\ \ (x + y) \cdot z = x \cdot z + y \cdot z$

$\forall x{:}\mathbb{N}, y{:}\mathbb{N}, z{:}\mathbb{N}\ \ x \cdot (y + z) = x \cdot y + x \cdot z$

$\forall x{:}\mathbb{N}, y{:}\mathbb{N}, z{:}\mathbb{N}\ \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$

$\forall x{:}\mathbb{N}, y{:}\mathbb{N}\ \ x \cdot y = y \cdot x$

ProofNavigator Proof Script

```
induction x in cql;
scatter;
auto;
scatter;
instantiate x_0, mult(y_0,z_0) in fcb;
instantiate y_0, z_0 in bwe;
lemma MULT_dist;
instantiate mult(x_0,y_0), y_0, z_0 in x3a;
instantiate x_0, y_0 in fcb;
```

induction command must be invoked first!

Inductive base is easy.

Another Example

Proving

(Claim) $\forall x{:}\mathbb{N}, y{:}\mathbb{N}, z{:}\mathbb{N}\ \ x \cdot (y \cdot z) = (x \cdot y) \cdot z$

from the axioms

(M1) $\forall x{:}\mathbb{N}\ \ 0 \cdot x = 0$

(M2) $\forall x{:}\mathbb{N}, y{:}\mathbb{N}\ (x + 1) \cdot y = x \cdot y + y$

by induction on x …

Inductive base.

$0 \cdot (y \cdot z) = 0 = 0 \cdot z = (0 \cdot y) \cdot z$ by axiom (M1)

Yet Another Example

Proving

(Claim) $\forall x{:}\mathbb{N}, y{:}\mathbb{N}\ \ x \cdot y = y \cdot x$

by induction on x …

Inductive base: $x = 0$

$0 \cdot x = 0 = x \cdot 0$ using lemma $\forall x{:}\mathbb{N}\ x \cdot 0 = 0$

Inductive hypothesis: $x = n$

$\forall y{:}\mathbb{N}\ n \cdot y = y \cdot n$ for some $n \in \mathbb{N}$

Inductive step: $x = n \rightsquigarrow x = n + 1$

is proven by induction on y …

Example continued

Inductive hypothesis.

$\forall y{:}\mathbb{N}, z{:}\mathbb{N}\ \ n \cdot (y \cdot z) = (n \cdot y) \cdot z$ for some $n \in \mathbb{N}$

Inductive step.

$(n + 1) \cdot (y \cdot z)$

$= n \cdot (y \cdot z) + y \cdot z$ by axiom (M2)

$= (n \cdot y) \cdot z + y \cdot z$ by inductive hypothesis

$= (n \cdot y + y) \cdot z$ by distributivity

$= ((n + 1) \cdot y) \cdot z$ by axiom (M2) □

Nested Induction

Inductive base: $y = 0$

$(n + 1) \cdot 0 = 0 = 0 \cdot (n + 1)$ using lemma $\forall x{:}\mathbb{N}\ \ x \cdot 0 = 0$

Inductive hypothesis: $y = m$

$(n + 1) \cdot m = m \cdot (n + 1)$ for some $m \in \mathbb{N}$

Inductive step: $y = m \rightsquigarrow y = m + 1$

$(n + 1) \cdot (m + 1)$

$= n \cdot (m + 1) + (m + 1)$ by axiom (M2)

$= (m + 1) \cdot n + m + 1$ by inductive hypothesis for n

$= m \cdot n + n + m + 1$ by axiom (M2)

$= n \cdot m + m + n + 1$ by inductive hypothesis for n

$= (n + 1) \cdot m + n + 1$ by axiom (M2)

$= m \cdot (n + 1) + n + 1$ by inductive hypothesis for m

$= (m + 1) \cdot (n + 1)$ by axiom (M2) □