CS3202: Logic, Specification and Verification

CS3202-LSV 2006–07

cs3202.lec@cs.st-andrews.ac.uk

Dr. James McKinna, RM 1.03

Dr. Stéphane Lengrand, Rm. 1.02

Lecture 7 (12/03/2007):

Induction

Problem

Term language of 1^{st}-order logic is not (quite) sufficient to prove properties of *data* D:

$$\forall x : D, P\ x$$

Problem

Term language of 1^{st}-order logic is not (quite) sufficient to prove properties of *data* D:

$$\forall x : D, P\ x$$

$\forall$-intro shows how to prove this for the *arbitrary* x;

but no insight obtainable into what forms such x may take.

Problem

Term language of 1^{st}-order logic is not (quite) sufficient to prove properties of *data* D:

$$\forall x : D, P\ x$$

$\forall$-intro shows how to prove this for the *arbitrary* x;

but no insight obtainable into what forms such x may take.

e.g. $\mathbb{B} = \{\texttt{true}, \texttt{false}\}$ We know $\mathbb{B}$ has two elements.

$\mathbb{C}$omp $= \{\texttt{LT}, \texttt{EQ}, \texttt{GT}\}$ $\mathbb{C}$omp has three (and some other stuff).

Problem

Term language of 1^{st}-order logic is not (quite) sufficient to prove properties of *data* D:

$$\forall x : D, P\ x$$

$\forall$-intro shows how to prove this for the *arbitrary* x;

but no insight obtainable into what forms such x may take.

e.g. $\mathbb{B} = \{\mathtt{true}, \mathtt{false}\}$ We know $\mathbb{B}$ has two elements.

$\mathbb{C}$omp $= \{\mathtt{LT}, \mathtt{EQ}, \mathtt{GT}\}$ $\mathbb{C}$omp has three (and some other stuff).

Natural numbers

$$\mathbb{N} = \{0, 1, 2, 3 \ldots\}$$

Natural numbers

$\mathbb{N} = \{0, 1, 2, 3 \ldots\}$

$\mathbb{N}$ has *lots* of structure (addition, multiplication, less-than relation, etc.)

Natural numbers

$\mathbb{N} = \{0, 1, 2, 3 \ldots\}$

$\mathbb{N}$ has *lots* of structure (addition, multiplication, less-than relation, etc.)

We could imagine a 1^{st}-order language with *all* the *names* of elements of $\mathbb{N}$, but still not be able to prove anything about them (without also throwing all the atomic propositions $3 < 4$ etc. in as well).

Natural numbers

$\mathbb{N} = \{0, 1, 2, 3 \ldots\}$

$\mathbb{N}$ has *lots* of structure (addition, multiplication, less-than relation, etc.)

We could imagine a 1^{st}-order language with *all* the *names* of elements of $\mathbb{N}$, but still not be able to prove anything about them (without also throwing all the atomic propositions $3 < 4$ etc. in as well).

Natural numbers

But we know this about $\mathbb{N}$ (roughly speaking, Peano's 1887 axioms 1–5):

1. $0 \in \mathbb{N}$ "there is a natural number"
2. if $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$ "there is a successor (function)"
3. if $n + 1 = m + 1$ then $n = m$ "the successor function is injective"
4. $0 \neq n + 1$ for any n (discrimination)

   otherwise put: if $0 = 1$ then anything might be true

Natural numbers

But we know this about $\mathbb{N}$ (roughly speaking, Peano's 1887 axioms 1–5):

1. $0 \in \mathbb{N}$ "there is a natural number"
2. if $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$ "there is a successor (function)"
3. if $n + 1 = m + 1$ then $n = m$ "the successor function is injective"
4. $0 \neq n + 1$ for any n (discrimination)

   otherwise put: if $0 = 1$ then anything might be true
5. *Induction.* 1) and 2) characterise $\mathbb{N}$:

   if [a property P holds of 0]

   and [for any $n \in \mathbb{N}$, if P holds of n then P holds of $n + 1$]

   then P holds of any number $n \in \mathbb{N}$

Natural numbers

But we know this about $\mathbb{N}$ (roughly speaking, Peano's 1887 axioms 1–5):

1. $0 \in \mathbb{N}$ "there is a natural number"
2. if $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$ "there is a successor (function)"
3. if $n + 1 = m + 1$ then $n = m$ "the successor function is injective"
4. $0 \neq n + 1$ for any n (discrimination)

   otherwise put: if $0 = 1$ then anything might be true
5. *Induction.* 1) and 2) characterise $\mathbb{N}$:

   if [a property P holds of 0]

   and [for any $n \in \mathbb{N}$, if P holds of n then P holds of $n + 1$]

   then P holds of any number $n \in \mathbb{N}$

Induction on natural numbers

Rule of mathematical induction on $\mathbb{N}$:

$$\dfrac{P\,0 \qquad \begin{matrix} [m:\mathbb{N}] \quad [P\,m] \\ \vdots \\ P\,(m+1) \end{matrix}}{\forall n:\mathbb{N}, P\,n}$$

Induction on natural numbers

Rule of mathematical induction on $\mathbb{N}$:

$$\frac{P\,0 \qquad \begin{array}{c}[m:\mathbb{N}] \qquad [P\,m] \\ \vdots \\ P\,(m+1)\end{array}}{\forall n:\mathbb{N}, P\,n}$$

Alternative with explicit equations

$$\frac{\begin{array}{c}[n:\mathbb{N}] \qquad [n=0] \\ \vdots \\ P\,n\end{array} \qquad \begin{array}{c}[m,n:\mathbb{N}] \qquad [P\,m] \qquad [n=m+1] \\ \vdots \\ P\,n\end{array}}{\forall n:\mathbb{N}, P\,n}$$

Induction on natural numbers

Rule of mathematical induction on $\mathbb{N}$:

$$\frac{P\,0 \qquad \begin{array}{c}[m:\mathbb{N}] \quad [P\,m] \\ \vdots \\ P\,(m+1)\end{array}}{\forall n:\mathbb{N}, P\,n}$$

Alternative with explicit equations

$$\frac{\begin{array}{c}[n:\mathbb{N}] \quad [n=0] \\ \vdots \\ P\,n\end{array} \qquad \begin{array}{c}[m,n:\mathbb{N}] \quad [P\,m] \quad [n=m+1] \\ \vdots \\ P\,n\end{array}}{\forall n:\mathbb{N}, P\,n}$$

Alternative as an implication

$$P(0) \Rightarrow [\forall m:\mathbb{N}, P(m) \Rightarrow P(m+1)] \Rightarrow \forall n:\mathbb{N}, P(n)$$

Induction on natural numbers

Rule of mathematical induction on $\mathbb{N}$:

$$\frac{P\,0 \qquad \begin{array}{c} [m:\mathbb{N}] \quad [P\,m] \\ \vdots \\ P\,(m+1) \end{array}}{\forall n:\mathbb{N}, P\,n}$$

Alternative with explicit equations

$$\frac{\begin{array}{c} [n:\mathbb{N}] \quad [n=0] \\ \vdots \\ P\,n \end{array} \qquad \begin{array}{c} [m,n:\mathbb{N}] \quad [P\,m] \quad [n=m+1] \\ \vdots \\ P\,n \end{array}}{\forall n:\mathbb{N}, P\,n}$$

Alternative as an implication

$$P(0) \Rightarrow [\forall m:\mathbb{N}, P(m) \Rightarrow P(m+1)] \Rightarrow \forall n:\mathbb{N}, P(n)$$

Other data structures

Booleans:

$$\frac{P\ \texttt{true} \qquad P\ \texttt{false}}{\forall b : \mathbb{B}, P\ b}$$

Other data structures

Booleans: $$\frac{P\ \mathtt{true} \qquad P\ \mathtt{false}}{\forall b : \mathbb{B}, P\ b}$$

Comparators (a function $A \to A \to \mathbb{C}\text{omp}$ simulates an ordering on A):

$$\frac{P\ \mathtt{LT} \qquad P\ \mathtt{EQ} \qquad P\ \mathtt{GT}}{\forall c : \mathbb{C}\text{omp}, P\ c}$$

Other data structures

Booleans:

$$\frac{P\ \mathtt{true} \qquad P\ \mathtt{false}}{\forall b : \mathbb{B}, P\ b}$$

Comparators (a function $A \to A \to \mathbb{C}\text{omp}$ simulates an ordering on A):

$$\frac{P\ \mathtt{LT} \qquad P\ \mathtt{EQ} \qquad P\ \mathtt{GT}}{\forall c : \mathbb{C}\text{omp}, P\ c}$$

In each case, the universal conclusion $\forall d : D, P\ d$ follows from

- one case for each way of forming a new data item –via *constructors*
- we can assume (*inductive hypothesis*) P holds for “smaller” data when proving P holds for data built by constructors.

Other data structures

Booleans: $$\frac{P\ \texttt{true} \qquad P\ \texttt{false}}{\forall b : \mathbb{B}, P\ b}$$

Comparators (a function $A \rightarrow A \rightarrow \mathbb{C}\text{omp}$ simulates an ordering on A):

$$\frac{P\ \texttt{LT} \qquad P\ \texttt{EQ} \qquad P\ \texttt{GT}}{\forall c : \mathbb{C}\text{omp}, P\ c}$$

In each case, the universal conclusion $\forall d : D, P\ d$ follows from

- one case for each way of forming a new data item –via *constructors*
- we can assume (*inductive hypothesis*) P holds for “smaller” data when proving P holds for data built by constructors.

Questions?