Sets

Overview

- Set notation
- Inductively defined sets

Set notation

Sets

Sets over type *’a*:

’a set

Sets

Sets over type *'a*:

$$'a\ set \quad = \quad 'a \Rightarrow bool$$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- *{}*, *{*$e_1, \ldots, e_n$*}*, *{x. P x}*

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1,\ldots,e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, $A - B$, $-A$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, $A - B$, $-A$
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, $A - B$, $-A$
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$
- $\{i..j\}$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1, \ldots, e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, $A - B$, $- A$
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$
- $\{i..j\}$
- *insert* :: $\textit{'a} \Rightarrow \textit{'a set} \Rightarrow \textit{'a set}$

Sets

Sets over type *'a*:

$$\textit{'a set} \quad = \quad \textit{'a} \Rightarrow \textit{bool}$$

- $\{\}$, $\{e_1,\ldots,e_n\}$, $\{x.\ P\ x\}$
- $e \in A$, $A \subseteq B$
- $A \cup B$, $A \cap B$, $A - B$, $-A$
- $\bigcup_{x \in A} B\ x$, $\bigcap_{x \in A} B\ x$
- $\{i..j\}$
- $\textit{insert} :: \textit{'a} \Rightarrow \textit{'a set} \Rightarrow \textit{'a set}$
- $\ldots$

Proofs about sets

Natural deduction proofs:

- `equalityI`: $\llbracket A \subseteq B;\ B \subseteq A \rrbracket \Longrightarrow A = B$

Proofs about sets

Natural deduction proofs:

- `equalityI`: $[\![A \subseteq B; B \subseteq A]\!] \Longrightarrow A = B$
- `subsetI`: $(\bigwedge x.\ x \in A \Longrightarrow x \in B) \Longrightarrow A \subseteq B$

Proofs about sets

Natural deduction proofs:

- `equalityI`: $[\![A \subseteq B; B \subseteq A]\!] \Longrightarrow A = B$
- `subsetI`: $(\bigwedge x.\ x \in A \Longrightarrow x \in B) \Longrightarrow A \subseteq B$
- ... (see Tutorial)

Demo: proofs about sets

Bounded quantifiers

- $\forall x \in A.\ P\ x$

Bounded quantifiers

- $\forall x \in A.\ P\ x \quad \equiv \quad \forall x.\ x \in A \longrightarrow P\ x$

Bounded quantifiers

- $\forall x \in A.\ P\ x \quad \equiv \quad \forall x.\ x \in A \longrightarrow P\ x$
- $\exists x \in A.\ P\ x$

Bounded quantifiers

- $\forall x \in A.\ P\ x \quad \equiv \quad \forall x.\ x \in A \longrightarrow P\ x$
- $\exists x \in A.\ P\ x \quad \equiv \quad \exists x.\ x \in A \wedge P\ x$

Bounded quantifiers

- $\forall x{\in}A.\ P\ x \quad \equiv \quad \forall x.\ x{\in}A \longrightarrow P\ x$
- $\exists x{\in}A.\ P\ x \quad \equiv \quad \exists x.\ x{\in}A \wedge P\ x$
- `ballI`: $(\bigwedge x.\ x \in A \Longrightarrow P\ x) \Longrightarrow \forall x{\in}A.\ P\ x$
- `bspec`: $[\![\forall x{\in}A.\ P\ x;\ x \in A]\!] \Longrightarrow P\ x$

Bounded quantifiers

- $\forall x{\in}A.\ P\ x \quad \equiv \quad \forall x.\ x{\in}A \longrightarrow P\ x$
- $\exists x{\in}A.\ P\ x \quad \equiv \quad \exists x.\ x{\in}A \wedge P\ x$
- `ballI`: $(\bigwedge x.\ x \in A \Longrightarrow P\ x) \Longrightarrow \forall x{\in}A.\ P\ x$
- `bspec`: $[\![\forall x{\in}A.\ P\ x;\ x \in A]\!] \Longrightarrow P\ x$
- `bexI`: $[\![P\ x;\ x \in A]\!] \Longrightarrow \exists x{\in}A.\ P\ x$
- `bexE`: $[\![\exists x{\in}A.\ P\ x;\ \bigwedge x.\ [\![x \in A;\ P\ x]\!] \Longrightarrow Q]\!] \Longrightarrow Q$

Inductively defined sets

Example: even numbers

Informally:

Example: even numbers

Informally:

- 0 is even

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n + 2$

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n + 2$
- These are the only even numbers

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n + 2$
- These are the only even numbers

In Isabelle/HOL:

inductive_set *Ev :: nat set* — The set of all even numbers

Example: even numbers

Informally:

- 0 is even
- If n is even, so is $n + 2$
- These are the only even numbers

In Isabelle/HOL:

inductive_set *Ev :: nat set* — The set of all even numbers
where
$0 \in Ev \quad |$
$n \in Ev \Longrightarrow n + 2 \in Ev$

Format of inductive definitions

inductive_set $S :: \tau\ set$

Format of inductive definitions

inductive_set S :: τ *set*

where

$\llbracket\ a_1 \in S;\ \ldots\ ;\ a_n \in S;\ A_1;\ \ldots;\ A_k\ \rrbracket \Longrightarrow a \in S\quad |$

$\vdots$

Format of inductive definitions

inductive_set $S :: \tau$ *set*

where

$[\![a_1 \in S; \ldots ; a_n \in S; A_1; \ldots; A_k]\!] \Longrightarrow a \in S \quad |$

$\vdots$

where $A_1; \ldots; A_k$ are side conditions not involving S.

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m+m \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m+m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m+m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0{+}0 \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0{+}0 \in Ev$
- rule $n \in Ev \Longrightarrow n{+}2 \in Ev$

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m{+}m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0{+}0 \in Ev$
- rule $n \in Ev \Longrightarrow n{+}2 \in Ev$
  $\Longrightarrow m = n{+}2$ and $n{+}n \in Ev$ (ind. hyp.!)

Proving properties of even numbers

Easy: $4 \in Ev$

$$0 \in Ev \Longrightarrow 2 \in Ev \Longrightarrow 4 \in Ev$$

Trickier: $m \in Ev \Longrightarrow m+m \in Ev$

Idea: induction on the length of the derivation of $m \in Ev$

Better: induction on the *structure* of the derivation

Two cases: $m \in Ev$ is proved by

- rule $0 \in Ev$
  $\Longrightarrow m = 0 \Longrightarrow 0+0 \in Ev$
- rule $n \in Ev \Longrightarrow n+2 \in Ev$
  $\Longrightarrow m = n+2$ and $n+n \in Ev$ (ind. hyp.!)
  $\Longrightarrow m+m = (n+2)+(n+2) = ((n+n)+2)+2 \in Ev$

Rule induction for *Ev*

To prove

$$n \in Ev \Longrightarrow P\ n$$

by *rule induction* on $n \in Ev$ we must prove

Rule induction for Ev

To prove

$$n \in Ev \Longrightarrow P\ n$$

by *rule induction* on $n \in Ev$ we must prove

- $P\ 0$

Rule induction for Ev

To prove

$$n \in Ev \Longrightarrow P\ n$$

by *rule induction* on $n \in Ev$ we must prove

- $P\ 0$
- $P\ n \Longrightarrow P(n+2)$

Rule induction for Ev

To prove

$$n \in Ev \Longrightarrow P\ n$$

by *rule induction* on $n \in Ev$ we must prove

- $P\ 0$
- $P\ n \Longrightarrow P(n+2)$

Rule `Ev.induct`:

$$\llbracket\, n \in Ev;\ P\ 0;\ \bigwedge n.\ P\ n \Longrightarrow P(n+2)\,\rrbracket \Longrightarrow P\ n$$

Rule induction in general

Set S is defined inductively.

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\,x$$

by *rule induction* on $x \in S$

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\ x$$

by *rule induction* on $x \in S$
we must prove for every rule

$$[\![\ a_1 \in S; \ \ldots\ ; a_n \in S\ ]\!] \Longrightarrow a \in S$$

that P is preserved:

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\ x$$

by *rule induction* on $x \in S$
we must prove for every rule

$$[\![\ a_1 \in S; \ldots ; a_n \in S\ ]\!] \Longrightarrow a \in S$$

that P is preserved:

$$[\![\ P\ a_1; \ldots ; P\ a_n\ ]\!] \Longrightarrow P\ a$$

Rule induction in general

Set S is defined inductively.
To prove

$$x \in S \Longrightarrow P\ x$$

by *rule induction* on $x \in S$
we must prove for every rule

$$[\![\ a_1 \in S; \ldots ; a_n \in S\ ]\!] \Longrightarrow a \in S$$

that P is preserved:

$$[\![\ P\ a_1; \ldots ; P\ a_n\ ]\!] \Longrightarrow P\ a$$

In Isabelle/HOL:

apply(*induct rule: S.induct*)

Demo: inductively defined sets

Inductive predicates

$$x \in S \quad \leadsto \quad S\,x$$

Inductive predicates

$$x \in S \quad \rightsquigarrow \quad S\,x$$

Example:

inductive $Ev :: nat \Rightarrow bool$

where

$Ev\ 0 \quad |$

$Ev\ n \Longrightarrow Ev\ (n + 2)$

Inductive predicates

$$x \in S \;\leadsto\; S\ x$$

Example:

inductive $Ev :: nat \Rightarrow bool$

where

$Ev\ 0 \quad |$

$Ev\ n \Longrightarrow Ev\ (n + 2)$

Comparison:

predicate: simpler syntax

set: direct usage of $\cup$ etc

Inductive predicates

$$x \in S \quad \rightsquigarrow \quad S\ x$$

Example:

inductive *Ev :: nat* $\Rightarrow$ *bool*

where

Ev 0 |

Ev n $\Longrightarrow$ *Ev (n + 2)*

Comparison:

predicate: simpler syntax

set: direct usage of $\cup$ etc

Inductive predicates can be of type $\tau_1 \Rightarrow \ldots \Rightarrow \tau_n \Rightarrow$ *bool*