Sets

Overview

- Set notation
- Inductively defined sets

Set notation

Sets

Type *'a set*: sets over type *'a*

Sets

Type *'a set*: sets over type *'a*

- *{}*, *{e*$_1$,...,*e*$_n$*}*, *{x. P x}*

Sets

Type *'a set*: sets over type *'a*

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

Sets

Type *'a set*: sets over type *'a*

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

Sets

Type *'a set*: sets over type *'a*

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

Sets

Type *'a set*: sets over type *'a*

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

Sets

Type *'a set*: sets over type *'a*

- *{}*, *{e*$_1$*,...,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 :: 'a* $\Rightarrow$ *'a set* $\Rightarrow$ *'a set*

Sets

Type *'a set*: sets over type *'a*

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

Sets

Type *'a set*: sets over type *'a*

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

Proofs about sets

Natural deduction proofs:

- `equalityI`: $[\![A \subseteq B;\ B \subseteq A]\!] \Longrightarrow A = B$

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`: $\llbracket A \subseteq B; B \subseteq A \rrbracket \Longrightarrow A = B$
- `subsetI`: $(\bigwedge x.\ x \in A \Longrightarrow x \in B) \Longrightarrow A \subseteq B$
- $\ldots$ (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: finite sets

Informally:

Example: finite sets

Informally:

- The empty set is finite

Example: finite sets

Informally:

- The empty set is finite
- Adding an element to a finite set yields a finite set

Example: finite sets

Informally:

- The empty set is finite
- Adding an element to a finite set yields a finite set
- These are the only finite sets

Example: finite sets

Informally:

- The empty set is finite
- Adding an element to a finite set yields a finite set
- These are the only finite sets

In Isabelle/HOL:

consts *Fin :: 'a set set* — The set of all finite set

Example: finite sets

Informally:

- The empty set is finite
- Adding an element to a finite set yields a finite set
- These are the only finite sets

In Isabelle/HOL:

consts *Fin :: 'a set set* — The set of all finite set

inductive *Fin*

Example: finite sets

Informally:

- The empty set is finite
- Adding an element to a finite set yields a finite set
- These are the only finite sets

In Isabelle/HOL:

consts *Fin :: 'a set set* — The set of all finite set

inductive *Fin*

intros

$\{\} \in Fin$

$A \in Fin \Longrightarrow insert\ a\ A \in Fin$

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:

consts *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:

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

inductive *Ev*

Example: even numbers

Informally:

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

In Isabelle/HOL:

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

inductive *Ev*

intros

$0 \in Ev$

$n \in Ev \Longrightarrow n + 2 \in Ev$

Format of inductive definitions

consts $S :: \tau\ set$

Format of inductive definitions

consts $S :: \tau\ set$

inductive S

Format of inductive definitions

consts $S :: \tau$ *set*

inductive S

intros

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

$\vdots$

Format of inductive definitions

consts S :: τ *set*

inductive S

intros

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

$\vdots$

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: $4 \in Ev$

$$0 \in Ev \implies 2 \in Ev \implies 4 \in Ev$$

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

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 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`:

$$[\![\ n \in Ev;\ P\ 0;\ \bigwedge n.\ P\ n \Longrightarrow P(n+2)\ ]\!] \Longrightarrow P\ n$$

An elimination rule

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(*erule S.induct*)

Demo: inductively defined sets