
Sets

Overview

- Set notation
- Inductively defined sets

Set notation

Sets

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

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

Proofs about sets

Natural deduction proofs:

- equalityI: $\llbracket A \subseteq B; B \subseteq A \rrbracket \Longrightarrow A = B$
- subsetI: $(\bigwedge x. x \in A \Longrightarrow x \in B) \Longrightarrow A \subseteq B$
- ... (see Tutorial)

Demo: proofs about sets

Bounded quantifiers

- $\forall x \in A. P x \equiv \forall x. x \in A \longrightarrow P x$
- $\exists x \in A. P x \equiv \exists x. x \in A \wedge P x$
- ballI: $(\wedge x. x \in A \implies P x) \implies \forall x \in A. P x$
- bspec: $\llbracket \forall x \in A. P x; x \in A \rrbracket \implies P x$
- bexI: $\llbracket P x; x \in A \rrbracket \implies \exists x \in A. P x$
- bexE: $\llbracket \exists x \in A. P x; \wedge x. \llbracket x \in A; P x \rrbracket \implies Q \rrbracket \implies Q$

Inductively defined 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

inductive *Fin*

intros

$\{\} \in Fin$

$A \in Fin \implies insert\ a\ A \in Fin$

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

$0 \in Ev$

$n \in Ev \implies n + (2::'a) \in Ev$

Format of inductive definitions

consts $S :: \tau$ *set*

inductive S

intros

$\llbracket a_1 \in S; \dots ; a_n \in S; A_1; \dots ; A_k \rrbracket \implies a \in S$

\vdots

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

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 $m \in Ev$

Better: induction on the *structure* of the derivation

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

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

Rule induction for Ev

To prove

$$n \in Ev \implies P n$$

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

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

Rule $Ev.induct$:

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

An elimination rule

Rule induction in general

Set S is defined inductively.

To prove

$$x \in S \implies P x$$

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

we must prove for every rule

$$\llbracket a_1 \in S; \dots ; a_n \in S \rrbracket \implies a \in S$$

that P is preserved:

$$\llbracket P a_1; \dots ; P a_n \rrbracket \implies P a$$

In Isabelle/HOL:

apply(erule S.induct)

Demo: inductively defined sets