Demo: Proof Methods

Sets

Type 'a set gives sets over type 'a

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

Proofs about Sets

Natural deduction proof rules:

- equalityI: $[\![A \subseteq B;\ B \subseteq A]\!] \Longrightarrow A = B$
- equalityE: $isrule A = B;\ [\![A \subseteq B;\ B \subseteq A]\!] \Longrightarrow PP$
- subsetI: $(\bigwedge x.\ x \in A \Longrightarrow x \in B) \Longrightarrow A \subseteq B$
- sutsetD: $[\![A \subset B;\ c \in A]\!] \Longrightarrow c \in B$
- IntI: $[\![c \in A;\ c \in B]\!] \Longrightarrow c \in A \cap B$
- IntD1: $c \in A \cap B \Longrightarrow c \in A$
- IntD2: $c \in A \cap B \Longrightarrow c \in B$
- set_eqI: $(\bigwedge x.\ (x \in A) = (x \in B)) \Longrightarrow A = B$
- mem_Collect_eq: $(a \in \{x.\ P\ x\}) = P\ a$
- Collect_mem_eq: $\{x.\ x \in A\} = A$
- ... (see Tutorial)

Bounded Quantification

- $\forall x \in A.\ P\ x \ \equiv \forall x.\ x \in A \longrightarrow P\ x$
- $\exists x \in A.\ P\ x \ \equiv \exists x.\ x \in A \wedge P\ x$
- ballI: $(\bigwedge x.\ x \in A \Longrightarrow P\ x) \Longrightarrow \forall x \in A.\ P\ x$
- 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: $[\![\exists x \in A.\ P\ x;\ \bigwedge x.\ [\![x \in A;\ P\ x]\!] \Longrightarrow Q]\!] \Longrightarrow Q$

Demo: Some Set Theory

Format for Inductive Set Definitions

inductive_set S :: "τ set" where

$[\![a_{1,1} \in S; \ldots;\ a_{1,n} \in S; A_{1,1};\ \ldots;\ A_{1,k}]\!] \Longrightarrow a_1 \in S$ |

... |

$[\![a_{m,1} \in S; \ldots;\ a_{m,1} \in S; A_{m,1};\ \ldots;\ A_{m,j}]\!] \Longrightarrow a_m \in S$

where $A_{i,j}$ are side conditions not involving S.

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

In Isabelle/HOL:

```
inductive_set Finites ::  'a set set
```

– The set of all finite sets

```
{ } ∈ Finites |
A ∈ Finites ⟹ insert a A ∈ Finites
```


Example: Even Numbers

Informally

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

Example: Even Numbers

In Isabelle/HOL:

```
inductive_set Ev ::  nat set
```

— The set of all even numbers

$0 \in Ev$ |

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

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: induct on the length of the derivation of $m \in EV$

Better: induct on the *structure* of the derivation

Proving Properties of Even Numbers

Induction leads to two cases:

- **rule:** $0 \in Ev$

  1. $0 + 0 \in Ev$ case $m = 0$

- **rule:** $n \in Ev \Longrightarrow n + 2 \in Ev$

  z 2. $\Lambda n. [\![n \in Ev;\ n + n \in Ev]\!] \Longrightarrow Suc(Suc n) + Suc(Suc n) \in Ev$

  case $m = n + 2$

Rule Induction for Ev

To prove

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

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

- $\mathtt{P\ 0}$
- $P \ \ n \Longrightarrow P(n+2)$

Uses rule `Ev.induct`:

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

An elimination rule

Rule Induction in General

Set $\mathtt{S}$ is defined inductively. To prove

$$\mathtt{x} \in \mathtt{S} \Longrightarrow \mathtt{P\ x}$$

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

$$[\![\mathtt{a}_1 \in \mathtt{S};\ \ldots;\ \mathtt{a}_n \in \mathtt{S}]\!] \Longrightarrow \mathtt{a} \in \mathtt{S}$$

that $\mathtt{P}$ is preserved:

$$[\![\mathtt{P\ a}_1;\ \ldots;\ \mathtt{P\ a}_n]\!] \Longrightarrow \mathtt{P\ a}$$

In Isabelle/HOL: `apply(erule S.induct)`

Demo: Inductive Set Definition

Demo: Evens are infinite