Demo: Proof Methods

Sets

Type `'a set` gives sets over type `'a`

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

Proofs about Sets

Natural deduction proof rules:

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

Bounded Quantification

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

Demo: Some Set Theory

Format for Inductive Set Definitions

$\texttt{inductive\_set}\ S :: \text{“}\tau\ \texttt{set}\text{”}\ \texttt{where}$

$[\![\mathtt{a}_{1,1} \in \mathtt{S}; \ldots;\ \mathtt{a}_{1,n} \in \mathtt{S}; \mathtt{A}_{1,1};\ \ldots;\ \mathtt{A}_{1,k}]\!] \Longrightarrow \mathtt{a}_1 \in \mathtt{S}\ |$

$\ldots\ |$

$[\![\mathtt{a}_{m,1} \in \mathtt{S}; \ldots;\ \mathtt{a}_{m,l} \in \mathtt{S}; \mathtt{A}_{m,1};\ \ldots;\ \mathtt{A}_{m,j}]\!] \Longrightarrow \mathtt{a}_m \in \mathtt{S}$

where $\mathtt{A}_{i,j}$ are side conditions not involving $\mathtt{S}$.

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 $\mathtt{n}$ is even, then so is $\mathtt{n} + 2$
- These are the only even numbers

Example: Even Numbers

In Isabelle/HOL:

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

— The set of all even numbers

$\mathtt{0} \in \mathtt{Ev}$ |

$\mathtt{n} \in \mathtt{Ev} \Longrightarrow \mathtt{n} + 2 \in \mathtt{Ev}$

Proving Properties of Even Numbers

Easy: $4 \in \texttt{Ev}$

$$0 \in \texttt{Ev} \Longrightarrow 2 \in \texttt{Ev} \Longrightarrow 4 \in \texttt{Ev}$$

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

Idea: induct on the length of the derivation of $\texttt{m} \in \texttt{EV}$

Better: induct on the *structure* of the derivation

Proving Properties of Even Numbers

Induction leads to two cases:

- **rule:** $0 \in \mathtt{Ev}$

  $\mathtt{1.}\ \ 0 + 0 \in \mathtt{Ev}$ case $\mathtt{m} = 0$

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

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

  case $\mathtt{m} = \mathtt{n} + 2$

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`:

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

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