CS576 Topics in Automated Deduction

Elsa L Gunter
2112 SC, UIUC
egunter@illinois.edu
http://courses.grainger.illinois.edu/cs576

Slides based in part on slides by Tobias Nipkow

February 26, 2026

Sets

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

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

Proofs about Sets

Natural deduction proof rules:

- `equalityI`: $[\![\mathtt{A} \subseteq \mathtt{B};\ \mathtt{B} \subseteq \mathtt{A}]\!] \Longrightarrow \mathtt{A} = \mathtt{B}$
- `equalityE`: $[\![\mathtt{A} = \mathtt{B};\ [\![\mathtt{A} \subseteq \mathtt{B};\ \mathtt{B} \subseteq \mathtt{A}]\!] \Longrightarrow \mathtt{P}]\!] \Longrightarrow \mathtt{P}$
- `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

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

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

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

$$\ldots\ |$$

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

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

$0 \in \mathtt{Ev}$ |

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

Proving Properties of Even Numbers

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

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

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

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

Better: induct on the *structure* of the derivation

Proving Properties of Even Numbers

Induction leads to two cases:

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

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

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

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

  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`:

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

An elimination rule

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: Inductive Set Definition

Demo: Evens are infinite