Topics in Automated Deduction (CS 576)

Elsa L. Gunter
2112 Siebel Center
egunter@illinois.edu
http://www.cs.illinois.edu/class/sp10/cs576/

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: $(\lambda x.x \in A \Longrightarrow P\ x) \Longrightarrow \forall x \in A.\ P\ x$
- 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: $[\![\exists x \in A.\ P\ x;\ \Lambda x.[\![x \in A;\ P\ x]\!] \Longrightarrow Q]\!] \Longrightarrow Q$

Format for Inductive Set Definitions

inductive_set S :: "τ set" where

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

... |

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

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 ∈ Ev |
n ∈ Ev ⟹ n + 2 ∈ 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:** $n \in Ev \Longrightarrow n + 2 \in Ev$

  2. $\bigwedge n.\, [\![n \in Ev;\ n+n \in Ev]\!] \Longrightarrow Suc(Sucn)+Suc(Sucn) \in Ev$

     case $m = n + 2$

Rule Induction for Ev

To prove

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

by textitrule induction on $n \in Ev$ we must prove

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

Uses 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. 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

Format for Inductive Relations Definitions

inductive R :: "$\tau \longrightarrow$ bool" where

$[\![R(a_{1,1}); \ldots; R(a_{1,n}); A_{1,1}; \ldots; A_{1,k}]\!] \Longrightarrow R(a_1)$ |

... |

$[\![R(a_{m,1}); \ldots; R(a_{m,l}); A_{m,1}; \ldots; A_{m,j}]\!] \Longrightarrow R(a_m)$

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