

# Introduction to Isabelle/HOL



Jacques Fleuriot

## Notes on Isabelle/HOL Notation

• In Isabelle/HOL:

$$[ [ A_1 ; A_2 ; \dots ; A_n ] ] \Rightarrow G$$

can be read as "if  $A_1$  and  $A_2$  and ... and  $A_n$  then  $G$ "

**Note:** -  $P x$  ( $P x$ ) stands for  $P(x)$  ( $P(x)$ )

-  $P(x, y)$  can be expressed as  $P x y$  or  $(P x) y$

- recall that in higher order logic: functions, sets and predicates can be identified with each other.

•  $\forall x. P, \exists x. P$  are quantified sentences (where  $P$  may or may not contain  $x$ )

• If and only if is expressed using "=" e.g.  $(P \wedge Q) = \neg(\neg P \vee \neg Q)$

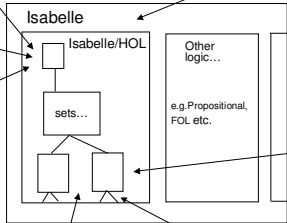
Has decision procedures e.g. linear arithmetic

## Isabelle

Meta-logic has Universal quantifier  $\wedge$  Implication  $\Rightarrow$  Conjunction ";"

Simplifier does rewriting

Has its own connectives and Quantifiers: e.g.  $\forall$  universal  $\exists$  existential  $\rightarrow$  implication  $\wedge$  conjunction ...



Has reasoning methods (based on natural deduction for example)

Hierarchy of theories e.g. sets, natural numbers, real numbers, security protocols ...

## Reasoning in Isabelle

• Forward and backward proofs

• Natural Deduction


- Introduction Rules
- Elimination Rules

• Isabelle tactics/methods

e.g. "rule", "drule", "auto", ...

• We will look at procedural proofs i.e. proofs will have sequences of

**apply** (*method theorem\_name*)


5 

## The Rules of the Game

- So far, we have seen (automatic) refutation proofs mainly
- Isabelle uses mostly **natural deduction**
- Natural deduction aims to capture human reasoning patterns when doing formal logic
- Each logical connective has two kinds of rules:
  - **Introduction Rules:** allow connective to be inferred
  - **Elimination Rules:** allow consequences from connective to be deduced
- In general, rules will involve other logical symbols e.g. user defined ones

---

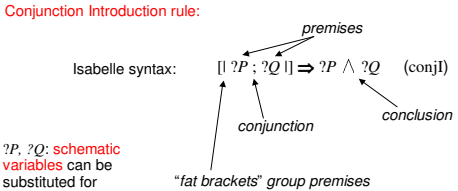
Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

7 

## Natural Deduction (Cont.)

**Conjunction Introduction rule:**

Isabelle syntax:  $[ [ ?P ; ?Q ] ] \Rightarrow ?P \wedge ?Q$  (conjI)




*?P, ?Q: schematic variables can be substituted for*

*"fat brackets" group premises*

In procedural style: mainly reason **backwards**

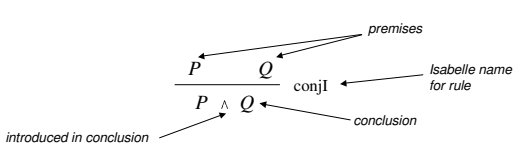
---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

6 

## Natural Deduction

**Example:** **Conjunction Introduction** enables us to introduce the  $\wedge$  connective




**Forward proof:** "If we have P and we have Q then we have  $P \wedge Q$ "

**Backward proof:** "To prove  $P \wedge Q$ , prove that P is true and prove that Q is true"

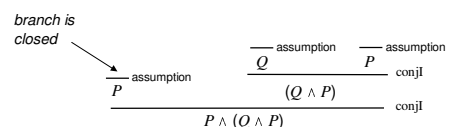
---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

8 

## A Simple Proof

Given that  $P$  is true and that  $Q$  is true prove  $P \wedge (Q \wedge P)$



*branch is closed*

Assumptions:  $P \quad Q$

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

9 School of Informatics

## A Simple Backward Proof in Isabelle

Given that  $P$  is true and that  $Q$  is true prove  $P \wedge (Q \wedge P)$

*Isabelle keyword*

**lemma** *a\_conj\_theorem*: "[[ P ; Q ]] => P & (Q & P)"

**apply** (rule conjI)

**apply** assumption

**apply** (rule conjI)

**apply** assumption

**apply** assumption

**qed**

*Isabelle commands*

*name given to resulting theorem*

The method/tactic called **rule** applies its argument (a theorem) **backwards**

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

11 School of Informatics

## Other Introduction Rules (II)

$$\frac{P}{P \vee Q} \text{ disjI1}$$

$$\frac{Q}{P \vee Q} \text{ disjI2}$$

$$\frac{\begin{matrix} [P] \\ \vdots \\ \text{false} \end{matrix}}{\neg P} \text{ notI}$$

Intuition:  $\neg P = (P \rightarrow \text{false})$

$$\frac{\begin{matrix} [P] & [Q] \\ \vdots & \vdots \\ Q & P \end{matrix}}{P = Q} \text{ iffI}$$

Isabelle: "[[ ?P => ?Q; ?Q => ?P ]] => P = Q"

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

10 School of Informatics

## Other Introduction Rules (I)

Common notation:

$$\frac{Q}{P \rightarrow Q} \text{ impl}$$

Isabelle:  $(?P \Rightarrow ?Q) \Rightarrow ?P \rightarrow ?Q \quad (\text{impl})$

or as  $\frac{P \Rightarrow Q}{P \rightarrow Q} \text{ impl}$

Note:  $[P]$ : assumption local to sub-proof

**Forward:** "If on the the assumption that P is true, Q can be shown to hold, then we can conclude  $P \rightarrow Q$ "

**Backward:** "To prove  $P \rightarrow Q$ , assume P is true and prove that Q follows"

More rules to come ...

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

12 School of Informatics

## Substitution

In Isabelle literature:  $P[t/x]$  is result of replacing  $x$  by  $t$  in  $P$

Note: this is same as  $P \cdot \{t/x\}$  that we saw before

$$\frac{s = t \quad P[s/x]}{P[t/x]} \text{ subst}$$

only positions designated by variable substituted by this rule

Substitution rule in Isabelle:  $[[ ?t = ?s ; ?P ?s ]] \Rightarrow ?P ?t \quad (\text{subst})$

**Example:** prove symmetry of equality predicate i.e.  $s = t \Rightarrow t = s$ :

$$\frac{s = t \quad \overline{s = s}}{t = s}$$

Justification:

$$\frac{s = t \quad (x = s)[s/x]}{t = s}$$

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

13

### Other Introduction Rules (III)

- Quantifiers  $\forall, \exists$ : need substitution and notion of arbitrary variable

**Universal Quantifier:**

$$\frac{P x_0}{\forall x. P x} \text{ all}$$

$x_0$  is arbitrary i.e. we make no assumptions about it  
*provided  $x_0$  does not occur in  $P x$  or any premise on  $P x_0$  which may depend*

In Isabelle: use underlying formalism of Isabelle, the meta-logic, to express the proviso logically

Isabelle's meta-logical universal quantifier enables notion of arbitrary value

don't confuse this with conjunction

$$(\lambda x. ?P x) \Rightarrow \forall x. ?P x$$


---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

15

### Elimination Rules

- Work in opposite direction from introduction rules
- Conjunction rules:  $\frac{P \wedge Q}{P} \text{ conjunct1}$        $\frac{P \wedge Q}{Q} \text{ conjunct2}$

In Isabelle:  $?P \wedge ?Q \Rightarrow ?P$        $?P \wedge ?Q \Rightarrow ?Q$

$[P], [Q]$  local to their subproofs

$$\frac{\begin{array}{c} [P] \\ \vdots \\ P \vee Q \\ R \end{array} \quad \begin{array}{c} [Q] \\ \vdots \\ R \end{array}}{R} \text{ disjE}$$

*have to prove "R" twice under different assumptions*

Disjunction rule:  $[\ ] ?P \vee ?Q ; ?P \Rightarrow ?R ; ?Q \Rightarrow ?R [\ ] \Rightarrow ?R \text{ (disjE)}$

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

14

### Other Introduction Rules (IV)

**Existential Quantifier:**

$$\frac{P a}{\exists x. P x}$$

"If we can exhibit some  $a$  such that  $P(a)$  is true then  $\exists x. P(x)$  is also true"

In Isabelle:  $?P ?a \Rightarrow \exists x. ?P x$

**Example:**  $\frac{\text{even } 2}{\exists x. \text{even } x}$

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

16

### Elimination Rules (II)

Using an elimination rule backwards produces a case-split

Example: Assume " $A \vee B$ " prove " $B \vee A$ "

*"erule" enables this subgoal to be proved immediately from premise of goal*

$$\frac{\frac{A \vee B}{A \vee B} \quad \frac{\frac{A}{B \vee A} \text{ disjI2} \quad \frac{B}{B \vee A} \text{ disjI2}}{B \vee A} \text{ disjE}}{B \vee A}$$

Note: can use "erule" method, designed to work with elimination rules

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

17 School of Informatics

## Elimination Rules (III)

Example: Assume " $A \vee B$ " prove " $B \vee A$ "

A possible Isabelle proof:

```

lemma disj_swap: "A ∨ B ⇒ B ∨ A"
apply (erule disjE)
apply (rule disjI2)
apply assumption
apply (rule disjI1)
apply assumption
qed

```

could have used "**apply** (rule disjE)".  
This need extra step though.

Try it in Isabelle!

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

19 School of Informatics

## Isabelle/HOL A Special Elimination Rule for Conjunction

- Isabelle provides an alternative conjunction elimination rule

$$\frac{P \wedge Q \quad \begin{array}{c} [P][Q] \\ \vdots \\ R \end{array}}{R} \text{conjE}$$

In Isabelle:  $[! ?P \wedge ?Q ; ! ?P ; ?Q ] \Rightarrow ?R ] \Rightarrow ?R$  (conjE)

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

18 School of Informatics

## Isabelle/HOL: A Special Elimination Rule

- Isabelle elimination rules for  $\wedge$  are:

$\text{conjunct1: } \frac{P \wedge Q}{P}$

$\text{conjunct2: } \frac{P \wedge Q}{Q}$

rules simply return 1<sup>st</sup>/2<sup>nd</sup> half of conjunct

- these are called **destruction** rules in Isabelle
- they break and destroy a premise (we lose info when we apply them)

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

20 School of Informatics

## Elimination Rules (IV)

**Implication:**  $\frac{P \rightarrow Q \quad P}{Q} \text{mp}$  In Isabelle:  $[! ?P \rightarrow ?Q ; ?P ] \Rightarrow ?Q$

**Example:** Prove  $P \rightarrow (Q \rightarrow R) \Rightarrow P \wedge Q \rightarrow R$

1.  $P \rightarrow (Q \rightarrow R)$
2.  $[P \wedge Q]$
3.  $[P]$  4.  $[Q]$

$$\frac{\frac{\frac{P \wedge Q \text{ assum}}{P} \text{assum} \quad \frac{Q \text{ assum}}{Q} \text{assum} \quad \frac{P \rightarrow (Q \rightarrow R) \text{assum}}{Q \rightarrow R} \text{mp}}{R} \text{mp}}{R} \text{conjE}}{P \wedge Q \rightarrow R} \text{impl}$$

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

21

## More Elimination Rules (V)

**Negation:**  
elimination rule deduces any formula in the presence of both  $P$  and  $\neg P$

$$\frac{\neg P \quad P}{R} \text{ notE}$$

Isabelle:  $[\neg ?P ; ?P] \Rightarrow ?R$  (*notE*)

- In Isabelle, there are many useful proved theorems about negation that can be used in proofs
- Proof by contradiction often uses theorems involving **contrapositives** such as  $P \rightarrow Q$  and  $\neg Q \rightarrow \neg P$

Example theorem:

$$\frac{[\neg P] \quad \dots \quad \neg Q \quad Q}{P}$$

Isabelle:  $[\neg ?Q ; \neg ?P \Rightarrow ?Q] \Rightarrow ?P$

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

23

## Elimination Rules for Quantifiers

**Existential Quantifier:** This proviso is part of the rule definition and cannot be omitted

$$\frac{[P x_0] \quad \dots \quad \exists x. P x \quad Q}{Q} \text{ exE}$$

Provided  $x_0$  does not occur in  $P x$  or  $Q$  or any other premises other than  $P x_0$  on which derivation of  $Q$  from  $P x_0$  depends

In Isabelle:  $[\exists x. ?P x ; \wedge x. ?P x \Rightarrow ?Q] \Rightarrow ?Q$  (*exE*)

This is (once again) universal quantification in the Isabelle meta-logic (cf. *allI*). It ensures that the proviso is enforced.

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

22

## Elimination Rules for Quantifiers

**Universal Elimination:**

$$\frac{\forall x. P x \quad P t}{P t} \text{ spec}$$

Isabelle:  $(\forall x. ?P x) \Rightarrow ?P ?x$  ← unknown variable can be freely instantiated to any term

- Note: In Isabelle terminology, this is a destruction rule
- Can provide an alternative non-destructive rule

Isabelle:

$$\frac{[P x] \quad \dots \quad \forall x. P x \quad R}{R} \text{ allE} \quad [ \forall x. ?P x ; ?P ?x \Rightarrow R ] \Rightarrow R \quad (\text{allE})$$


---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9

24

## Summary

- A first look at theorem proving in Isabelle/HOL
- Natural Deduction
  - introduction and elimination rules in Isabelle
  - some rules have provisos
- Proofs can be given as a tree for natural deduction
- Read Chapter 5 of tutorial on Isabelle/HOL
  - available via AR web page
- More to come ...

---

Automated Reasoning      Introduction to Isabelle/HOL      Lecture 8/9