Slide 1

NICTA Advanced Course

Theorem Proving
Principles, Techniques, Applications

Slide 2

Content

- ➜ Intro & motivation, getting started with Isabelle
- ➜ **Foundations & Principles**
  - Lambda Calculus
  - Higher Order Logic, natural deduction
  - **Term rewriting**
- ➜ Proof & Specification Techniques
  - Inductively defined sets, rule induction
  - Datatypes, recursion, induction
  - Calculational reasoning, mathematics style proofs
  - Hoare logic, proofs about programs

Slide 3

Last Time

- ➜ Introducing new Types
- ➜ Equations and Term Rewriting
- ➜ Confluence and Termination of reduction systems
- ➜ Term Rewriting in Isabelle
- ➜ First structured proofs (Isar)

Slide 4

Applying a Rewrite Rule

- ➜ $l \longrightarrow r$ **applicable** to term $t[s]$
  if there is substitution σ such that $\sigma\ l = s$
- ➜ **Result:** $t[\sigma\ r]$
- ➜ **Equationally:** $t[s] = t[\sigma\ r]$

Example:

Rule: $0 + n \longrightarrow n$

Term: $a + (0 + (b + c))$

Substitution: $\sigma = \{n \mapsto b + c\}$

Result: $a + (b + c)$

CONDITIONAL TERM REWRITING

Rewrite rules can be conditional:

$$[\![P_1 \ldots P_n]\!] \Longrightarrow l = r$$

is **applicable** to term $t[s]$ with σ if

Slide 5

- ➜ $\sigma\ l = s$ and
- ➜ $\sigma\ P_1, \ldots, \sigma\ P_n$ are provable by rewriting.

REWRITING WITH ASSUMPTIONS

Last time: Isabelle uses assumptions in rewriting.

Can lead to non-termination.

Example:

lemma "$f\ x = g\ x \wedge g\ x = f\ x \Longrightarrow f\ x = 2$"

Slide 6

simp	**use and simplify** assumptions
(simp (no_asm))	**ignore** assumptions
(simp (no_asm_use))	**simplify**, but do **not use** assumptions
(simp (no_asm_simp))	**use**, but do **not simplify** assumptions

PREPROCESSING

Preprocessing (recursive) for maximal simplification power:

$$\begin{array}{rcl} \neg A & \mapsto & A = False \\ A \longrightarrow B & \mapsto & A \Longrightarrow B \\ A \wedge B & \mapsto & A,\ B \\ \forall x.\ A\ x & \mapsto & A\ ?x \\ A & \mapsto & A = True \end{array}$$

Slide 7

Example: $(p \longrightarrow q \wedge \neg r) \wedge s$

$$\mapsto$$

$$p \Longrightarrow q = True \qquad r = False \qquad s = True$$

Slide 8

DEMO

Case splitting with simp

Slide 9

$$P \ (\text{if } A \text{ then } s \text{ else } t)$$
$$=$$
$$(A \longrightarrow P\ s) \wedge (\neg A \longrightarrow P\ t)$$

Automatic

$$P \ (\text{case } e \text{ of } 0 \ \Rightarrow \ a \mid \text{Suc } n \ \Rightarrow \ b)$$
$$=$$
$$(e = 0 \longrightarrow P\ a) \wedge (\forall n.\ e = \text{Suc } n \longrightarrow P\ b)$$

Manually: apply (simp split: nat.split)

Similar for any data type t: **t.split**

Congruence Rules

Slide 10

congruence rules are about using context

Example: in $P \longrightarrow Q$ we could use P to simplify terms in Q

For $\Longrightarrow$ hardwired (assumptions used in rewriting)

For other operators expressed with conditional rewriting.

Example: $[\![P = P'; P' \Longrightarrow Q = Q']\!] \Longrightarrow (P \longrightarrow Q) = (P' \longrightarrow Q')$

Read: to simplify $P \longrightarrow Q$

- ➜ first simplify P to P'
- ➜ then simplify Q to Q' using P' as assumption
- ➜ the result is $P' \longrightarrow Q'$

More Congruence

Slide 11

Sometimes useful, but not used automatically (slowdown):
conj_cong: $[\![P = P'; P' \Longrightarrow Q = Q']\!] \Longrightarrow (P \wedge Q) = (P' \wedge Q')$

Context for if-then-else:
if_cong: $[\![b = c; c \Longrightarrow x = u; \neg c \Longrightarrow y = v]\!] \Longrightarrow$
$(\text{if } b \text{ then } x \text{ else } y) = (\text{if } c \text{ then } u \text{ else } v)$

Prevent rewriting inside then-else (default):
if_weak_cong: $b = c \Longrightarrow (\text{if } b \text{ then } x \text{ else } y) = (\text{if } c \text{ then } x \text{ else } y)$

- ➜ declare own congruence rules with **[cong]** attribute
- ➜ delete with **[cong del]**

Ordered rewriting

Slide 12

Problem: $x + y \longrightarrow y + x$ does not terminate

Solution: use permutative rules only if term becomes lexicographically smaller.

Example: $b + a \leadsto a + b$ but not $a + b \leadsto b + a$.

For types nat, int etc:

- lemmas **add_ac** sort any sum ($+$)
- lemmas **times_ac** sort any product ($*$)

Example: **apply** (simp add: add_ac) yields
$(b + c) + a \leadsto \cdots \leadsto a + (b + c)$

Slide 13

AC Rules

Example for associative-commutative rules:

Associative: $(x \odot y) \odot z = x \odot (y \odot z)$

Commutative: $x \odot y = y \odot x$

These 2 rules alone get stuck too early (not confluent).

Example: $(z \odot x) \odot (y \odot v)$

We want: $(z \odot x) \odot (y \odot v) = v \odot (x \odot (y \odot z))$

We get: $(z \odot x) \odot (y \odot v) = v \odot (y \odot (x \odot z))$

We need: **AC rule** $x \odot (y \odot z) = y \odot (x \odot z)$

If these 3 rules are present for an AC operator
Isabelle will order terms correctly

Slide 14

Demo

Slide 15

Back to Confluence

Last time: confluence in general is undecidable.
But: confluence for terminating systems is decidable!
Problem: overlapping lhs of rules.

Definition:

Let $l_1 \longrightarrow r_1$ and $l_2 \longrightarrow r_2$ be two rules with disjoint variables.
They form a **critical pair** if a non-variable subterm of l_1 unifies with l_2.

Example:

Rules: (1) $f\ x \longrightarrow a$ (2) $g\ y \longrightarrow b$ (3) $f\ (g\ z) \longrightarrow b$

Critical pairs:

(1)+(3) $\{x \mapsto g\ z\}$ $a \xleftarrow{(1)} f\ g\ t \xrightarrow{(3)} b$

(3)+(2) $\{z \mapsto y\}$ $b \xleftarrow{(3)} f\ g\ t \xrightarrow{(2)} b$

Slide 16

Completion

(1) $f\ x \longrightarrow a$ (2) $g\ y \longrightarrow b$ (3) $f\ (g\ z) \longrightarrow b$

is not confluent

But it can be made confluent by adding rules!

How: join all critical pairs

Example:

(1)+(3) $\{x \mapsto g\ z\}$ $a \xleftarrow{(1)} f\ g\ t \xrightarrow{(3)} b$

shows that $a = b$ (because $a \overset{*}{\longleftrightarrow} b$), so we add $a \longrightarrow b$ as a rule

This is the main idea of the Knuth-Bendix completion algorithm.

Slide 17

DEMO: WALDMEISTER

Slide 18

ORTHOGONAL REWRITING SYSTEMS

Definitions:
A **rule** $l \longrightarrow r$ is **left-linear** if no variable occurs twice in l.
A **rewrite system** is **left-linear** if all rules are.

A system is **orthogonal** if it is left-linear and has no critical pairs.

Orthogonal rewrite systems are confluent

Application: functional programming languages

Slide 19

LAST TIME ON ISAR

- ➜ basic syntax
- ➜ proof and qed
- ➜ assume and show
- ➜ from and have
- ➜ the three modes of Isar

Slide 20

BACKWARD AND FORWARD

Backward reasoning: ... **have** "$A \wedge B$" **proof**

- ➜ **proof** picks an **intro** rule automatically
- ➜ conclusion of rule must unify with $A \wedge B$

Forward reasoning: ...
assume AB: "$A \wedge B$"
from AB **have** "..." **proof**

- ➜ now **proof** picks an **elim** rule automatically
- ➜ triggered by **from**
- ➜ first assumption of rule must unify with AB

General case: from $A_1 \ldots A_n$ **have** R **proof**

- ➜ first n assumptions of rule must unify with $A_1 \ldots A_n$
- ➜ conclusion of rule must unify with R

Slide 21

FIX AND OBTAIN

fix $v_1 \ldots v_n$

Introduces new arbitrary but fixed variables
($\sim$ parameters, $\bigwedge$)

obtain $v_1 \ldots v_n$ **where** <prop> <proof>

Introduces new variables together with property

Slide 22

DEMO

Slide 23

FANCY ABBREVIATIONS

this	=	the previous fact proved or assumed
then	=	**from** this
thus	=	**then show**
hence	=	**then have**
with $A_1 \ldots A_n$	=	**from** $A_1 \ldots A_n$ this
?thesis	=	the last enclosing goal statement

Slide 24

MOREOVER AND ULTIMATELY

have X_1: P_1 ...	**have** P_1 ...
have X_2: P_2 ...	**moreover have** P_2 ...
$\vdots$	$\vdots$
have X_n: P_n ...	**moreover have** P_n ...
from $X_1 \ldots X_n$ **show** ...	**ultimately show** ...

wastes lots of brain power
on names $X_1 \ldots X_n$

Slide 25

GENERAL CASE DISTINCTIONS

show $formula$
proof -
  have $P_1 \vee P_2 \vee P_3$ <proof>
  moreover { **assume** P_1 ... **have** ?thesis <proof> }
  moreover { **assume** P_2 ... **have** ?thesis <proof> }
  moreover { **assume** P_3 ... **have** ?thesis <proof> }
  ultimately show ?thesis **by** blast
qed

{ ... } is a proof block similar to **proof** ... **qed**

{ **assume** P_1 ... **have** P <proof> }
stands for $P_1 \Longrightarrow P$

Slide 26

MIXING PROOF STYLES

from ...
have ...
  apply -   make incoming facts assumptions
  apply (...)
  ⋮
  apply (...)
  done

Slide 27

DEMO

Slide 28

WE HAVE LEARNED TODAY ...

➜ Conditional term rewriting
➜ Congruence and AC rules
➜ More on confluence
➜ Completion
➜ Isar: fix, obtain, abbreviations, moreover, ultimately

EXERCISES

Slide 29

- ➜ Find critical pairs for your DNF solution from last time
- ➜ Complete rules to a terminating, confluent system
- ➜ Add AC rules for $\wedge$ and $\vee$
- ➜ Decide $((C \vee B) \wedge A) = (\neg(A \wedge B) \longrightarrow C \wedge A)$ with these simp-rules
- ➜ Give an Isar proof of the rich grandmother theorem
  (automated methods allowed, but proof must be explaining)