System Demonstration

The ΩMEGA Group
Presentation: Andreas Meier[1] & Volker Sorge[2]

[1] University of Saarbrücken, Germany
[2] University of Birmingham, UK

Overview

I. Introduction

II. Interactive theorem proving with ΩMEGA

III. Proof Planning in ΩMEGA

IV. Exploration

I. INTRODUCTION

- Aims and Philosophy
- Background
- System

Aims

Goal: Mathematical Assistant System for proof development

- human-oriented
- abstract (top-down)
- knowledge-based
- mixed-initiative

Current status: implementation as a joint research platform for a collection of related and integrated research projects

Philosopy

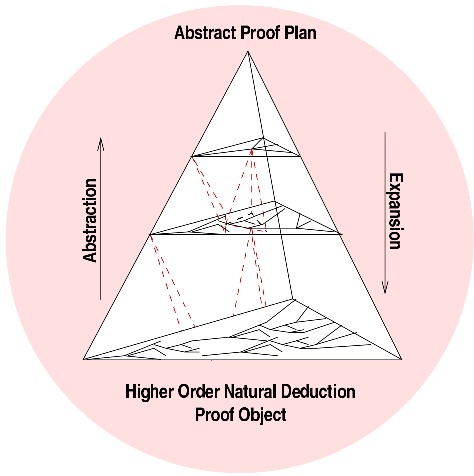
- 'Top-down' approach to theorem proving
  - Proof construction with abstract steps
  - Expansion onto a basic logic level
  - Proof checking in a small ND calculus

$\Rightarrow$ Proving and expansion are equivalent problems

- Do not re-invent the wheel!
  (i.e., use existing technology)

Proof Object

Proof Data Structure of ΩMEGA



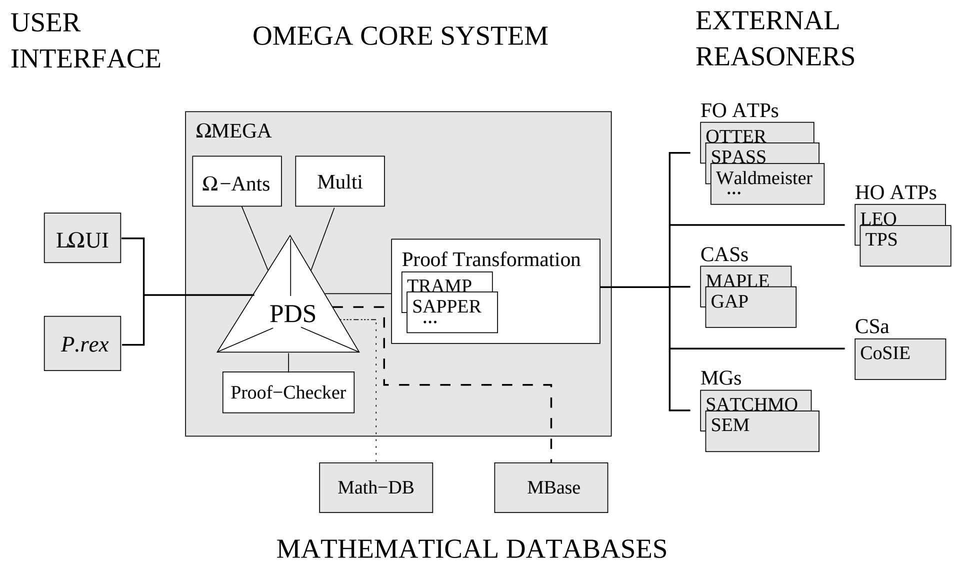
maintains simultaneously
a proof at
different levels of abstraction

Higher-order language
based on a
simply-typed λ-calculus

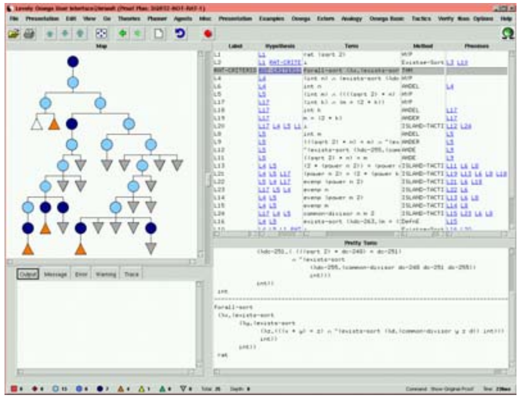
Proof Construction

- Interactive proof construction with
  - 'failing' tactics (correctness not guranteed, unlike LCF)
  - embedded external reasoners (ATP, CAS, . . .)
  - facts from knowledge base
- Usable for both proving and expanding
- Automation via proof planning and agent mechanism

Architecture



$\mathcal{L}\Omega\mathcal{U}\mathcal{I}$: Graphical User Interface



multi modal:
proof tree
linearized proof
term browser

II. Interactive Theorem Proving

- Applying rules and tactics
- Using suggestion mechanism Ω-ANTS
- Proof construction with islands
- Proof expansion and proof explanation

The $\sqrt{2}$-Problem

Theorem: $\sqrt{2}$ is irrational.

Proof: (by contradiction)

Assume $\sqrt{2}$ is rational, that is, there exist natural numbers m, n with no common divisor such that $\sqrt{2} = m/n$. Then $n\sqrt{2} = m$, and thus $2n^2 = m^2$. Hence m^2 is even and, since odd numbers square to odds, m is even; say $m = 2k$. Then $2n^2 = (2k)^2 = 4k^2$, that is, $n^2 = 2k^2$. Thus, n^2 is even too, and so is n. That means that both n and m are even, contradicting the fact that they do not have a common divisor.

Formalization

The Problem:

```
(th~defproblem sqrt2-not-rat
  (in real)
  (conclusion (not (rat (sqrt 2))))
  (help "sqrt 2 is not a rational number."))
```

Formalization

SQRT:

```
(th~defdef sqrt
  (in real)
  (definition
    (lam (x num)
       (that (lam (y num) (= (power y 2) x)))))
  (help "Definition of square root."))
```


Formalization

Rat-Criterion:

```
(th~deftheorem rat-criterion
  (in rational)
  (conclusion
    (forall-sort (lam (x num)
     (exists-sort (lam (y num)
      (exists-sort (lam (z num)
       (and (times x y) z)
            (not (exists-sort (lam (d num)
                    (common-divisor y z d))
                   int))))
       int)) int)) rat))
  (help "x rational implies there exist integers y,z

         which have no common divisor with x=y*z."))
```


Interactive Proof Construction

Successive proof construction by

- applying rules
- applying tactics
- using external systems
- using facts from the database

Problems:

- Which facts are needed from database?
- Which rules/tactics/external systems are applicable?
  How are they applicable?

Suggestion Mechanism Ω-ANTS

Goal:

- Compute possible next proof step
- Consider rules, tactics, external systems, theorems etc.
- Suggest commands + parameters to the user

Realization:

- Realized in concurrent processes
- Computations in the background
- Exhibits anytime behavior

Proof Construction with Islands

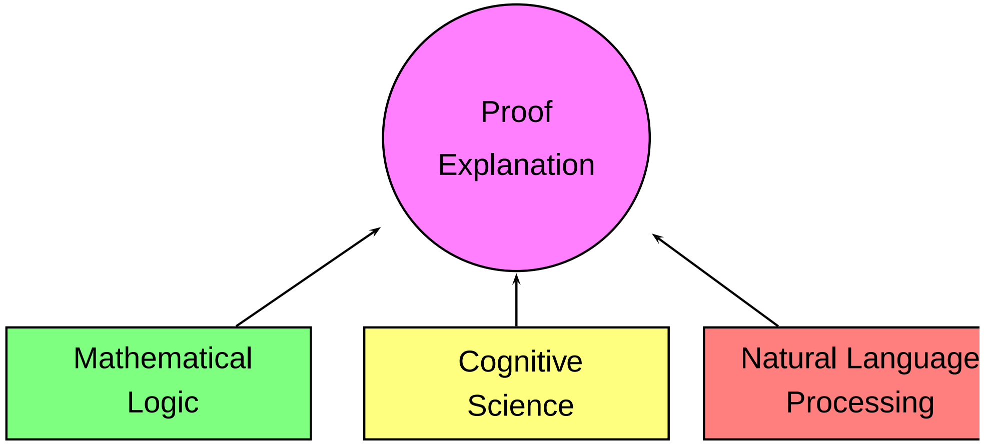
Problem: How do we get the desired proof, if the tactics do not corrspond to the necessary steps?

Insert steps as proof 'islands'

$$\cfrac{\cfrac{2*n^2=m^2}{Even(m^2)}\;Island}{Even(m)}\;Island$$
$$\vdots$$

Valid proof is generated by expansion.

P.rex: An Interactive Proof Explainer



Calculus of Constructions ACT-R Discourse Planning

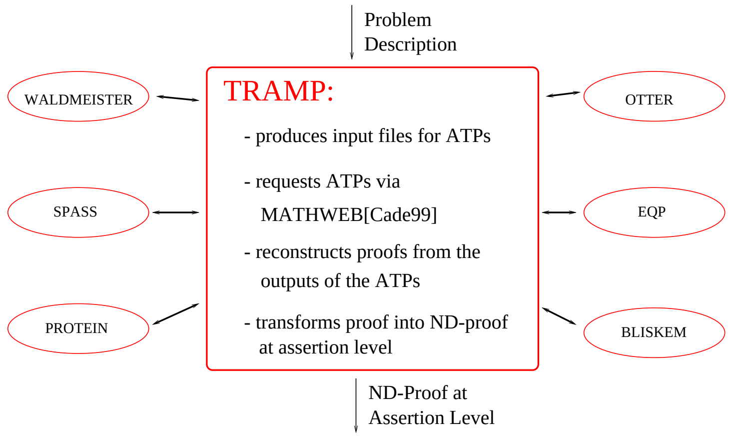
Expansion of Proofs

Recursive and interleaved process:

- Normal 'failing' tactics
  - expansion (hopefully) automatic
- Island Tactic
  - manually construct expansion
  - close gap with external reasoners
- External reasoners
  - compute automatically expansions with special systems/interfaces (e.g. TRAMP, SAPPER, ...)

The TRAMP System

Transformation of ATP output into ND-proofs at assertion level

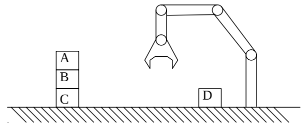


III. Proof Planning

- Automated theorem proving at abstract level
- AI planning paradigm
- Knowledge Acquisition

AI Planning

- Initial State



  $on(A,B)$, $on(B,C)$, $on\_table(C)$, $on\_table(D)$, $free(A)$, ...
- Goal: $on\_table(B)$
- Operators

  PUTDOWN(X)
  prec: $holding(X)$
  effect:
  $\oplus$ $on\_table(X)$, $hand\_empty$
  $\ominus$ $holding(X)$
- Plan $pick(A), putdown(A), pick(B), putdown(B)$

Theorem Proving as Planning

Initial State: proof assumptions
Goal: theorem
Operators: called methods

- Methods representing (abstract) proving steps
- Method = tactic + specification

Proof Plan: sequence of actions, i.e., instantiated methods
Planning Process: precondition achievement planning

Proof Planning in ΩMEGA

Knowledge-based proof planning

- domain-specific methods
- use of domain-specific external systems
- control-rules prune search space in particular domains

with multiple strategies

- strategies define different plan refinements (e.g. supply planner with different sets of methods and control rules)
- flexible combination and interleaving of strategies

Proof Planning the $\sqrt{2}$-Problem

Knowledge acquisition, e.g.

PrimeFacs-Product-m-f		
prec.	L: $n * t = t'$	
appl.-cond.	$n = p_1 * \ldots * p_n$ (CAS)	
effect:	$\oplus$ L_1: prime-divisor(p_1,t')	(Expand-PrimeFacs(L))
	$\vdots$	
	$\oplus$ L_n: prime-divisor(p_n,t')	(Expand-PrimeFacs(L))

Methods include specification of expansion scheme

Case Studies

- Limit Theorems

  (employs COSIE, MAPLE)
- Residue Class Domain

  (employs MAPLE, GAP, WALDMEISTER, SEM, HR)
- Homomorphism Theorems

Only with older version of ΩMEGA:

- Diagonalization proofs
- Completeness of resolution calculi

IV. Exploration

- Motivation
- Exploration with Oants
- Exploration with Multi

Motivation

Do not only re-prove known theorems, but

- Experiment with new conjectures
- Explore properties of structures

$\Rightarrow$ Postulate, prove, and refute conjectures

Set Problems

Examine different arbitrary set equations:

$$A \cup (B \cap C) = (A \cup B) \cap C$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Show validity or invalidity

Exploring with Ω-ANTS

- Consider some tactics and external reasoners
- Automated application of suggestions
- Involve complementary reasoning specialists
  - prove with automated theorem prover
  - refute with model generator
- Set examples: Proofs are simplified with some tactics and concluded by external reasoners

The Residue Class Domain

What kind of algebraic structures are ...

$$(\mathbb{Z}_4, \bar{+}), \qquad (\mathbb{Z}_5, (x \bar{*} y) \bar{+} \bar{1}_5), \quad (\{\bar{0}_6, \bar{2}_6, \bar{4}_6\}, (x \bar{+} x) \bar{+} (y \bar{+} y))$$

...?

Successively check properties such as associativity, unit element, etc.

Which structures are isomorphic ?

$$(\mathbb{Z}_3, \bar{+}) \cong (\{\bar{0}_6, \bar{2}_6, \bar{4}_6\}, \bar{+}) \quad (\mathbb{Z}_2 \otimes \mathbb{Z}_2, \bar{+} \otimes \bar{+}) \ncong (\mathbb{Z}_4, \bar{+})$$

Exploration with Proof Planning

Examine properties step-by-step

- Exploration module employs Multi
  - Several strategies in Multi
  - Supported by CAS, Model Generator
- Proof plan a conjecture or its negation
- Guidance by example computation

Credits

`http://www.ags.uni-sb.de/~omega`

Jörg Siekmann, Christoph Benzmüller, Vladimir Brezhnev, Lassaad Cheikhrouhou, Armin Fiedler, Andreas Franke, Helmut Horacek, Michael Kohlhase, Andreas Meier, Erica Melis, Markus Moschner, Immanuel Normann, Martin Pollet, Volker Sorge, Carsten Ullrich, Claus-Peter Wirth, Jürgen Zimmer