



# Proof Development With $\Omega$ MEGA: $\sqrt{2}$ Is Irrational

J. Siekmann, C. Benz Müller, A. Fiedler, A. Meier, and M. Pollet

University of Saarbrücken, Germany

LPAR 2002, Tbilisi, Georgia, 14 Oct 2002

# Research in the $\Omega$ MEGA project

---

Aim: assistant for the working mathematician

Means: **development and integration of heterogenous tools**

- **reasoning** proof planning (PP), agent-based reasoning, ATP
- **computation** computer algebra
- **interaction** tactical TP, mixed initiative PP
- **proof maintenance** proof object, diff. levels of detail
- **user interface** graphical UI, natural language
- **knowledge management** mathematical database
- **infrastructure** network of service systems

$\Omega$ MEGA project :=

collection of integrated **heterogeneous research projects** linked

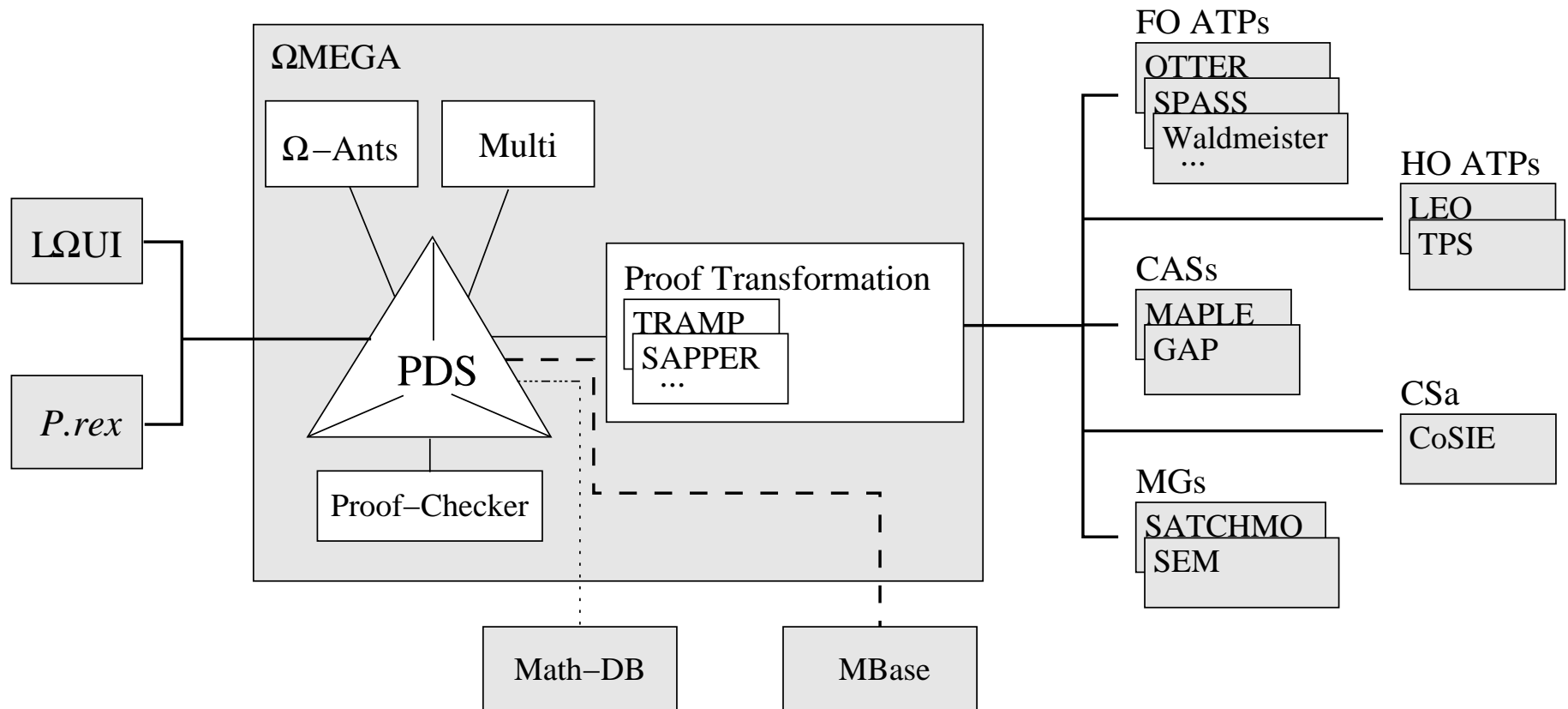
via the core  $\Omega$ MEGA-system

# System Overview

USER  
INTERFACE

OMEGA CORE SYSTEM

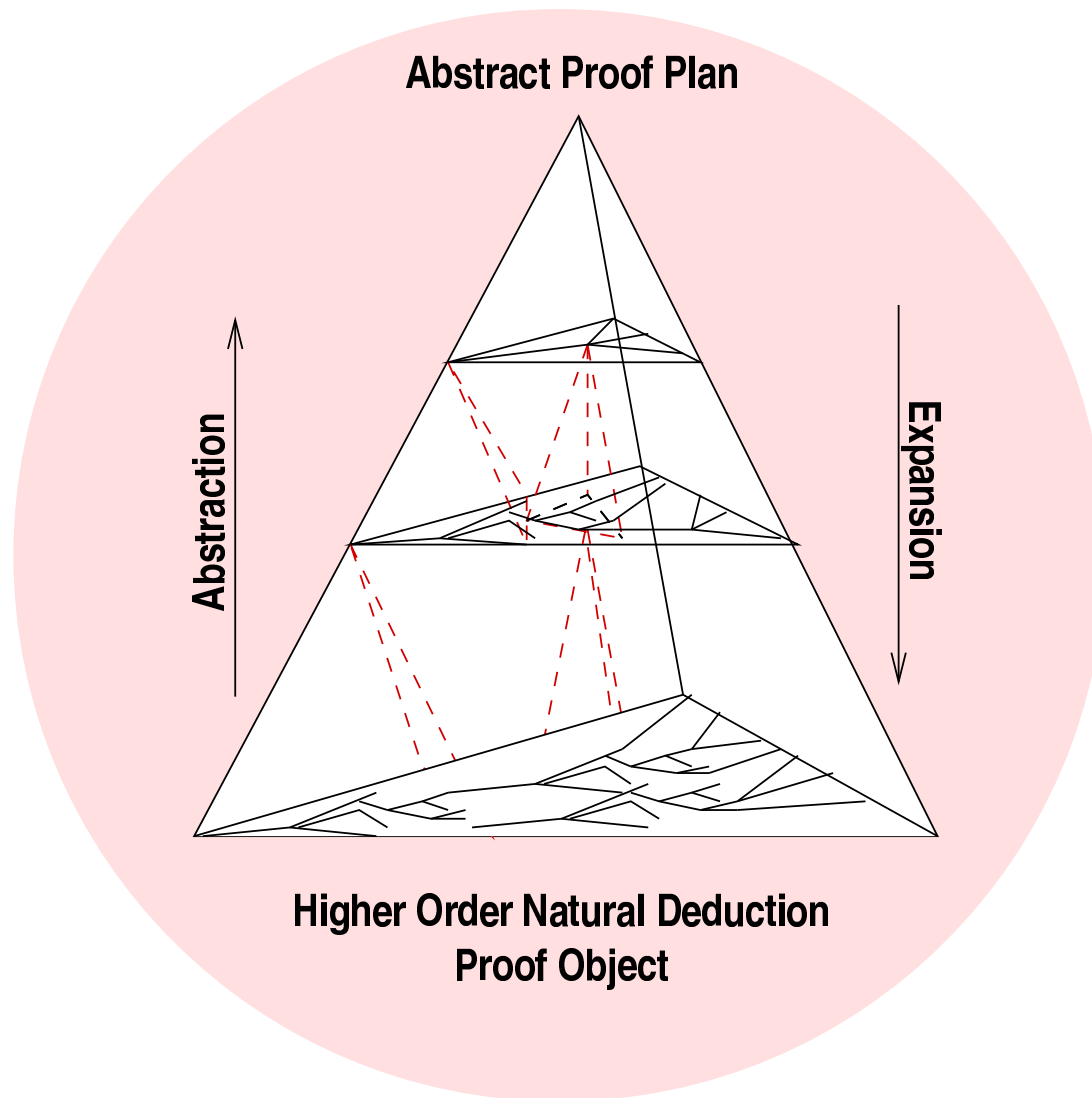
EXTERNAL  
REASONERS



MATHEMATICAL DATABASES

# $\Omega$ MEGA's Proof Data Structure

---



# Case Study: $\sqrt{2}$ is irrational

---

- Suggested by Henk Barendregt and Freek Wiedijk
- Comparison of mathematical assistant systems?
- Good test for  $\Omega$ MEGA!
- Three contributions:
  1. Tactical theorem proving
  2. New: Interactive island planning
  3. Automated proof planning
- Focus in this talk: Tactical theorem proving and interactive island planning

# The $\sqrt{2}$ -Problem

---

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

# 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.

# The $\sqrt{2}$ -Problem

---

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

How closely can we prove the theorem interactively along the previous lines?



# Formalization

---

## The Problem:

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

## Definitions and Lemmas:

```
(th~deftheorem rat-criterion (in real)
  (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 "for rationals x there exist integers y,z which
    have no common divisor and z=x*y."))
```

# Formalization

---

```
(th~defdef evenp (in integer)
  (definition
    (lam (x num) (exists-sort (lam (y num) (= x (times 2 y))) int)))
  (help "Definition of even.))

(th~deftheorem square-even (in integer)
  (conclusion
    (forall-sort (lam (x num) (equiv (evenp (power x 2)) (evenp x))) int))
  (help "x is even, iff x^2 is even.))

(th~deftheorem even-common-divisor (in integer)
  (conclusion
    (forall-sort (lam (x num) (forall-sort (lam (y num)
      (implies (and (evenp x) (evenp y)) (common-divisor x y 2)))
      int)) int))
  (help "If x and y are even, then they have a common divisor.))
```

# Formalization

---

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

```
(th~defdef rat (in rational)
  (definition
    (lam (x num)
      (exists-sort (lam (y num) (exists-sort (lam (z num)
        (and (not (= (mod x y) zero)) (= x (frac y z))))
        pos-nat)) int)))
(help "Rationals as reduced fractions a/b of integers."))
```

# Tactical TP in $\Omega$ MEGA

---

Procedural approach: proof construction by

- applying rules
- applying tactics  
(note difference to LCF style tactics!)
- using external systems
- using facts from the database

# Tactical TP in $\Omega$ MEGA

---

Procedural approach: proof construction by

- applying rules
- applying tactics  
(note difference to LCF style tactics!)
- using external systems
- using facts from the database

Verification by proof expansion

# Tactical TP in $\Omega$ MEGA

---

Procedural approach: proof construction by

- applying rules
- applying tactics  
(note difference to LCF style tactics!)
- using external systems
- using facts from the database

Verification by proof expansion

Tools for proof presentation

# Tactical TP in $\Omega$ MEGA

---

OMEGA: load-problems real

;;; Rules loaded for theory REAL.

;;; Theorems loaded for theory REAL.

;;; Tactics loaded for theory REAL.

;;; Methods loaded for theory REAL.

;;; Strategies loaded for theory REAL.

...

OMEGA: prove sqrt2-not-rat

Changing to proof plan Sqrt2-NOT-RAT-1

Sqrt2-NOT-RAT () |- (NOT (RAT (SQRT 2)))

OPEN

OMEGA: noti

NEGATION (NDLINE) A negated line: [Sqrt2-NOT-RAT]

FALSITY (NDLINE) A falsity line: [()]

L1 (L1) |- (RAT (SQRT 2))

HYP

L2 (L1) |- FALSE

OPEN

Sqrt2-NOT-RAT () |- (NOT (RAT (SQRT 2)))

NOTI: (L2)

# Tactical TP in $\Omega$ MEGA

---

OMEGA: import-ass rat-criterion

```
RAT-CRITERION (RAT-CRITERION) |- (FORALL-SORT ([X].                                THM
    (EXISTS-SORT ([Y].
        (EXISTS-SORT ([Z].
            (AND (= (TIMES X Y) Z)
                (NOT (EXISTS-SORT ([D].
                    (COMMON-DIVISOR Y Z D))
                    INT))))
            INT))
        INT))
    RAT)
```



# Tactical TP in $\Omega$ MEGA

---

OMEGA: forall-sort

UNIV-LINE (NDLINE) Universal line: [RAT-CRITERION]

LINE (NDLINE) A line: [()]

TERM (TERM) Term to substitute: (sqrt 2)

SO-LINE (NDLINE) A line with sort: [L1]

```
L3 (L1) |- (EXISTS-SORT ([DC-248].                                FORALLE-SORT: ((SQRT 2))
              (EXISTS-SORT ([DC-251].                                (RAT-CRITERION L1)
                (AND (= (TIMES (SQRT 2) DC-248) DC-251)
                  (NOT (EXISTS-SORT ([DC-255].
                                (COMMON-DIVISOR DC-248 DC-251 DC-255))
                                INT))))
              INT))
INT)
```

# Tactical TP in $\Omega$ MEGA

---

OMEGA: mexistse-sort\*

CONCLINE (NDLINE) Conclusion Line.: [L2]

EXLINE (NDLINE) An existentially quantified line: [L3]

SUBGOAL (NDLINE) Subgoal Line.: [()]

PARAMETER (TERMSYM-LIST) Termsym List.: [(dc-2481 dc-2511)](n m)

```
L4 (L4)      |- (AND (INT N)                                     HYP
                (EXISTS-SORT ([DC-251].
                (AND (= (TIMES (SQRT 2) N) DC-251)
                (NOT (EXISTS-SORT ([DC-255].
                (COMMON-DIVISOR N DC-251 DC-255))
                INT))))
                INT))
L6 (L4)      |- (INT N)                                           ANDEL: (L4)
L5 (L5)      |- (AND (INT M)                                       HYP
                (AND (= (TIMES (SQRT 2) N) M)
                (NOT (EXISTS-SORT ([DC-255].
                (COMMON-DIVISOR N M DC-255))
                INT))))
L8 (L5)      |- ...
```

# Tactical TP in $\Omega$ MEGA

---

OMEGA: ande

CONJUNCTION (NDLINE) Conjunction to split: [L9]

LCONJ (NDLINE) Left conjunct: [()]

RCONJ (NDLINE) Right conjunct: [()]

L11 (L5) |- (= (TIMES (SQRT 2) N) M)

ANDE: (L9)

L12 (L5) |- (NOT (EXISTS-SORT ([DC-255].

ANDE: (L9)

(COMMON-DIVISOR N M DC-255)) INT))

Now we are stuck: from L11 we want to infer

(= (times 2 (power n 2)) (power m 2))

then (evenp (power m 2)) and (evenp m)

No tactic available for this; instead cut rule is needed



# Tactical TP in $\Omega$ MEGA

---

...

```
(L89 (TERTIUM-NON-DATUR POWER-INT-CLOSED NAT-INT SUCC-NAT ZERO-NAT
      EVEN-COMMON-DIVISOR SQUARE-EVEN L4)
      (EQUIV (EVENP (POWER N 2)) (EVENP N))
      (0 ("IMPE" ()) (L6 L88) "grounded" ()) ("EXISTENT" "EXISTENT" "EXISTENT"))
      )
```

```
(L90 (TERTIUM-NON-DATUR POWER-INT-CLOSED NAT-INT SUCC-NAT ZERO-NAT
      EVEN-COMMON-DIVISOR SQUARE-EVEN L4)
      (IMPLIES (EVENP (POWER N 2)) (EVENP N))
      (2 ("EQUIVE" ()) (L89) "expanded" ()) ("EXISTENT" "L91" "EXISTENT"))
      ("ANDE" ()) (L125) "expanded" ()) ("EXISTENT" "L91" "EXISTENT"))
      ("ANDEL" ()) (L125) "grounded" ()) ("EXISTENT" "EXISTENT"))
      )
```

...

# Tactical TP in $\Omega$ MEGA

Lovely Omega User Interface@church (Proof Plan: SQRT2-NOT-RAT-1)

File Presentation Edit View Go Theories Planner Agents Misc Presentation Examples Omega Extern Analogy Omega Basic Tactics Verify Mbase ult Options Help

Map

Label	Hypothesis	Term	Method	Premises
L11	L8	((sqrt 2) * n) = m	ANDE*	L8
L12	L8	~(exists-sort ( $\lambda$ dc-270, (comm	ANDE*	L8
L13	L8 L4 RAT-CRI	(power m 2) = (2 * (power n	BY-COMPUTATIO	L11
L14	L8 L4 RAT-CRI	evenp (power m 2)	DefnI	L15
L15	L8 L4 RAT-CRI	exists-sort ( $\lambda$ dc-278, ((power	EXISTSI-SORT	L13 L16
L16	L8 L4 RAT-CRI	int (power n 2)	WELLSORTED	L6
SQUARE-EVEN	SQUARE-EVEN	forall-sort ( $\lambda$ x, ((evenp (pow	THM	
L17	SQUARE-EVEN L	evenp m	ASSERT	SQUARE-EVEN L10 L1.
L18	SQUARE-EVEN L	exists-sort ( $\lambda$ dc-334, (m = (2	DefnE	L17
L19	L19	(int k) $\wedge$ (m = (2 * k))	HYP	
L20	SQUARE-EVEN L	1	WEAKEN	L29
L21	L19	int k	ANDE	L19
L22	L19	m = (2 * k)	ANDE	L19
L23	L19 SQUARE-EVI	(power n 2) = (2 * (power k	BY-COMPUTATIO	L13 L22
L24	L19 SQUARE-EVI	evenp (power n 2)	DefnI	L25
L25	L19 SQUARE-EVI	exists-sort ( $\lambda$ dc-344, ((power	EXISTSI-SORT	L23 L26
L26	L19 SQUARE-EVI	int (power k 2)	WELLSORTED	L21
L27	L19 SQUARE-EVI	evenp n	ASSERT	SQUARE-EVEN L6 L24
EVEN-COMMON-D	EVEN-COMMON-D	forall-sort ( $\lambda$ x, (forall-sort	THM	
L28	EVEN-COMMON-D	int 2	WELLSORTED	
L29	EVEN-COMMON-D	1	ASSERT	EVEN-COMMON-DIVISIO

Pretty Term

```
( $\lambda$ x. (forall-sort ( $\lambda$ y. (((evenp x)  $\wedge$  (evenp y))  $\supset$  (common-divisor x y 2))) int))
int
-----
evenp n
-----
int (power k 2)
-----
exists-sort ( $\lambda$ dc-344, ((power n 2) = (2 * dc-344))) int
-----
(power m 2) = (2 * (power n 2))
-----
m = (2 * k)
-----
(power n 2) = (2 * (power k 2))
```

Output Message Error Warning Trace

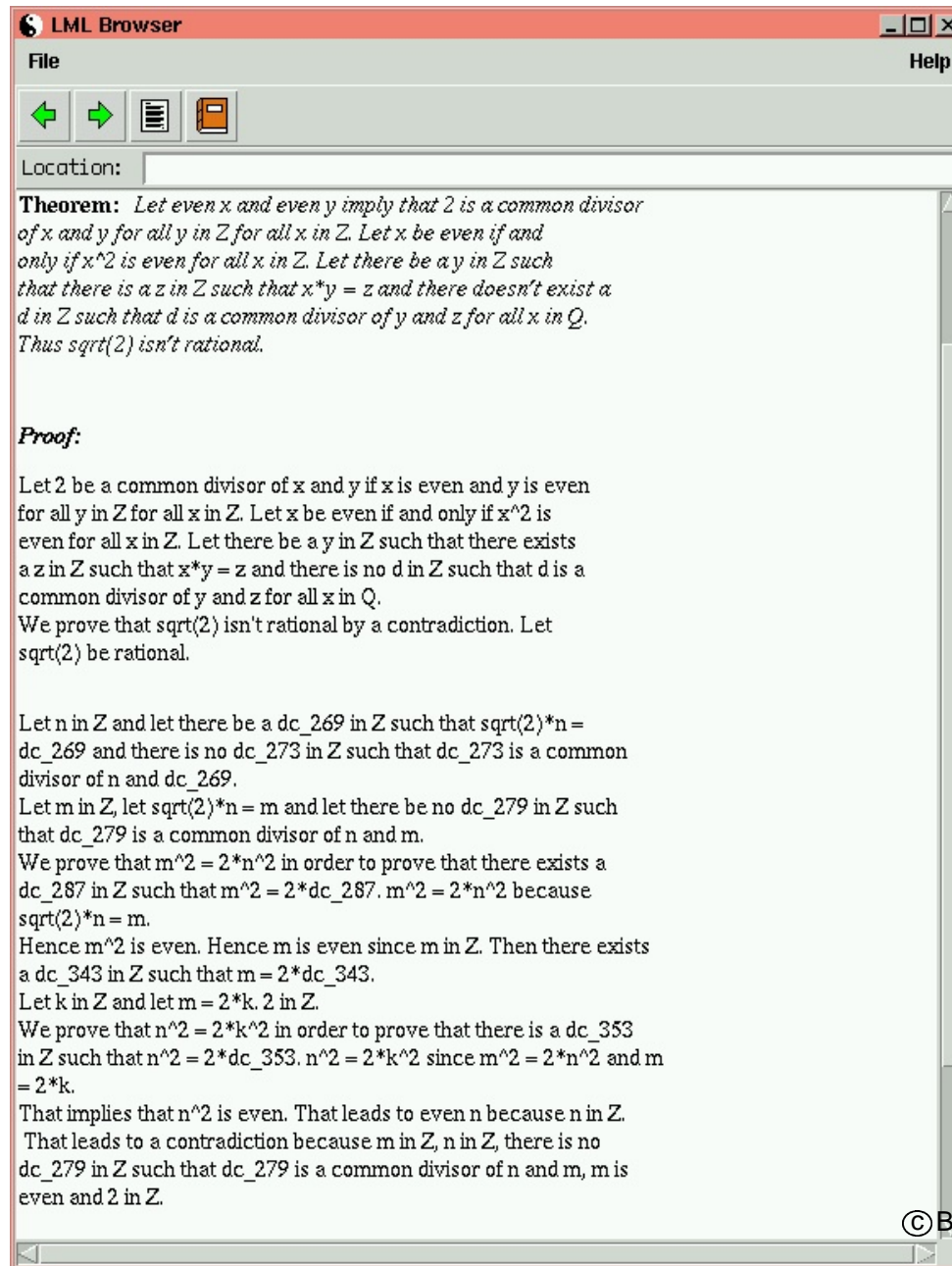
```
:::CSM Creator [2]: Command agent for command NEUT
:::CSM Creator [2]: Defining 3 default agents for
:::CSM Creator [2]: Blackboard for command INVERSE
:::CSM Creator [2]: Command agent for command INVE
:::CSM Creator [2]: Defining 2 default agents for
:::CSM Creator [2]: Blackboard for command APPLY-A
:::CSM Creator [2]: Command agent for command APPL
:::CSM Creator [2]: Defining 2 default agents for
:::CSM Creator [2]: Blackboard for command DEFNEXP
:::CSM Creator [2]: Command agent for command DEFN
:::CSM Creator [2]: Defining 1 default agents for
:::CSM Creator [2]: Blackboard for command REFLEX-
:::CSM Creator [2]: Command agent for command REFL

"Agents now NOT resource adaptive !" Initialized h
```

0 0 21 0 5 4 3 0 0 Total: 33 Depth: 0

© Benz Müller, Fiedler & Meier, 2002, Tbilissi  
Command: Execute-Theorem-Log Time: 1.56s

# Tactical TP in $\Omega$ MEGA



**LML Browser**

File Help

Location:

**Theorem:** *Let even  $x$  and even  $y$  imply that 2 is a common divisor of  $x$  and  $y$  for all  $y$  in  $\mathbb{Z}$  for all  $x$  in  $\mathbb{Z}$ . Let  $x$  be even if and only if  $x^2$  is even for all  $x$  in  $\mathbb{Z}$ . Let there be a  $y$  in  $\mathbb{Z}$  such that there is a  $z$  in  $\mathbb{Z}$  such that  $x*y = z$  and there doesn't exist a  $d$  in  $\mathbb{Z}$  such that  $d$  is a common divisor of  $y$  and  $z$  for all  $x$  in  $\mathbb{Q}$ . Thus  $\sqrt{2}$  isn't rational.*

**Proof:**

Let 2 be a common divisor of  $x$  and  $y$  if  $x$  is even and  $y$  is even for all  $y$  in  $\mathbb{Z}$  for all  $x$  in  $\mathbb{Z}$ . Let  $x$  be even if and only if  $x^2$  is even for all  $x$  in  $\mathbb{Z}$ . Let there be a  $y$  in  $\mathbb{Z}$  such that there exists a  $z$  in  $\mathbb{Z}$  such that  $x*y = z$  and there is no  $d$  in  $\mathbb{Z}$  such that  $d$  is a common divisor of  $y$  and  $z$  for all  $x$  in  $\mathbb{Q}$ . We prove that  $\sqrt{2}$  isn't rational by a contradiction. Let  $\sqrt{2}$  be rational.

Let  $n$  in  $\mathbb{Z}$  and let there be a  $dc\_269$  in  $\mathbb{Z}$  such that  $\sqrt{2}*n = dc\_269$  and there is no  $dc\_273$  in  $\mathbb{Z}$  such that  $dc\_273$  is a common divisor of  $n$  and  $dc\_269$ .

Let  $m$  in  $\mathbb{Z}$ , let  $\sqrt{2}*n = m$  and let there be no  $dc\_279$  in  $\mathbb{Z}$  such that  $dc\_279$  is a common divisor of  $n$  and  $m$ .

We prove that  $m^2 = 2*n^2$  in order to prove that there exists a  $dc\_287$  in  $\mathbb{Z}$  such that  $m^2 = 2*dc\_287$ .  $m^2 = 2*n^2$  because  $\sqrt{2}*n = m$ .

Hence  $m^2$  is even. Hence  $m$  is even since  $m$  in  $\mathbb{Z}$ . Then there exists a  $dc\_343$  in  $\mathbb{Z}$  such that  $m = 2*dc\_343$ .

Let  $k$  in  $\mathbb{Z}$  and let  $m = 2*k$ .  $2$  in  $\mathbb{Z}$ .

We prove that  $n^2 = 2*k^2$  in order to prove that there is a  $dc\_353$  in  $\mathbb{Z}$  such that  $n^2 = 2*dc\_353$ .  $n^2 = 2*k^2$  since  $m^2 = 2*n^2$  and  $m = 2*k$ .

That implies that  $n^2$  is even. That leads to even  $n$  because  $n$  in  $\mathbb{Z}$ . That leads to a contradiction because  $m$  in  $\mathbb{Z}$ ,  $n$  in  $\mathbb{Z}$ , there is no  $dc\_279$  in  $\mathbb{Z}$  such that  $dc\_279$  is a common divisor of  $n$  and  $m$ ,  $m$  is even and  $2$  in  $\mathbb{Z}$ .

# Tactical TP in $\Omega$ MEGA

---

Result:

- 33 interactive steps
- resulting proof consists of 33 nodes
- expanded proof consists of about 200 nodes (automatic expansion)

Problematic (this also applies to other systems):

- tactics are not fitted to the problem at hand
- proving is tedious and user has to adapt to the system



# Interactive islands planning

---

Declarative approach versus procedural approach

# Interactive islands planning

---

Declarative approach versus procedural approach

Network of proof 'islands'

$$\begin{array}{l} \frac{2 * n^2 = m^2}{\text{Even}(m^2)} \text{ Island} \\ \frac{\text{Even}(m^2)}{\text{Even}(m)} \text{ Island} \\ \vdots \end{array}$$

# Interactive islands planning

---

Declarative approach versus procedural approach

Network of proof 'islands'

$$\begin{array}{l} \frac{2 * n^2 = m^2}{\text{Even}(m^2)} \text{ Island} \\ \frac{\text{Even}(m^2)}{\text{Even}(m)} \text{ Island} \\ \vdots \end{array}$$

- Islands structure the proof in natural form
  - Islands provide no argument for soundness
- ⇒ Verification: expansion of island steps  
(automated, interactive, recursive island approach)

---

L6 (L4) ! (INT N) ANDEL: (L4)  
L8 (L5) ! (INT M) ANDEL: (L5)  
L11 (L5) ! (= (TIMES (SQRT 2) N) M) ANDE: (L9)  
OMEGA: island-tactic  
CONC (NDLINE) Conclusion of step: nil  
PREMS (NDLINE-LIST) Premises of step: (L11 L6 L8)  
PARAM (TERM) Formula of Conclusion: (= (times 2 (power n 2)) (power m 2))  
  
L13 (L4 L5) |- (= (TIMES 2 (POWER N 2)) (POWER M 2)) ISLAND-TACTIC: (L11 L6 L8)  
OMEGA: island-tactic nil (L13 L6 L8) (evenp (power m 2))  
  
L14 (L4 L5) |- (EVENP (POWER M 2)) ISLAND-TACTIC: (L13 L6 L8)  
OMEGA: island-tactic nil (L14 L8) (evenp m)  
  
L15 (L4 L5) |- (EVENP M) ISLAND-TACTIC: (L14 L8)

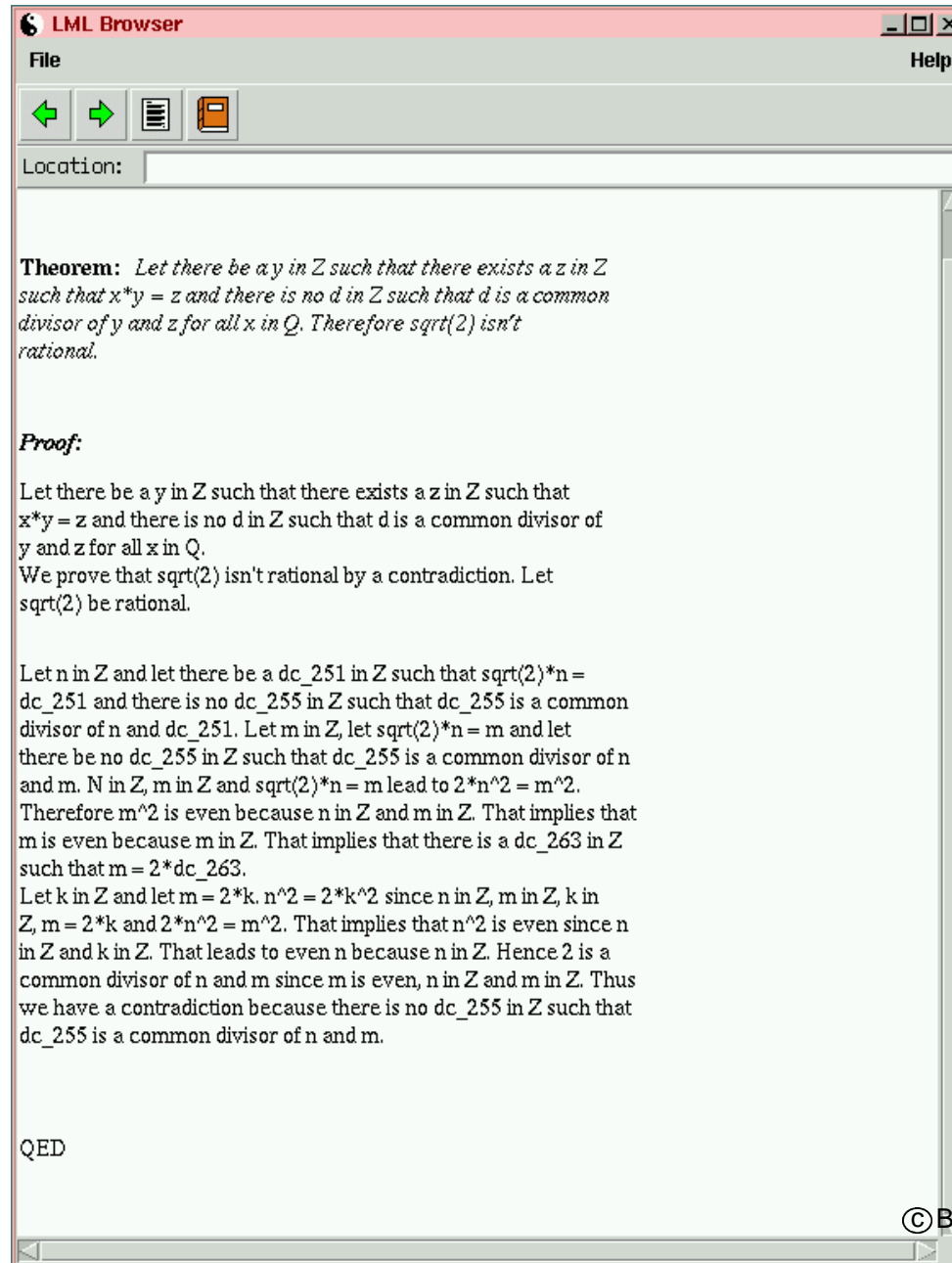
# Proof with Islands

---

Results:

- 15 interactive steps (8 island steps, 7 tactic steps)
- resulting proof consists of 25 nodes
- expanded proof consists of about 280 nodes (interactive expansion)

# Proof with Islands



**Theorem:** *Let there be  $a, y$  in  $\mathbb{Z}$  such that there exists a  $z$  in  $\mathbb{Z}$  such that  $x \cdot y = z$  and there is no  $d$  in  $\mathbb{Z}$  such that  $d$  is a common divisor of  $y$  and  $z$  for all  $x$  in  $\mathbb{Q}$ . Therefore  $\sqrt{2}$  isn't rational.*

**Proof:**

Let there be a  $y$  in  $\mathbb{Z}$  such that there exists a  $z$  in  $\mathbb{Z}$  such that  $x \cdot y = z$  and there is no  $d$  in  $\mathbb{Z}$  such that  $d$  is a common divisor of  $y$  and  $z$  for all  $x$  in  $\mathbb{Q}$ . We prove that  $\sqrt{2}$  isn't rational by a contradiction. Let  $\sqrt{2}$  be rational.

Let  $n$  in  $\mathbb{Z}$  and let there be a  $dc\_251$  in  $\mathbb{Z}$  such that  $\sqrt{2} \cdot n = dc\_251$  and there is no  $dc\_255$  in  $\mathbb{Z}$  such that  $dc\_255$  is a common divisor of  $n$  and  $dc\_251$ . Let  $m$  in  $\mathbb{Z}$ , let  $\sqrt{2} \cdot n = m$  and let there be no  $dc\_255$  in  $\mathbb{Z}$  such that  $dc\_255$  is a common divisor of  $n$  and  $m$ .  $n$  in  $\mathbb{Z}$ ,  $m$  in  $\mathbb{Z}$  and  $\sqrt{2} \cdot n = m$  lead to  $2 \cdot n^2 = m^2$ . Therefore  $m^2$  is even because  $n$  in  $\mathbb{Z}$  and  $m$  in  $\mathbb{Z}$ . That implies that  $m$  is even because  $m$  in  $\mathbb{Z}$ . That implies that there is a  $dc\_263$  in  $\mathbb{Z}$  such that  $m = 2 \cdot dc\_263$ .

Let  $k$  in  $\mathbb{Z}$  and let  $m = 2 \cdot k$ .  $n^2 = 2 \cdot k^2$  since  $n$  in  $\mathbb{Z}$ ,  $m$  in  $\mathbb{Z}$ ,  $k$  in  $\mathbb{Z}$ ,  $m = 2 \cdot k$  and  $2 \cdot n^2 = m^2$ . That implies that  $n^2$  is even since  $n$  in  $\mathbb{Z}$  and  $k$  in  $\mathbb{Z}$ . That leads to even  $n$  because  $n$  in  $\mathbb{Z}$ . Hence  $2$  is a common divisor of  $n$  and  $m$  since  $m$  is even,  $n$  in  $\mathbb{Z}$  and  $m$  in  $\mathbb{Z}$ . Thus we have a contradiction because there is no  $dc\_255$  in  $\mathbb{Z}$  such that  $dc\_255$  is a common divisor of  $n$  and  $m$ .

QED

# Summary of Island Approach

---

- Sketch top-level proof in a declarative way
- In general: expansion of island steps generates proof object in its own right
- In our case study: Expansion of island steps with external systems almost completely automatic.
- Problems in the automatization:
  - Which definitions need to be folded or unfolded?
  - Which assumptions are missing?
  - Which facts need to be included from the database?

# Proof Planning the Problem

---

Since  $\Omega$ MEGA is also a proof planner: **Can the proof can be automatically proof planned?**

- First needed: Acquisition of methods by generalization of steps in island proof
- Possible then: automatically prove plan arbitrary problems of the  $\sqrt[k]{l}$  is irrational domain
- But note: knowledge acquisition process is crucial for the success
- Methods still to problem specific: e.g. with respect to lemma retrieval or folding/unfolding of definitions
- See article submitted to Journal of Automated Reasoning



# Proof Planning the Problem

---

- (1) Use RAT-CRITERION and construct an indirect proof.
- (2) To get a contradiction show that the two constants (existential variables) in RAT-CRITERION, which are supposed to have no common divisor, actually do have a common divisor  $d$ .
- (3) To find a common divisor transform equations (for example,  $\sqrt{2} \cdot n = m \longrightarrow 2 \cdot n^2 = m^2$ ), derive new divisor statements (for example, from  $2 \cdot n^2 = m^2$  derive that  $m^2$  has divisor 2, or from  $m^2$  has divisor 2 derive that  $m$  has divisor 2); derive from given divisor statements new representations of terms, and use them for further transformations.

# Conclusion

---

Although the  $\sqrt{2}$ -example is mathematically trivial, it nevertheless provides a challenge for mathematical assistant systems: **not about automation, but about “natural” interaction and proof construction.**

The example particularly requires the combination of

- deduction
- computation
- lemma retrieval
- folding or unfolding definitions

There should be more such case studies!

Criteria for the comparison of systems?

# Conclusion cont'd

---

$\Omega$ MEGA is much more than just a proof planner:

- tactical theorem prover
- new: interactive island planning
- it provides various integrated support tools

Automated proof planning of  $\sqrt[k]{l}$ -examples is of course possible: by generalizing and programming reasoning patterns

But note the price to be paid: knowledge acquisition!

There is still much to do! And the main problem is not that we need stronger proof tools!