

COMPUTER-BASED MATHEMATICS

Mathematische Assistenzsysteme

Jörg Siekmann

<http://www.dfki.de/~siekmann>
Universität des Saarlandes
und
Deutsches Forschungszentrum
für Künstliche Intelligenz GmbH
DFKI

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

Was ist ein mathematisches Assistenzsystem?

<http://www.activemath.org>

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

Was ist ein mathematisches Assistenzsystem?

- Textverarbeitung** a la LATEX: TeXmacs
- Information Retrieval** aus einer mathematischen Datenbank (MBase, Open Math, OmDoc, ...)
- Theorie Kontext**
- Semantik:** der Definitionen, Theoreme, Beweise und Lemmata . . . und partiell der Textfragmente!
- Hilfsmittel und Tools: **Computer-Algebra Systeme**
- Hilfsmittel und Tools: **Deduktions Systeme**
- Hilfsmittel und Tools: **Proofchecker**

<http://www.activemath.org>

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

..... to set the stage.

1954: Martin Davis
Theorem: The Sum of two even numbers is again even
Proof: (Presburger Arithmetic)

1956: Alan Newell, Herb Simon
Theorems: from Principia Mathematica
Proof: Logic Theorist

Dartmouth Conference

Psychology Logic GPS

Logic Theorist Matrix Resolution

Woody Bledsoe Wang Neat

Scruffy Logic

Newell

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

3 Paradigms:

1. Classical Automated Theorem Proving
 - Resolution
 - Tableaux-Methods
 - Matrix and Connection Method
2. Tactical Theorem Proving
 - Automath
 - NUPRL
 - IMPS
 - ISABELLE etc.
3. Human oriented Theorem Proving
 - Natural Deduction
 - Woody Bledsoe
 - Proof Planing: OYSTER-CLAM, QMEGA

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

Deduction Systems

I. : Axioms , Theorem
II. : Proof , Failure

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

... Set The Fair, But Tis Not
REVIous RENEGADE;

Woody Bledsoe

Automated theorem proving is not the beautiful process we know as mathematics.
This is „cover your eyes with blinder and hunt through a cornfield for a diamond-shaped grain of corn“ ...
Mathematicians have given us a great deal of direction over the last two or three millennia.
Let us pay attention to it.

Woody Bledsoe, 1986

Ringvorlesung: Modellbasierte Software Entwicklung DFK Berlin den 29. April 2004



Can we do better?

?

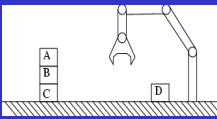
Ringvorlesung: Modellbasierte Software Entwicklung DFK Berlin den 29. April 2004

Knowledge based Proof Planning

AI-PLANNING IN THE BLOCKS WORLD

- Initial State**
on(A,B), on(B,C), on_table(C),
on_table(D), free(A), ...
- Goal**
on_table(B)
- Operators**
PUTDOWN(X);
precondition: holding (X)
effect: (+) on_table(X), hand_empty
(-) holding(X)
- Plan**
pick(A), putdown(A), pick(B), putdown(B)

Ringvorlesung: Modellbasierte Software Entwicklung DFK Berlin den 29. April 2004



Methods in Proof Planning

Specification	Declarations	Declarative Part
	Premises	
	Constraints	
	Conclusions	
Tactic	Declarative Content	Procedural Part
	Procedural Content	

Alan Bundy (1989): "A Science Of Reasoning"

Ringvorlesung: Modellbasierte Software Entwicklung DFK Berlin den 29. April 2004

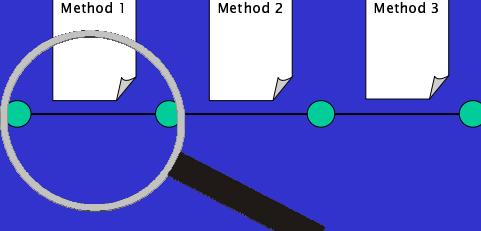
Methods: An Example

method: Indirect	
premises	$\oplus L2$
conclusions	$\ominus L4$
appl.cond	
proof schema	$L1. \neg Th \vdash \neg Th$ (HYP) $L2. \Delta \neg Th \vdash \perp$ (OPEN) $L3. \Delta \vdash \neg \neg Th$ ($\neg I; 2$) $L4. \Delta \vdash Th$ ($\neg E; 3$)

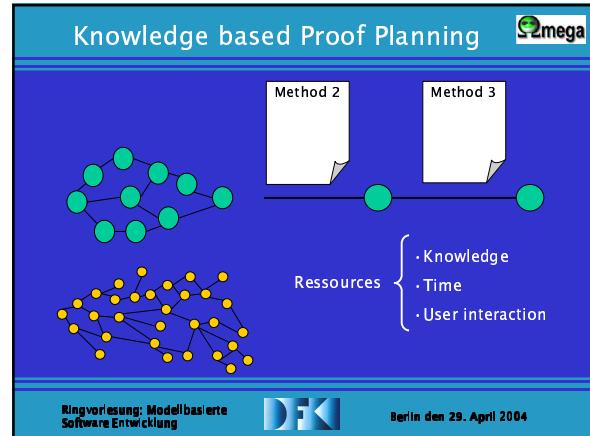
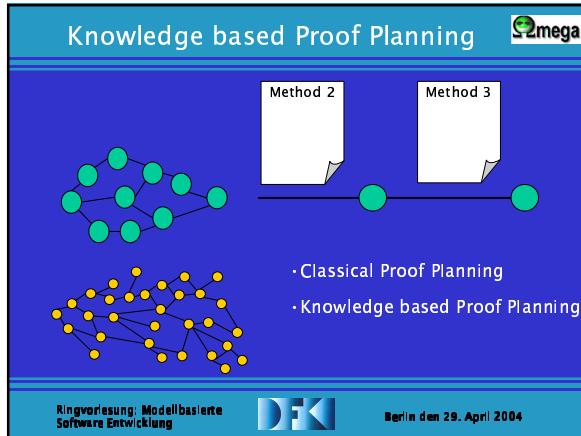
Ringvorlesung: Modellbasierte Software Entwicklung DFK Berlin den 29. April 2004

Knowledge based Proof Planning

megame



Ringvorlesung: Modellbasierte Software Entwicklung DFK Berlin den 29. April 2004



Mathematical Control Knowledge

Global mathematical control:

- Prove $|a| < b$ directly or via auxiliary variables
⇒ prove $|a| < b$ by **solve_b**, **solve*** or ... **LimHeuristic**.
- Use important parts of assumptions to introduce auxiliary variables/inequalities:
e.g. LimHeuristic requires:
 - Focus
 - UNWRAPHYP
 - REmoveFocus
 - MP-b

Source: Erica Melis

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Control knowledge represented as rules:

```
(control-rule attack-inequality
(IF (goal-matches (?goal (?x < ?y))))
(THEN
  (prefer(Solve< ?goal)
    (Solve* ?goal)
    (ComplexEstimate ?goal)
    (Simplify ?goal))))
```

```
(control-rule case-analysis-intro
(IF (last-method (Rewrite (?C -> ?R))) AND
(failure-condition (trivial ?C)))
(THEN (select (CaseSplit (?C or not ?C))))))
```

Source: Erica Melis

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Peter Deussen: Semigroups and Automata, Springer Verlag, 1971

*Theorem 4.8: Let σ and τ be two equivalence relations.
Then $(\sigma \cup \tau)^t$ is also an equivalence relation.*

Proof: (Idea)

To be shown:

- Symmetry
- Reflexivity
- Transitivity

of $(\sigma \cup \tau)^t$

No	S:D	Formula	Reason
1.	1;	$\vdash \text{EqRel}(\sigma)$	(Hyp)
2.	2;	$\vdash \text{EqRel}(\rho)$	(Hyp)
3.	1;	$\vdash \text{ref}(\sigma) \wedge \text{symm}(\sigma) \wedge \text{trans}(\sigma)$	(Def-EqRel 1)
4.	2;	$\vdash \text{ref}(\rho) \wedge \text{symm}(\rho) \wedge \text{trans}(\rho)$	(Def-EqRel 2)
5.	5;	$\vdash \forall x. \forall \mu. \forall x. (\tau \cup \mu)(x) \Leftrightarrow (\tau(x) \vee \mu(x))$	(Def-Union)
97.	1.25;	$\vdash \text{ref}((\sigma \cup \rho)^t)$	(PLAN)
98.	1.25;	$\vdash \text{symm}((\sigma \cup \rho)^t)$	(PLAN)
99.	1.25;	$\vdash \text{trans}((\sigma \cup \rho)^t)$	(PLAN)
Thrm.	1.25;	$\vdash \text{EqRel}((\sigma \cup \rho)^t)$	(Def-EqRel 97 98 99)

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

More Examples: epsilon-delta Proofs

- **Summensatz** (LIM+)
 $\lim_{x \rightarrow a} f(x) = L_1 \wedge \lim_{x \rightarrow a} g(x) = L_2 \rightarrow \lim_{x \rightarrow a} f(x) + g(x) = L_1 + L_2$
- **Produktsatz** (LIM*)
 $\lim_{x \rightarrow a} f(x) = L_1 \wedge \lim_{x \rightarrow a} g(x) = L_2 \rightarrow \lim_{x \rightarrow a} f(x) * g(x) = L_1 * L_2$
- LIM-, ContIfDeriv, Continuous+, Continuous-, Continuous*, ContCompos, $\lim_{x \rightarrow a} x^2 = a^2$ etc.

$\lim_{x \rightarrow a} f(x) = L :$

$\forall \epsilon < 0 \exists \delta > 0 \forall x (|x - a| < \delta \wedge x \neq a \rightarrow |f(x) - L| < \epsilon))$

Woody Bledsoe: "Challenges"

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Method for Limit Theorems

method: ComplexEstimate																						
premises	L1, $\oplus L2, \oplus L3, \oplus L4$																					
conclusions	$\ominus L7$																					
appl.cond	$\exists k, l, \sigma (\text{CASextract}(a, b) = (k, l, \sigma))$																					
proof schema	<table border="0" style="width: 100%; border-collapse: collapse;"> <tr><td>L1. Δ</td><td>$\vdash a < \epsilon_1$</td><td>$\vdash a < \epsilon_1$</td></tr> <tr><td>L2. Δ</td><td>$\vdash k \leq M$</td><td>(OPEN)</td></tr> <tr><td>L3.</td><td>$\vdash \alpha_\sigma < \epsilon/2 * M$</td><td>(OPEN)</td></tr> <tr><td>L4. Δ</td><td>$\vdash l < \epsilon/2$</td><td>(OPEN)</td></tr> <tr><td>L5.</td><td>$\vdash b = b$</td><td>(Ax)</td></tr> <tr><td>L6.</td><td>$\vdash b = k * \alpha_\sigma + l$</td><td>(CAS1.5)</td></tr> <tr><td>L7. Δ</td><td>$\vdash b < \epsilon$</td><td>(! x L2, L3, L4, L6)</td></tr> </table>	L1. Δ	$\vdash a < \epsilon_1$	$\vdash a < \epsilon_1$	L2. Δ	$\vdash k \leq M$	(OPEN)	L3.	$\vdash \alpha_\sigma < \epsilon/2 * M$	(OPEN)	L4. Δ	$\vdash l < \epsilon/2$	(OPEN)	L5.	$\vdash b = b$	(Ax)	L6.	$\vdash b = k * \alpha_\sigma + l$	(CAS1.5)	L7. Δ	$\vdash b < \epsilon$	(! x L2, L3, L4, L6)
L1. Δ	$\vdash a < \epsilon_1$	$\vdash a < \epsilon_1$																				
L2. Δ	$\vdash k \leq M$	(OPEN)																				
L3.	$\vdash \alpha_\sigma < \epsilon/2 * M$	(OPEN)																				
L4. Δ	$\vdash l < \epsilon/2$	(OPEN)																				
L5.	$\vdash b = b$	(Ax)																				
L6.	$\vdash b = k * \alpha_\sigma + l$	(CAS1.5)																				
L7. Δ	$\vdash b < \epsilon$	(! x L2, L3, L4, L6)																				

$\text{CASextract}(\underbrace{f(X_1) - l_1}_{a}, \underbrace{f(x) + g(x) - (l_1 + l_2)}_{b}) = (1, (g(x) - l_2), [x/X_1])$

Source: Erica Melis

Construction of mathematical Objects

CONSTRAINT SOLVING:
Collecting constraints and check for consistency

Final constraint store for LIM+

0 < E ₂ ≤ ε/2;
0 < D ≤ δ ₂ , δ ₁ ;
0 < E ₁ ≤ ε/(2 * M), ε/2;
1 ≤ M < ε/(2 * E ₁);
-∞ < X ₁ = x = X ₂ < +∞

Source: Erica Melis

Proof Presentation to the User

Verbalisation of ComplexEstimate:

In order to estimate the magnitude of $|b|$ we rewrite the term to $|k * a + l|$ and use the Triangle Inequality $|k * a + l| \leq |k * a| + |l|$. Now the goal can be shown in three steps:

- There exists an M such that $|k| < M$ and
- $|a| < \epsilon/(2 * M)$, and
- $|l| < \epsilon/2$.

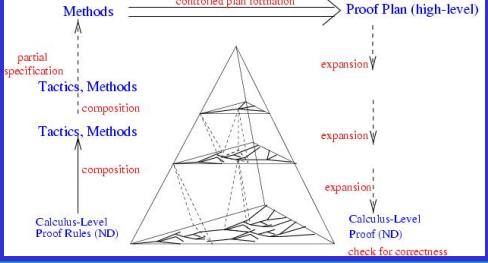
Then $|b| \leq |k| * |a| + |l| < M * \epsilon/(2 * M) + \epsilon/2 = \epsilon$ and therefore $|b| < \epsilon$.

Source: Erica Melis

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

PDS: Representation of (partial) Proofs



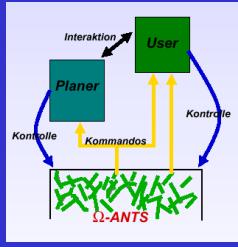
Methods → controlled plan formation → Proof Plan (high-level)
 partial specification
 Tactics, Methods
 composition
 Tactics, Methods
 composition
 Calculus-Level Proof Rules (ND)
 expansion
 expansion
 expansion
 expansion
 Calculus-Level Proof (ND)
 check for correctness

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

ΩMEGA – ANTS: Combining ATP with Proof Planning

- concurrency and resource adaptive behaviour
- anytime algorithms
- flexible integration of:
 - natural deduction
 - tactics and methods
 - external systems

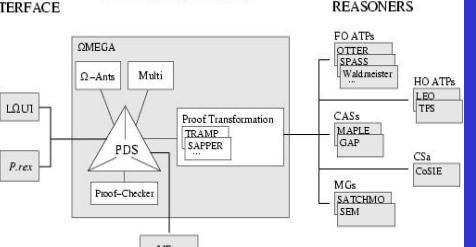


chris benzmueller, volker sorge

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004

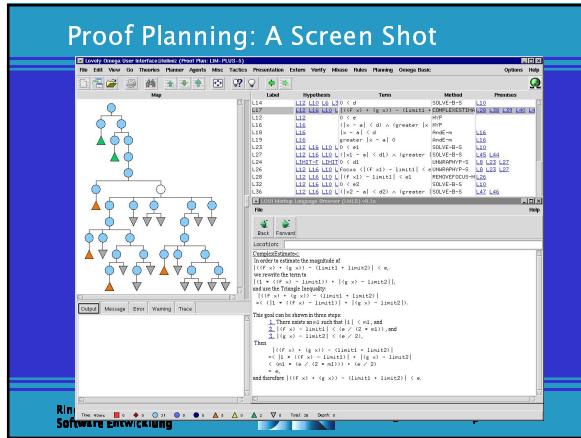
The OMEGA SYSTEM



USER INTERFACE: LQT, P.rex
 OMEGA CORE SYSTEM: ΩMEGA (Ω-Ants, Multi), Proof Transformation (TRAMP, SAPPER, ...), Proof-Checker, MBASE
 EXTERNAL REASONERS: EO ATPs (OTTER, SPASS, Waldmeister, ...), HO ATPs (LEO, TPS), CAs (MAPLE, GAP), MGs (SATCHMO, SEM), CSs (CoSIE)
 MATHEMATICAL DATABASE: MBASE

Ringvorlesung: Modellbasierte Software Entwicklung

Berlin den 29. April 2004



Zwei Entwicklungsrichtungen:

1. Verifikationswerkzeuge: z.B. VSE am DFKI
2. Mathematische Tutorsysteme: z.B. ActiveMath am DFKI

anwendungsorientierte
Grundlagenforschung!

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Zwei Entwicklungsrichtungen:

CHALLENGE:
Ein integriertes mathematisches Assistenzsystem

Grundlagenforschung!

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Knowledge Representation for Mathematics

- XML-Representation
- Semantics (OpenMath) extended by meta data (publ, mathematical, and pedagogical)
- Formal content for
 - Calling external systems
 - Intelligent search functionalities

Mathematical Ontology

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Knowledge: the building blocks in OMDoc

```
<definition id="c6elp4.Th2_def_monoid" for="c6elp4_monoid">
<metadata>
  <depends-on>
    <ref theory="cpl_Th3" name="structure" />
  </depends-on>
</metadata>
<title xml:lang="en">Definition of a monoid</Title>
<CMB xml:lang="en" format="omtext">
A monoid is a <ref xref="cpl_Th3_structure"> structure </ref>
<OMOBJ>
<OMD cd="elementary" name="ordered-triple">
<OMV name="M"/> <OMS cd="cp4_Th2" name="times"/> <OMS cd="cp4_Th2" name="unit"/>
</OMOBJ>
in which
<OMOBJ>
<OMD cd="elementary" name="ordered-pair">
<OMV name="M"/> <OMS cd="cp4_Th2" name="times"/>
</OMOBJ>
is a semi-group
with <ref xref="c6elp3.Th2_def_unit">unit</ref>
<OMOBJ> xmlns="http://www.openmath.org/OpenMath"
<OMS cd="cp4_Th2" name="unit"/>
</OMOBJ>.
<OMOBJ>
<PMD><OMOBJ> ... </OMOBJ></PMD>
</definitions>
```

**An Example:
A MONOID**

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Ein mathematisches Assistenzsystem

The diagram shows three main components: TeXmacs (a large text editor window), MBase/Maya (a database-like interface), and Omega (a small circular logo). Arrows indicate interactions: "Provision of Semantic Background" from TeXmacs to MBase/Maya, "Storing Documents" from MBase/Maya back to TeXmacs, and "Interactive Proof Support" from Omega to TeXmacs.

Ringvorlesung: Modellbasierte Software Entwicklung DFKI Berlin den 29. April 2004

Computer Supported Mathematics !!



Schickard:
Die erste mechanische
Rechenmaschine der Welt.

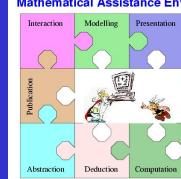
..... **Zuse:** die erste elektronische Rechenmaschine.

Ringvorlesung: Modellbasierte
Software Entwicklung



Berlin den 29. April 2004

Integrated Mathematical Assistance Environment



versus
'Pen-and-Paper'
Mathematics

- Applications**
- Mathematics research
 - Mathematics Education
 - Formal Methods, Bio-Informatics

Join of resources necessary

- System level
 - Coq, NuPrl, Isabelle/HOL, PVS, Theorema, OMEGA, Clam, ...
- Networks
 - CoCo, MxM, Monet, MoWGLI, ...



Berlin den 29. April 2004