COMPUTER-BASED MATHEMATICS

Mathematische Assistenzsysteme

Jörg Siekmann

http://www.dfki.de/~siekmann

Universität des Saarlandes
und
Deutsches Forschungszentrum
für Künstliche Intelligenz GmbH
DFKI

Was ist ein mathematisches Assistenzsystem?

http://www.activemath.org

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***
- Hilsmittel und Tools: ***Deduktions Systeme***
- Hilfsmittel und Tools: ***Proofchecker***

http://www.activemath.org

..... 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

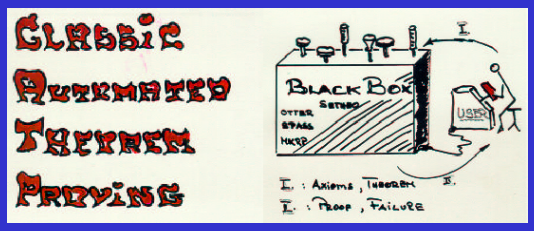
Psychology — *Scruffy*
Logic Theorist
GPS
Woody Bledsoe
Newell

Neat — Logic
Wang
Matrix
Resolution

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, ΩMEGA

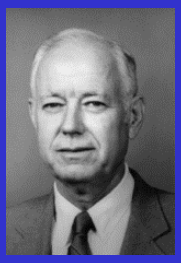
Deduction Systems



... Not The First, But The Most Serious Renegade!
Woody Bledsoe

Automated theorem proving is not the beautiful process we know as mathematics. This is „cover your eyes with blinders 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.



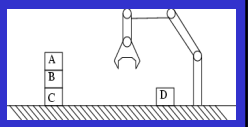
Woody Bledsoe, 1986

Can we do better ?

Knowledge based Proof Planning

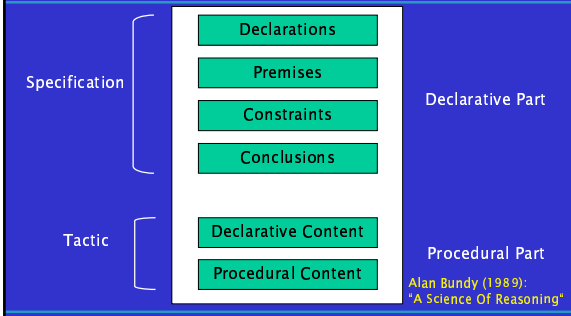
- Initial State
  on(A,B), on(B,C), on_table(C), on_table(D), free(A), ...
- Goal
  on_table(B)
- Operators
- Plan
  pick(A), putdown(A), pick(B), putdown(B)

AI–PLANNING IN THE BLOCKS WORLD



PUTDOWN(X):
precondition: holding (X)
effect: (+) on_table(X), hand_empty
(–) holding(X)

Methods in Proof Planning



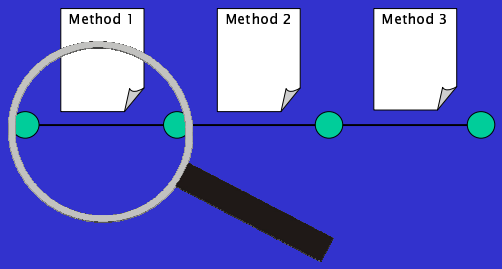
Alan Bundy (1989): "A Science Of Reasoning"

Methods: An Example

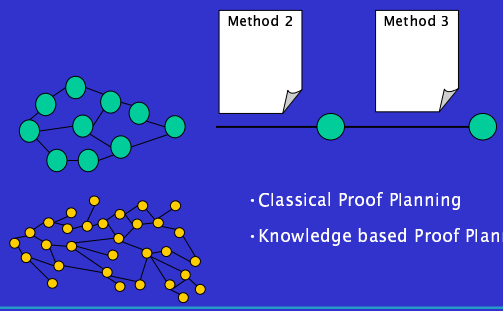
method: `Indirect`	
premises	⊕L2
conclusions	⊖L4
appl.cond	
proof schema	L1. $\neg Th \vdash \neg Th$ (HYP) L2. $\Delta, \neg Th \vdash \bot$ (OPEN) L3. $\Delta \vdash \neg\neg Th$ ($\neg$I;2) L4. $\Delta \vdash Th$ ($\neg$E;3)

Knowledge based Proof Planning

Ω mega

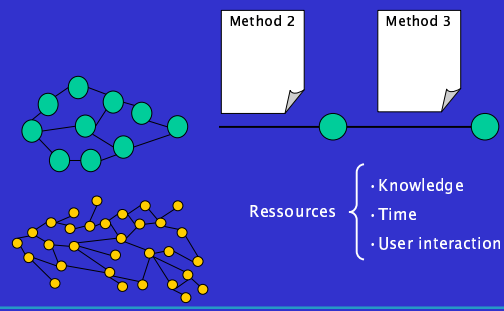


Knowledge based Proof Planning



- Classical Proof Planning
- Knowledge based Proof Planning

Knowledge based Proof Planning



Ressources
- Knowledge
- Time
- User interaction

Mathematical Control Knowledge

Global mathematical control:

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

Source: Erica Melis

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

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;	$\vdash \mathrm{EqRel}(\sigma)$	(Hyp)
2.	2;	$\vdash \mathrm{EqRel}(\rho)$	(Hyp)
3.	1;	$\vdash \mathrm{ref}(\sigma) \wedge \mathrm{symm}(\sigma) \wedge \mathrm{trans}(\sigma)$	(Def-EqRel 1)
4.	2;	$\vdash \mathrm{ref}(\rho) \wedge \mathrm{symm}(\rho) \wedge \mathrm{trans}(\rho)$	(Def-EqRel 2)
5.	5;	$\vdash \forall \tau.\forall \mu.\forall x.(\tau \cup \mu)(x) \Leftrightarrow (\tau(x) \vee \mu(x))$	(Def-Union)
97.	1,2;5	$\vdash \mathrm{ref}((\sigma \cup \rho)^t)$	(PLAN)
98.	1,2;5	$\vdash \mathrm{symm}((\sigma \cup \rho)^t)$	(PLAN)
99.	1,2;5	$\vdash \mathrm{trans}((\sigma \cup \rho)^t)$	(PLAN)
Thm.	1,2;5	$\vdash \mathrm{EqRel}((\sigma \cup \rho)^t)$	(Def-EqRel 97 98 99)

More Examples: epsilon-delta Proofs

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

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

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

Woody Bledsoe: "Challenges"

Method for Limit Theorems

method: ComplexEstimate	
premises	L1, ⊕L2,⊕L3, ⊕L4
conclusions	⊖L7
appl.cond	$\exists k, l, \sigma(\mathtt{CASextract}(a, b) = (k, l, \sigma))$
proof schema	L1. Δ ⊢ $\lvert a\rvert < e_1$ () L2. Δ ⊢ $\lvert k\rvert \leq \mathbf{M}$ (OPEN) L3. ⊢ $\lvert a_\sigma\rvert < \epsilon/2 * \mathbf{M}$ (OPEN) L4. Δ ⊢ $\lvert l\rvert < \epsilon/2$ (OPEN) L5. ⊢ $b = b$ (Ax) L6. ⊢ $b = k * a_\sigma + l$ (CAS;L5) L7. Δ ⊢ $\lvert b\rvert < \epsilon$ (fix;L2, L3,L4,L6)

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

Source: Erica Melis

Construction of mathematical Objects

CONSTRAINT SOLVING:

Collecting constraints and check for consitency

Final constraint store for LIM+

$$\begin{array}{rcccl} 0 & < & E_2 & \leq & \epsilon/2; \\ 0 & < & D & \leq & \delta_2, \delta_1; \\ 0 & < & E_1 & \leq & \epsilon/(2 * \mathbf{M}), \epsilon/2; \\ 1 & \leq & \mathbf{M} & < & \epsilon/(2 * E_1); \\ -\infty & < & X_1 = x = X_2 & < & +\infty \end{array}$$

Source: Erica Melis

Proof Presentation to the User

Verbalisation of ComplexEstimate:

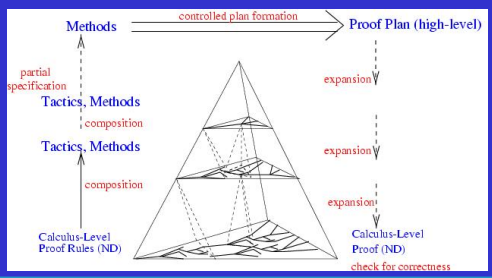
In order to estimate the magnitude of $|b|$
we rewrite the term to $|k * a + l|$
and use the Triangle Inequality $|k * a + l| \leq |k * a| + |l|$.
Now the goal can be shown in three steps:

- 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 $|b| < \epsilon$.

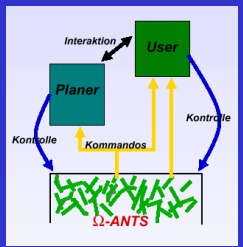
Source: Erica Melis

PDS: Representation of (partial) Proofs



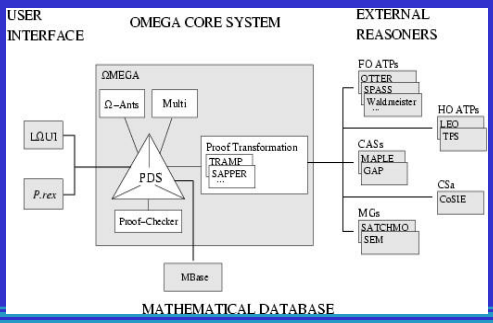
ΩMEGA –ANTS: Combining ATP with Proof Planning

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

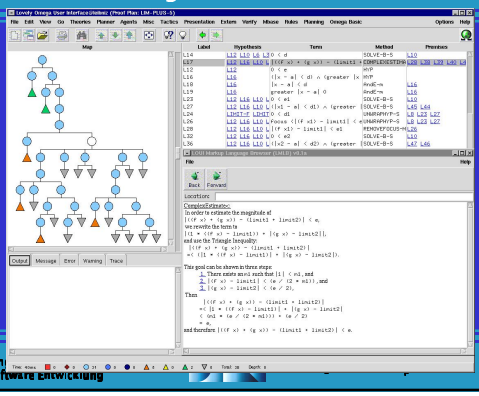


Chris Benzmüller, Volker Sorge

The OMEGA SYSTEM



Proof Planning: A Screen Shot



Zwei Entwicklungsrichtungen:

1. Verifikationswerkzeuge: z.B. **VSE** am DFKI

2. Mathematische Tutorsysteme:
   z.B. **ActiveMath** am DFKI

---

anwendungsorientierte Grundlagenforschung!

Zwei Entwicklungsrichtungen:

CHALLENGE:

Ein integriertes mathematisches Assistenzsystem

Grundlagenforschung!

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

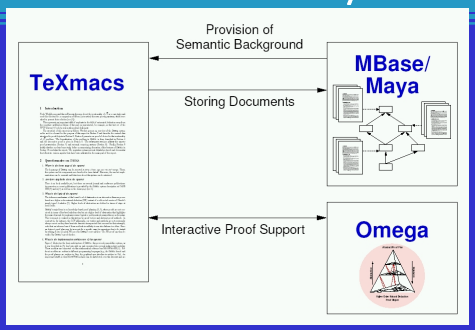
Mathematical Ontology

Knowledge: the building blocks in OMDoc

```
<definition id="c6s1p4_Th2_def_monoid" for="c6s1p4_monoid">
<metadata>
    <depends-on>
    <ref theory="cp1_Th3" name="structure" />
  </depends-on>
  <Title xml:lang="en">Definition of a monoid</Title>
 </metadata>
<CMP xml:lang="en" format="omtext">
A monoid is a <ref xref="cp1_Th3_def_structure"> structure </ref>
 <OMOBJ>
<OMS cd="elementary" name="ordered-triple"/>
    <OMV name="M"/> <OMS cd="cp4_Th2" name="times"/> <OMS cd="cp4_Th2" name="unit"/>
</OMOBJ>
in which
<OMOBJ>
<OMS cd="elementary" name="ordered-pair"/>
    <OMV name="M"/> <OMS cd="cp4_Th2" name="times"/>
</OMOBJ>
is a semi-group
with <ref xref="c6s1p3_Th2_def_unit">unit</ref>
<OMOBJ xmlns="http://www.openmath.org/OpenMath">
    <OMS cd="cp4_Th2" name="unit"/>
</OMOBJ>.
</CMP>
<FMP><OMOBJ> ... </OMOBJ></FMP>
</definition>
```

An Example:
A MONOID

Ein mathematisches Assistenzsystem



Computer Supported Mathematics !!

Schickard:
Die erste mechanische Rechenmaschine der Welt.

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