OpenMath for knowledge-based automated theorem proving

Michael Kohlhase
Fachbereich Informatik
Universität des Saarlandes
66041 Saarbrücken, Germany
http://www.ags.uni-sb.de/~kohlhase/

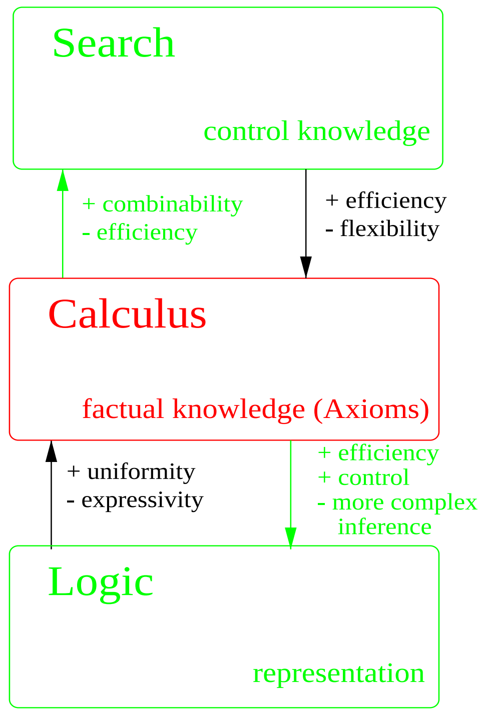
What is Mechanised Reasoning

- The field is 40 years old now
- It is a subfield of Artificial Intelligence
- **Motivation**:
  Exhibiting Intelligence by mechanising the “Queen of Sciences”
- Mechanised Reasoning System (MRS) = software system that synthesises proofs
  - Representing the problem in formal logic
  - search for the proof on the level of a logical calculus (automatically (ATP), interactively (ITP), human-oriented (HTP))
  - (optional) Proof beautification/presentation

State of the Art in Mechanised Reasoning

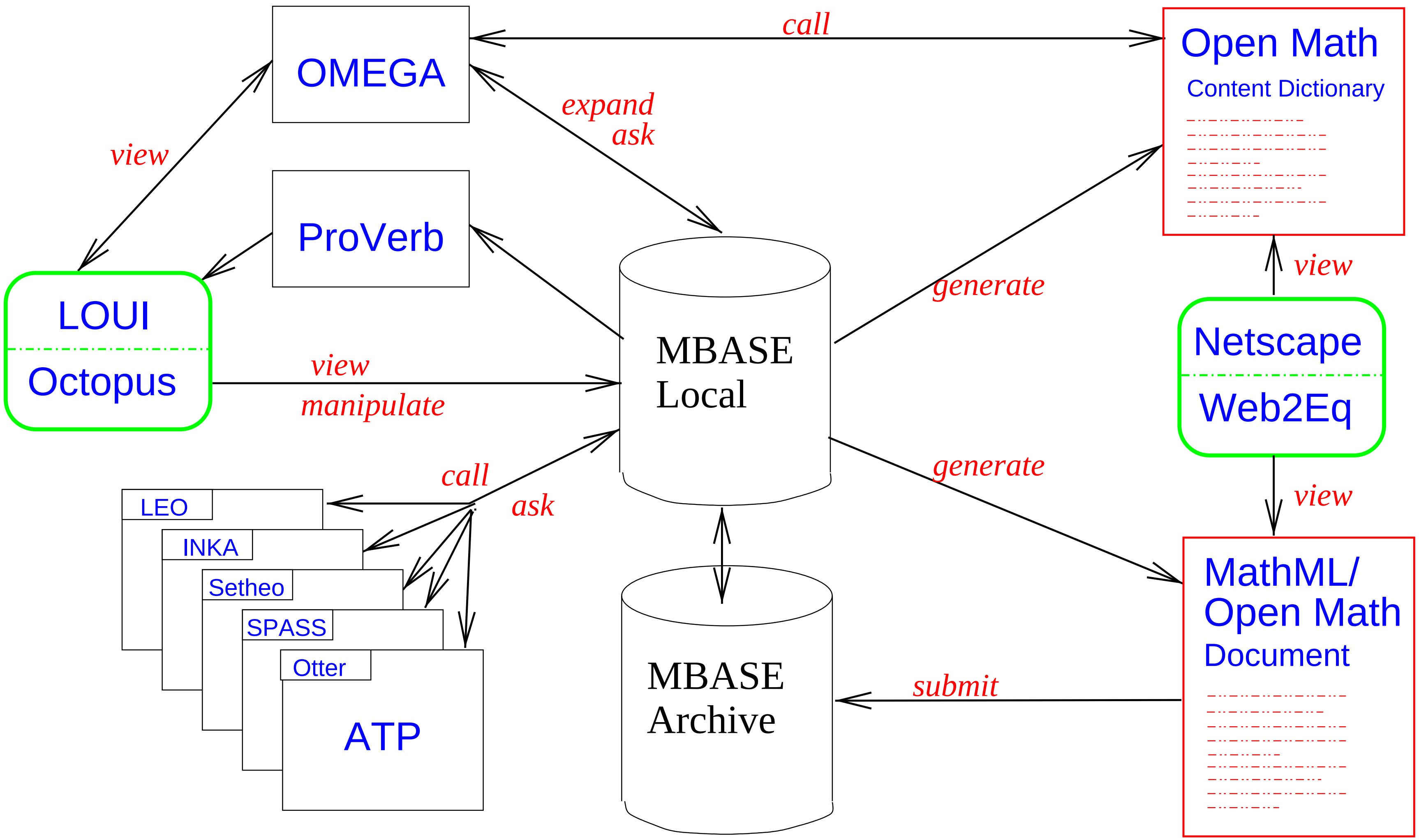
- In the Applications
  - Program verification/synthesis: Moving into industrial applications
  - Mathematics: only applicable for relatively trivial problems
  - Natural Language Processing: Basic research necessary
- Is not an accepted tool in mathematical practice.
- Trends: Try to overcome limitations by AI methods
  - Knowledge-based theorem proving, Cooperation of ATP
  - Idea:, use agents and OpenMath for this
  - In this talk: MBase a mathematical knowledge base system.

Knowledge-Based Theorem Proving?



- Expressive representation formalisms (Knowledge local)
  - Higher-order logic, sorted λ-calculus, . . .
- Specialized inference processes (Knowledge implicit)
  - Superposition, LEO, constraint-solvers, computer-algebra, . . .
- proof planning (explicit method- and control knowledge)
  - methods as plan operators, control rule interpreter . . .
- Knowledge base (stockpiling knowledge)
  - Inheritance, structure morphisms, RDBMS, semantic search,. . .
- knowledge acquisition (e.g. reading math books)

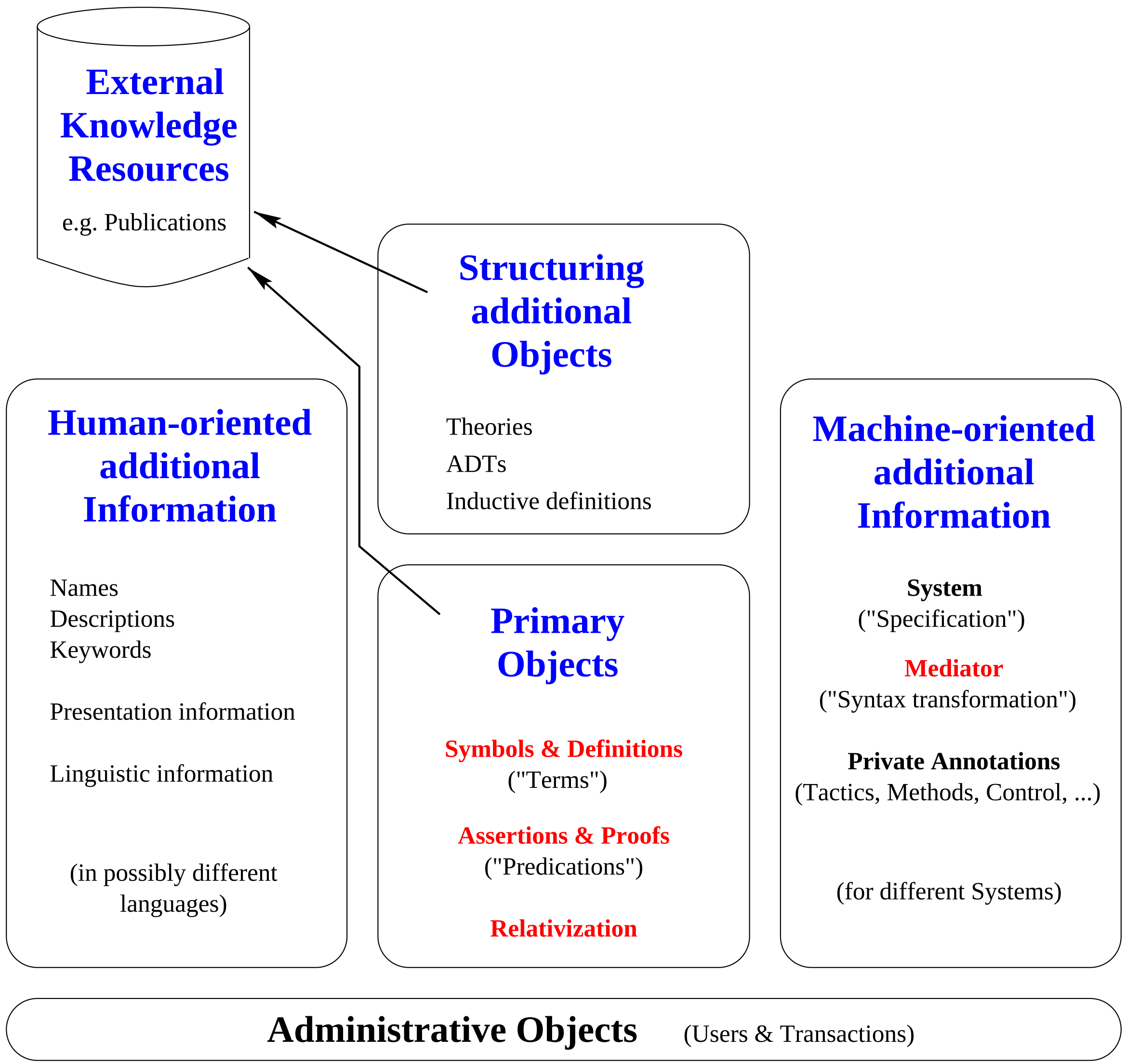
Knowledge-Based, Distributed TP in MATHWEB



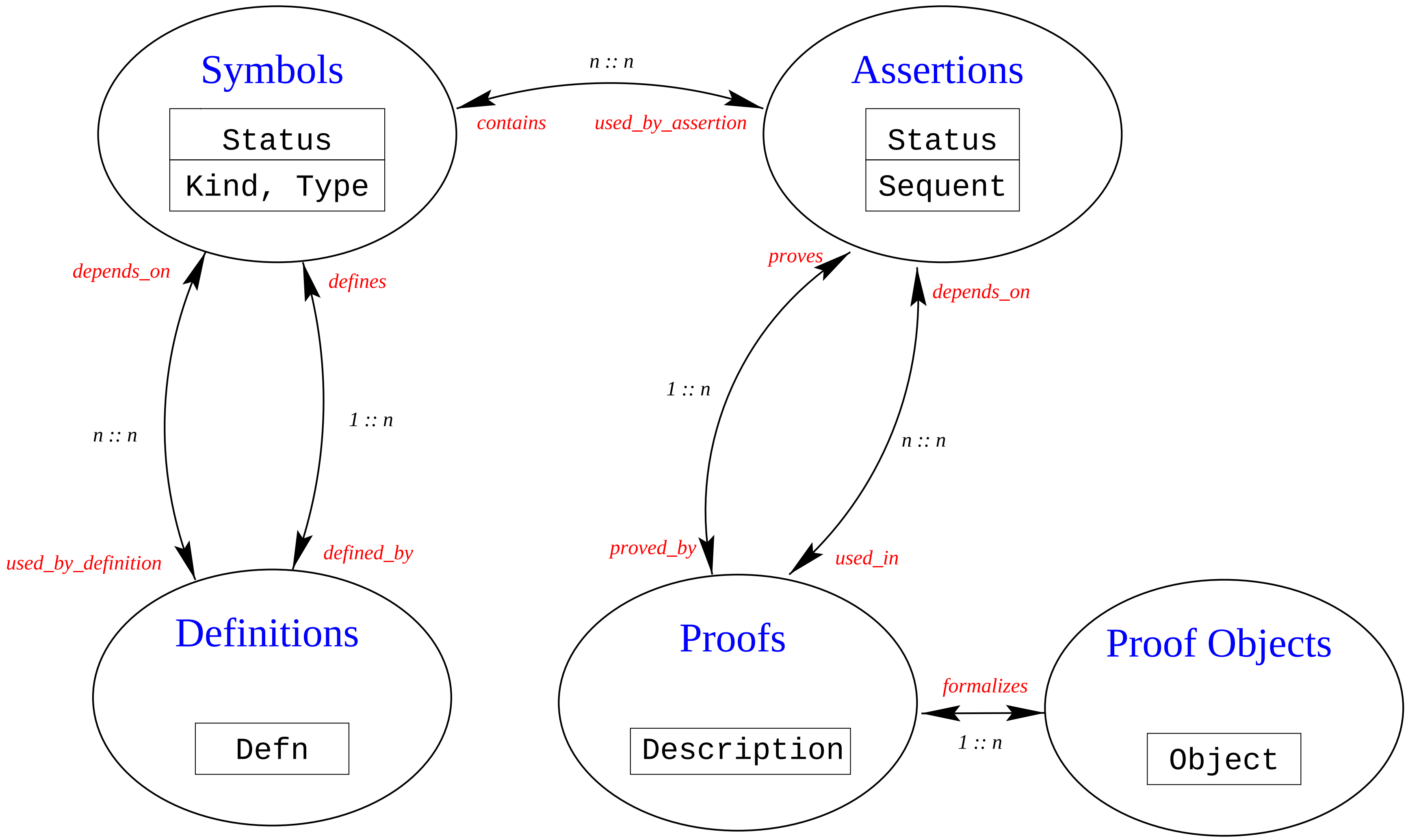
MATHWEB: Implementation and Availability

- Agent shells are implemented in MOZART OZ 3.0 (concurrent, OO, constraint-logic programming language)
  - Get network communication layer for free
  - Tested with ΩMEGA, DORIS
- Available Mathematical Services include:
  - Automated theorem provers: OTTER, SPASS, PROTEIN, BLIKSEM, TPS, EQP, ...
  - Proof Transformers: from these to Natural Deduction
  - Computer Algebra Systems: MAPLE, MAGMA, GAP
  - User Interface: $\mathcal{L}\Omega\mathcal{UI}$ (runs as an agent on client machine)
  - Proof Presentation: Verbalization in natural language (English)
  - Knowledge base: MBASE (rest of the talk)

The Data Model in MBase



Primary Objects in MBASE



λ-Calculus: an expressive Formalism for Mathematics

- **Example**: Cantor's Theorem: $\neg(countable(\mathbb{N}^{\mathbb{N}}))$
- **Theorem**: *The set of sequences of natural numbers is uncountable.*
  - **countable** $:= \lambda M.\exists F.surj(F, \mathbb{N}, M)$ or $\lambda M.\neg\exists F.inj(F, M, \mathbb{N})$
  - **surj** $:= \lambda FMN.\forall X \in M.\exists Y \in N.FY = X$
  - $\mathbf{A}^{\mathbf{B}} = \lambda F.\forall X.\mathbf{A}X \Rightarrow \mathbf{B}(FX)$.
- **Proof**: (Diagonalisation)
  Assume that there is a surjective mapping $f\colon \mathbb{N} \longrightarrow \mathbb{N}^{\mathbb{N}}$. Consider the diagonal sequence $g(i) := f(i,i)$. Increment ($h(i) := f(i,i) + 1$); obviously $h \neq f(j)$ for all $j \in \mathbb{N}$, so $h \notin \mathbf{Im}(f)$ (contradiction).

Correctness Management

- Problem: Consistency is a central concern for any knowledge base.
- Theory: Consistency cannot be ensured [Gödel'32].
- Practice: Reduce problem to small set of axioms. (Conservative/Definitional Extension, proofs)
- Evidence for consistency in MBase
  - published NL proof, typical examples, semi-formal proof, peer review.
  - Full proofs can be too large/tedious
  - Conjectures are first-class citizens of mathematics, e.g. in the initial development of a theory.

OpenMath as a Content Language for MathWeb

- Desiderata: Need to express
  - Formulae and terms with meta-variables
  - Formal proof objects and computations (with meta-variables)
  - Specifications of (fragments of) logical systems,
- Schematic Objects $(decl, object, seqent, resource, language)$
- Idea: Use OpenMath with new content dictionary `OpenProof`.
  - Schema Symbols: `formula`, `term`, `proof`, `computation`
  - Attribute Symbols: `language`, `type`
  - Further CDs for logical systems proper `FFOL`, `ND(FOL)`, `HOL`, `ECC`,...

Example: Schematic Formula

```
<OMOBJ><OMBIND>
   <OMS cd="openproof" name="formula"/>
   <OMBVAR>
      <OMATTR><OMATP>
                <OMS cd="openproof" name="language"/>
                <OMS cd="FFOL" name="CNF"/>
              </OMATP>
           <OMV name="F"/>
      </OMATTR>
   </OMBVAR>
   <OMV name="F"/>
</OMBIND><OMOBJ>
```

Proofs in OpenMath

- Idea: Use Propositions-as-Types: $\Rightarrow I(\lambda X_{A\wedge B}.\wedge I(\wedge ER(X), \wedge EL(X))$

$$\cfrac{\cfrac{\cfrac{[A\wedge B]}{B}\wedge ER \quad \cfrac{[A\wedge B]}{A}\wedge EL}{B\wedge A}\wedge I}{A\wedge B\Rightarrow B\wedge A}\Rightarrow I$$

```
<OMOBJ><OMBIND><OMS cd="ND(FOL)" name="impliesI"/>
   <OMBVAR><OMATTR>
      <OMATP>
         <OMS cd="openproof" name="type"/>
          A ∧ B
      </OMATP>
   <OMV name="X"/>
</OMATTR></OMBVAR>
   <OMA><OMS cd="ND(FOL)" name="andI" >
     <OMA><OMA><OMS cd="ND(FOL)" name="andEr">
             <OMV name="X"/>
          </OMA>
        <OMA><OMS cd="ND(FOL)" name="andEl">
           <OMV name="X"/>
   </OMA></OMA></OMA>
</OMBIND></OMOBJ>
```

The Curry-Howard Isomorphism

- Idea: use the structural similarity between λ-Calculus and ND.
  - $\rightarrow$ vs. $\Rightarrow$
  - Types vs. Formulae ("'propositions as types"')
  - λ-terms vs. Proofs ("'Proof terms"', "'proofs as programs"')
  - $\mathit{wff}{:}\mathit{app}$ vs. $\Rightarrow E$, $\mathit{wff}{:}\mathit{abs}$ vs. $\Rightarrow I$
- $\mathbf{A}$ provable, iff α non-empty e.g. for Hilbert-Axioms
  - $\lambda X_\alpha \lambda Y_\beta . X_\alpha$ has Type $\alpha \rightarrow \beta \rightarrow \alpha$
  - $\lambda X_{\alpha\rightarrow\beta\rightarrow\gamma} \lambda Y_{\alpha\rightarrow\gamma} \lambda Z_\gamma . X(Z, Y(Z)) : (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta) \rightarrow \alpha \rightarrow \gamma$
- New CD `OpenProof` containing symbols for all ND inference rules

The Curry-Howard Isomorphism (Example)

$$\dfrac{\dfrac{\Gamma \vdash X{:}\alpha \to \beta \to \gamma \quad \Gamma \vdash Z{:}\alpha \quad \dfrac{\Gamma \vdash Y{:}\alpha \to \beta \quad \Gamma \vdash Z{:}\alpha}{\Gamma \vdash YZ{:}\beta}}{\Gamma \vdash X(Z,Y(Z)){:}\gamma}}{\dfrac{[X{:}\alpha \to \beta \to \gamma],[Y{:}\alpha \to \beta] \vdash_\Sigma \lambda Z.X(Z,Y(Z)){:}\alpha \to \gamma}{\dfrac{[X{:}\alpha \to \beta \to \gamma] \vdash_\Sigma \lambda YZ.X(Z,Y(Z)){:}(\alpha \to \beta) \to \alpha \to \gamma}{\emptyset \vdash_\Sigma \lambda XYZ.X(Z,Y(Z)){:}(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma}}}$$

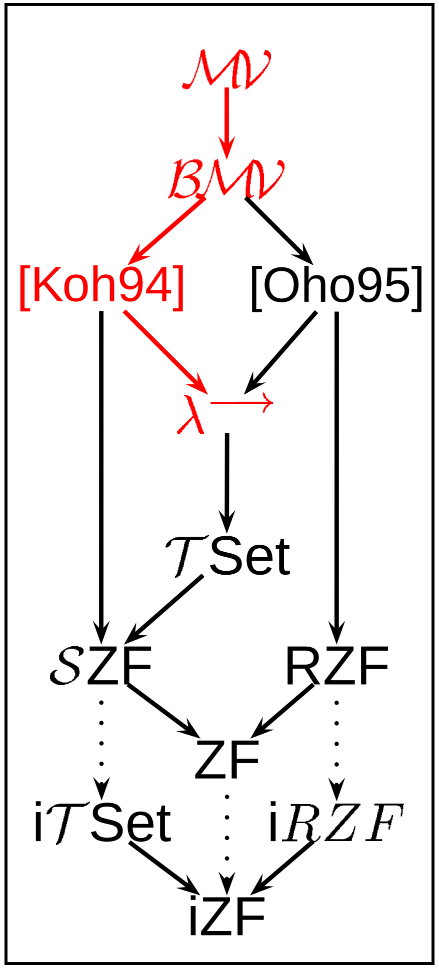
wobei $\Gamma = [X{:}\alpha \to \beta \to \gamma],[Y{:}\alpha \to \beta],[Z{:}\alpha]$

Logical Issues

- The representation formalism must meed conflicting requirements!
- Quasi-religious battle over the “right logic”
  - classical vs. constructive
  - typed (λ-calculus) vs. untyped (set theory)
  - if types, how strong? (simple, polymorphic, records, dependent)
  - machine-oriented vs. human-readable
  - partial functions? multi-valued?
- MBase: Conservative Extension Principle with Logic Morphisms (accommodate for all possible desires.)

Logic Morphisms

- Definition: **Logical System** $\mathcal{S} = (\mathcal{L}, \mathcal{C})$,
  - $\mathcal{L}$ language (set of well-formed formulae)
  - $\mathcal{C}$ calculus (set of inference rules)
  - $\mathcal{D}{:}\,\mathcal{H} \vdash_{\mathcal{C}} \mathbf{A}$ is a $\mathcal{C}$-derivation of $\mathbf{A}$ from $\mathcal{H}$
- Definition: **Logic Morphism** $\mathcal{F}{:}\,\mathcal{S} \longrightarrow \mathcal{S}'$,
  - **Language Morphism** $\mathcal{F}^{\mathcal{L}}{:}\,\mathcal{L} \longrightarrow \mathcal{L}'$
  - **Calculus Morphism** $\mathcal{F}^{\mathcal{D}}$ from $\mathcal{C}$-derivations to $\mathcal{C}'$-derivations, such that for any $\mathcal{C}$-derivation $\mathcal{D}{:}\,\mathcal{H} \vdash_{\mathcal{C}} \mathbf{A}$, we have $\mathcal{F}^{\mathcal{D}}(\mathcal{D}){:}\,\mathcal{F}^{\mathcal{L}}(\mathcal{H}) \vdash_{\mathcal{C}'} \mathcal{F}^{\mathcal{L}}(\mathbf{A})$.
- Logic morphisms transport proofs!



Sorted λ-Calculus

- Distinguish between **Sorts** and **Types**
- **Term declarations** as general Mechanism

Example:

$$[+::\mathbb{N} \to \mathbb{N} \to \mathbb{N}]$$
$$[+::\mathbb{E} \to \mathbb{E} \to \mathbb{E}]$$
$$[+::\mathbb{O} \to \mathbb{O} \to \mathbb{E}]$$
$$[(\lambda X. + X\,X)::\mathbb{N} \to \mathbb{E}]$$

Higher-Order Unification

$$\mathbf{G}_{\mathbb{E}}{}^{+}(\Sigma) = \left\{ \begin{array}{l} +Z_{\mathbb{E}}W_{\mathbb{E}}, \\ +Z_{\mathbb{O}}W_{\mathbb{O}}, \\ +Z_{\mathbb{N}}Z_{\mathbb{N}} \end{array} \right\}$$

- **functional** base sorts: e.g. $(\lambda X.X)::\mathbb{C} \leq \mathbb{R} \to \mathbb{R}$,
- **intersection sorts**: z.B. $[+::\mathbb{N} \to \mathbb{N} \to \mathbb{N} \sqcap \mathbb{E} \to \mathbb{E} \to \mathbb{E} \sqcap \mathbb{O} \to \mathbb{O} \to \mathbb{E}]$
- Closure under $\beta\eta$-equality

Relativisation = Morphism to $\Lambda^{\rightarrow}$

- Signature: $\mathcal{R}([+{::}\mathbb{N} \to \mathbb{N} \to \mathbb{N}]) = \forall X, Y.\mathbb{N}(X) \wedge \mathbb{N}(Y) \Rightarrow \mathbb{N}(X + Y)$.
- Formulae: $\mathcal{R}(\forall X_{\mathbb{B}}.\mathbf{A}) = \forall X.\mathbb{B}(X) \Rightarrow \mathcal{R}(\mathbf{A})$
- Sorts: $\mathcal{R}\left(\dfrac{\mathbf{A}{::}\mathbb{B} \to \mathbb{C} \quad \mathbf{B}{::}\mathbb{B}}{\mathbf{A}\mathbf{B}{::}\mathbb{C}}\right) = \dfrac{\dfrac{\forall X.\mathbb{B}(X) \Rightarrow \mathbb{C}(\mathbf{A}X)}{\mathbb{B}(\mathbf{B}) \Rightarrow \mathbb{C}(\mathbf{A}\mathbf{B})} \quad \mathbb{B}(\mathbf{B})}{\mathbb{C}(\mathbf{A}\mathbf{B})}$
- Proofs: $\mathcal{R}\left(\dfrac{\forall X_{\mathbb{B}}.\mathbf{A} \quad \mathbf{B}{:}\,\mathbb{B}}{[\mathbf{B}/X]\mathbf{A}}\right) = \dfrac{\dfrac{\forall X.\mathbb{B}(X) \Rightarrow \mathcal{R}(\mathbf{A})}{\mathbb{B}(\mathcal{R}(\mathbf{B})) \Rightarrow \mathcal{R}([\mathbf{B}/X]\mathbf{A})} \quad \mathbb{B}(\mathbf{B})}{\mathcal{R}([\mathbf{B}/X]\mathbf{A})}$

Mathematical Vernacular (Structures)

- Approximate day-to-day language of mathematicians
- In particular support for **algebraic structures**.
- **Record-Sorts**: e.g. group $\begin{bmatrix} \mathsf{Set} & :: \mathbb{T}\mathsf{op}_{\alpha\to o} \\ \mathsf{Op} & :: \mathbb{A}\to\mathbb{A}\to\mathbb{A} \\ \mathsf{Neut} & :: \mathbb{A} \\ \mathsf{Inv} & :: \mathbb{A}\to\mathbb{A} \end{bmatrix}$
- Analogous: application with labels, e.g. associativity

$$\mathsf{assoc} := \lambda^{\mathsf{Set}} S.\lambda^{\mathsf{Op}} F.\forall X_{\mathbb{A}}.\forall Y_{\mathbb{A}}.\forall Z_{\mathbb{A}}.FX(FYZ) = F(FXY)Z$$

- Problem: what is the relation between Sort $\mathbb{A}$ and set S.

Dependent Sorts, Selection Sorts

- Idea: Use record-labels as dependent sorts
- Example: set operation $\mathbb{S}\mathsf{etop} := [\mathsf{Set}::\mathbb{T}\mathsf{op}_{\alpha\to o}, \mathsf{Op}::\mathsf{Set} \to \mathsf{Set} \to \mathsf{Set}]$
- prove $\mathbb{N}::\mathbb{T}\mathsf{op}_\iota$ and $+::\mathbb{N} \to \mathbb{N} \to \mathbb{N}$ for $[\mathsf{Set} = \mathbb{N}; \mathsf{Op} = +]::\mathbb{S}\mathsf{etop}$
- Analogous: $\mathsf{assoc}::\mathbb{T}\mathsf{op}_{\alpha\to o} \xrightarrow{\mathsf{Set}} (\mathsf{Set} \to \mathsf{Set} \to \mathsf{Set}) \xrightarrow{\mathsf{Op}} \mathbb{T}\mathsf{op}_o$
- Problem: semigroups are associative
- Idea: Use **selection sorts**: (compare to $\{X \in \mathbb{A} \mid \mathbf{A}\}$).

$$\mathbb{S}\mathsf{emigroup} := \{\mathbb{S}\mathsf{etop} | (\lambda X.[\mathsf{assoc}@_{\mathsf{Set}}(X.\mathsf{Set})@_{\mathsf{Op}}(X.\mathsf{Op})])\}$$

- and so on...

Knowledge Acquisition (Rambo)

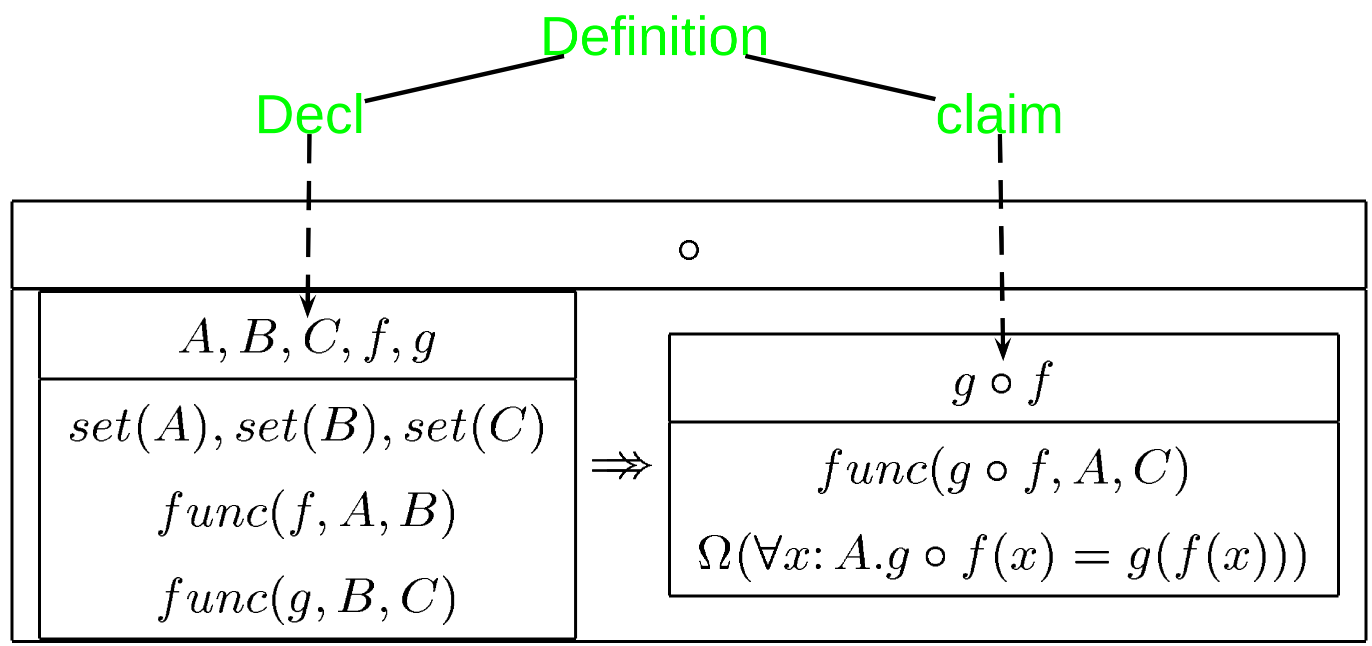
- Where does all the knowledge for MBASE come from?
- Idea: Reading math books!
  - Cooperative, restricted vocab, syntax and ambiguity.
  - discourse structure explicitly marked
  - Object ontology (mathematics) totally formalized (Bourbaki)
- State: 3 Theorems + proofs (Masters Thesis Baur)
  - Theorem 2.3.3 (Triangle Inequality) For any a and b in $\mathbb{R}$, we have $|a + b| \leq |a| + |b|$.
  - Proof: From 2.3.2(e), we have $-|a| \leq a \leq |a|$ and $-|b| \leq b \leq |b|$. Then, adding and using 2.2.6(b), we obtain

$$-(|a| + |b|) \leq a + b \leq |a| + |b|$$

Hence we have $|a + b| \leq |a| + |b|$ by 2.3.2(d).

Discourse Semantics of a Definition

- **Definition 1.2.8**: For functions $f\colon A \longrightarrow B$ and $g\colon B \longrightarrow C$, the **composite function** $g \circ f$ (note the order!) is the function from A to C defined by $g \circ f(x) := g(f(x))$ for $x \in A$. (see figure 1.2.5.)
- Semantics = Discourse structure + Discourse representation structures (DRS)

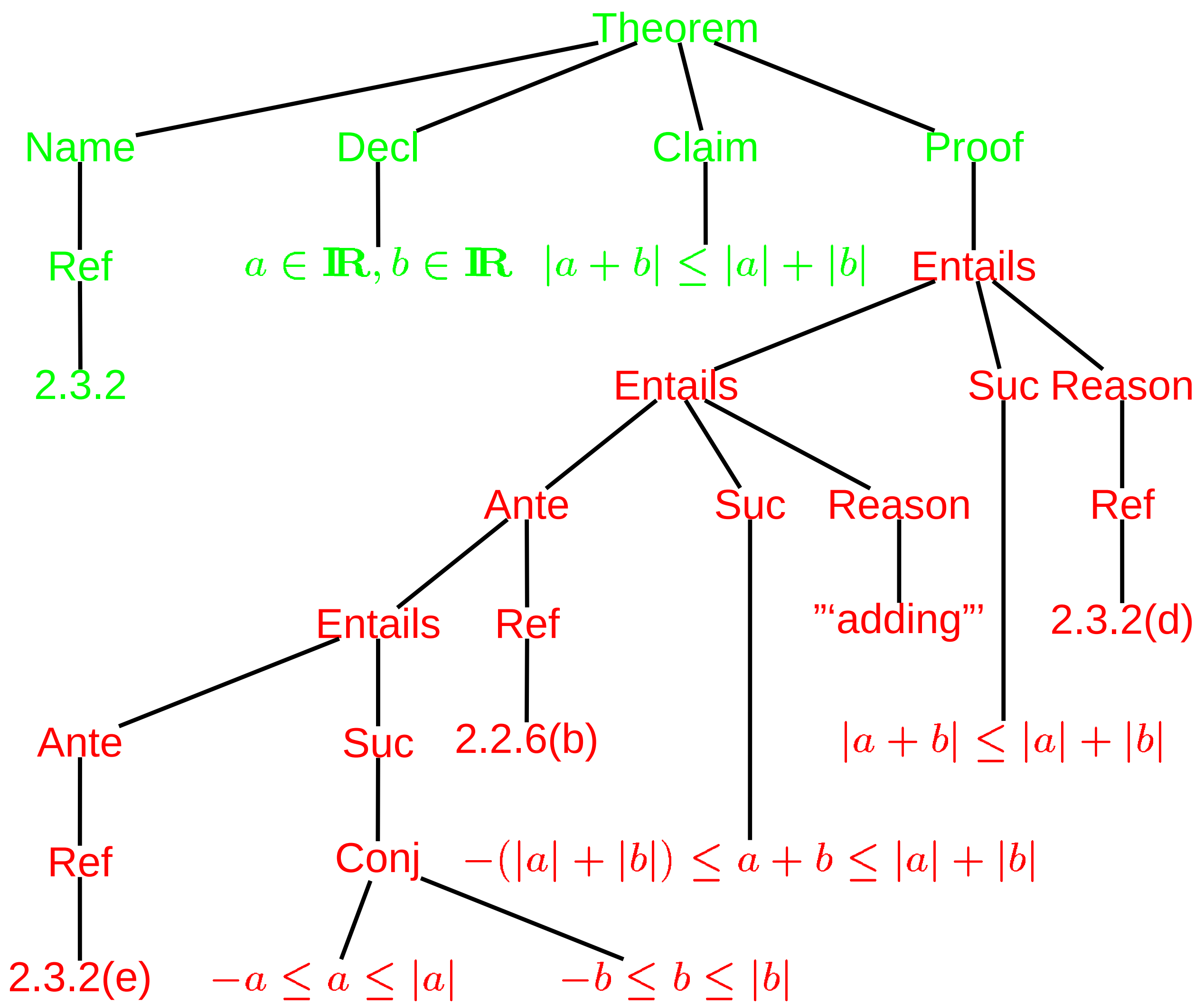


Representation in MBase

symbol

$Name$	:	compose-functions
Key	:	`BarShe:itra82;1.2.8`
$Type$	:	$\forall\alpha\beta\gamma.(\beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma$
$Formula$	:	$\lambda F \lambda G \lambda z.F(Gz)$
$Help$	:	Function Composition

Discourse Structure of a Theorem



Yields the Proof Plan

L1	L1	$\vdash a \in \mathbb{R}$	(Ass)
L2	L2	$\vdash b \in \mathbb{R}$	(Ass)
L3	L1	$\vdash -a \leq a \leq \lvert a\rvert$	(plan L1 2.3.2(e))
L4	L2	$\vdash -b \leq b \leq \lvert b\rvert$	(plan L2 2.3.2(e))
L5	L1,L2	$\vdash -(\lvert a\rvert + \lvert b\rvert) \leq a + b \leq \lvert a\rvert + \lvert b\rvert$	(plan L3 L4 2.3.2(b) “adding”)
Ass	L1,L2	$\vdash \lvert a + b\rvert \leq \lvert a\rvert + \lvert b\rvert$	(plan L5 2.3.2(d))

- Direct image of the discourse semantics

Conclusions

- Cooperative knowledge-based Theorem proving as an application area for OpenMath.
  - agent-based model for integration of mathematical services
  - Communication Language: KQML; Content language OpenMath
  - Implemented (http://www.ags.uni-sb.de/~omega)!
- Knowledge base system MBase
  - gives a semantics to interaction/integration
  - can be used to generate/replace content dictionaries
  - Knowledge Acquisition by reading MathML/OpenMath

Desiderata for OpenMath

- Status of Content Dictionaries
  - `<Defmp>` proposal (see last talk)
  - Inheritance of CDs (Model the structure of MBase?)
  - Dynamic CDs (as a joint base of communication)
- Integrate OpenMath/MathML beyond K-12 (Definitions, Theorems, proofs,. . .)
- Towards Plug-and-Play mathematics