Logosphere

A Digital Library of Formal Proof

Carsten Schürmann

IT University of Copenhagen

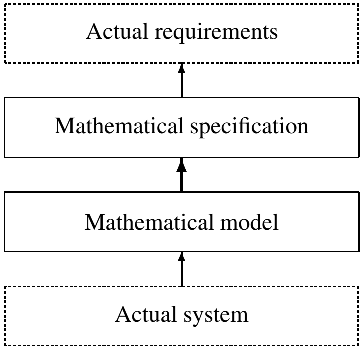
Processor Verification

- INTEL (HOL/HOL light). [John Harrison]
  - $500mio Pentium bug.

- AMD (ACL2, Nqthm). [Matt Kaufmann]
- Siemens, Microsoft (ASM). [Yuri Gurevich]

What's Intel up to?

HOL [Harrison'03]



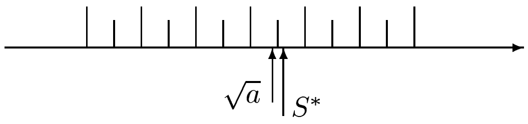
Actual requirements

Mathematical specification

Mathematical model

Actual system

Floating Point arithmetic.



Round the same way if

$$|\sqrt{a} - S^*| < |\sqrt{a} - m|$$

```
|- ¬(precision fmt = 0) ∧
   (∀m. m IN midpoints fmt
        ⟹ abs(x - y) < abs(x - m))
   ⟹ (round fmt Nearest x =
        round fmt Nearest y)
```

What’s Intel up to?

Trigonometric range reduction.

HOL $x = N(\pi/2) + r$

where N is the integer closest to $x \cdot \frac{2}{\pi}$ and $|r| \leq \pi/4$.

What happens if x close to a multiple of $\pi/2$?

```
#let pth = PI_APPROX_RULE 5;;
pth : thm =
   |- abs(pi - &26696452523 / &8498136384)
      <= inv (&2 pow 5)
```

```
|- integer(N) ∧ ¬(N = &0) ∧
   a ∈ iformat (rformat Register) ∧
   abs(a) < &2 pow 64
   ⟹ abs (a - N * pi / &2) >= &113 / &2 pow 76
```

What’s Intel up to?

Large HOL libraries of mathematical knowledge and proofs.

Example: Reals library.

Years of development effort.

Little sharing with the community.

Not surprising: Intel intellectual property.

NASA Space Shuttle

Langely Research Center. [Butler ‘98]

PVS (Prototype Verification System). [Owre]

Example:

GPS Receiver State Processing.

GPS Reference Sate Processing.

Result: 86 issues or minor discrepancies were discovered.

NASA Space Shuttle

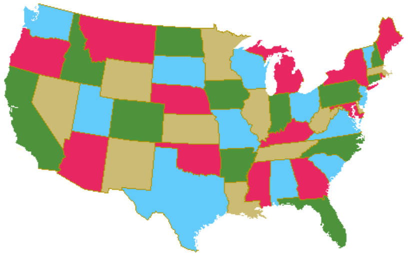
Huge PVS libraries developed at NASA.

Algebra, Real analysis, Complex numbers, Directed graphs, Graph theory, Integer division, Abstract orders, Lattices, Fixed Points, Power sets, Trigonometry, Series, Taylor's theorem etc.

Sharing ok, but how?

Mathematics

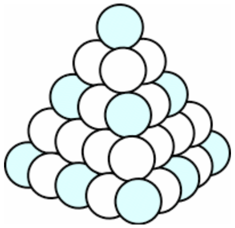
Four-Color theorem [Appel, Haken 1976]



Kepler's Conjecture

2D [Thue 1890]

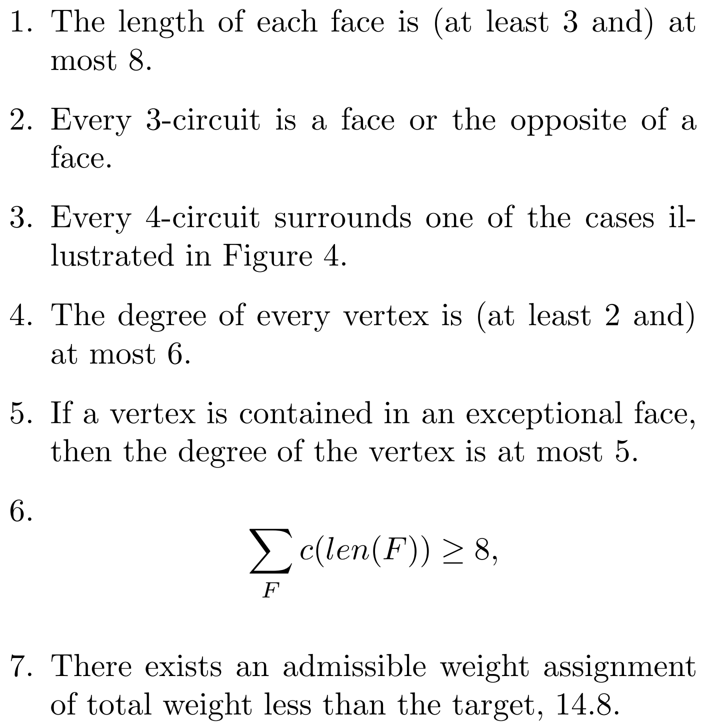
3D [Hales 1989]



The Flyspeck Project

- Formal proof of Kepler's conjecture.
- ETA: 20 years.
- HOL light.
- Hopes for access to Coq, Isabelle/HOL.
- Tame Planar Graphs.

[Hales, Nipkow, MacLaughlin]

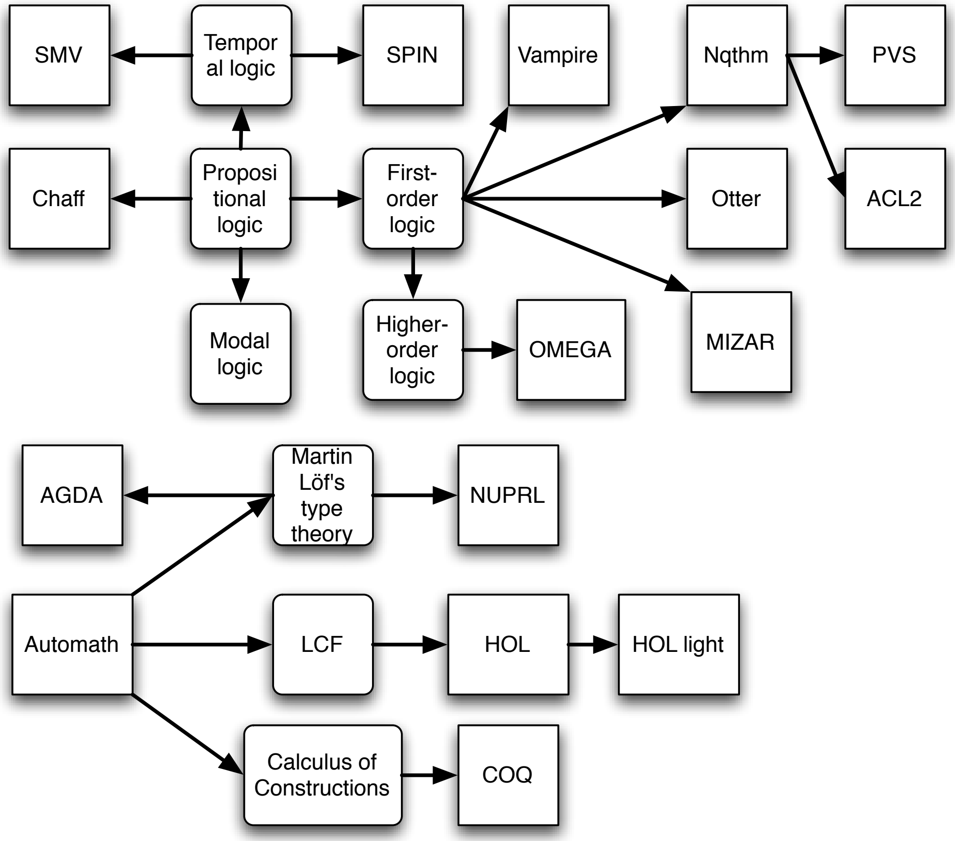


1. The length of each face is (at least 3 and) at most 8.
2. Every 3-circuit is a face or the opposite of a face.
3. Every 4-circuit surrounds one of the cases illustrated in Figure 4.
4. The degree of every vertex is (at least 2 and) at most 6.
5. If a vertex is contained in an exceptional face, then the degree of the vertex is at most 5.
6. $$\sum_F c(len(F)) \geq 8,$$
7. There exists an admissible weight assignment of total weight less than the target, 14.8.

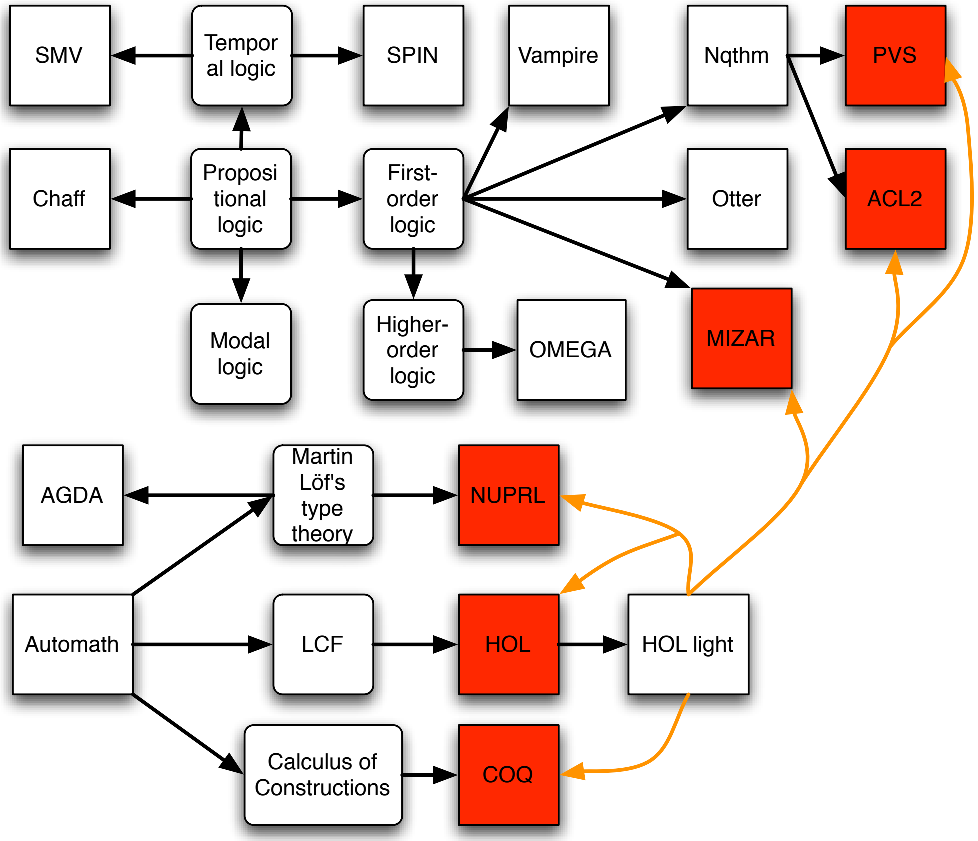
MIZAR [Trybulec'72]

- Reconstruct mathematical vernacular.
- Proof verifier.
- Large body of mathematical knowledge.
- No explicit proof objects.
- Journal of formalized mathematics.
  - On the Hausdorff distance between compact subsets. [Adam Grabowski]
  - Chains on a grating in Euclidean space. [Freek Wiedijk]

Logic Diversification



Library Growth



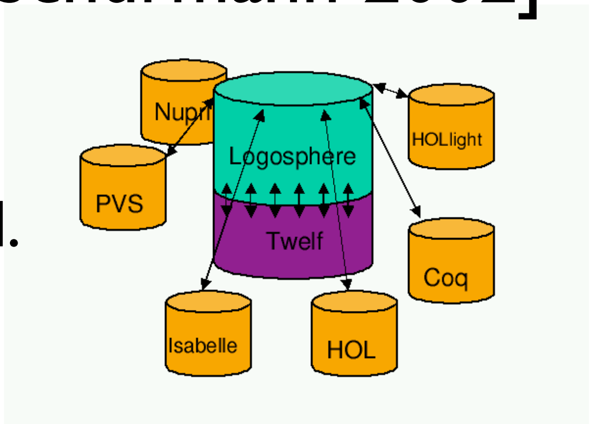
Digital Libraries

FDL library. [Constable 2000]

- Storage, retrieval of mathematical facts.
- Logic dependent.

Logosphere. [Schürmann 2002]

- Logical framework.
- Foundationally uncommitted.
- Theory morphisms.
- Currently under development.



What shall we store?

Semantic meaning of a theorem!

Formulas alone insufficient.

- Logics vary in proof-theoretic strength.
- Example: First-order logic vs. impredicative type theory.
- Semantics-preserving transformations.

$$\models_{\mathcal{L}_1} F_1 \quad \Longrightarrow \quad \models_{\mathcal{L}_2} F_2$$

Meaning of theorems ...

... are mathematical entities expressed as

- Denotations (Domain theory).
- Objects (Category theory).
- {0,1} (Model theory).
- Strategies (Game theory).
- Syntactic Proofs (Proof Theory).

Large proofs but small trustworthy checkers.

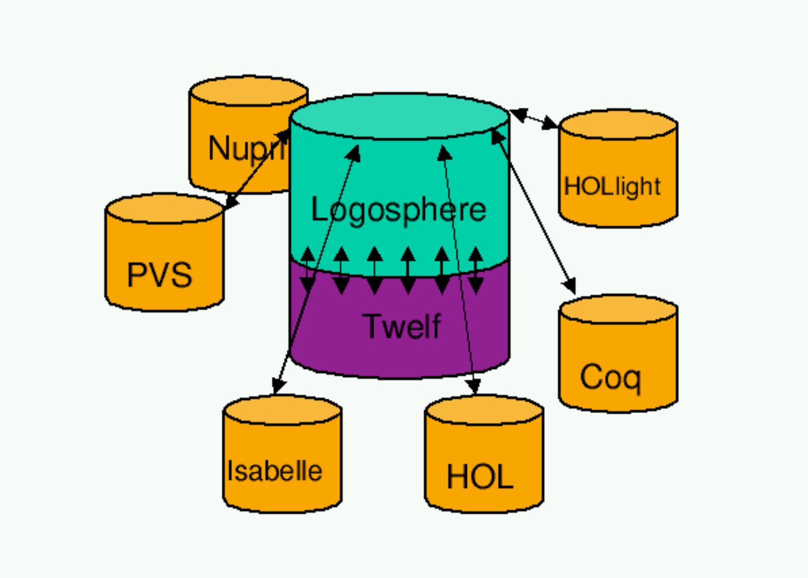
Proofs are important

> Although the *Annals* will publish Dr Hales's paper, Peter Sarnak, an editor of the *Annals*, whose own work does not involve the use of computers, says that the paper will be accompanied by an unusual disclaimer, stating that the computer programs accompanying the paper have not undergone peer review. There is a simple reason for that, Dr Sarnak says—it is impossible to find peers who are willing to review the computer code.

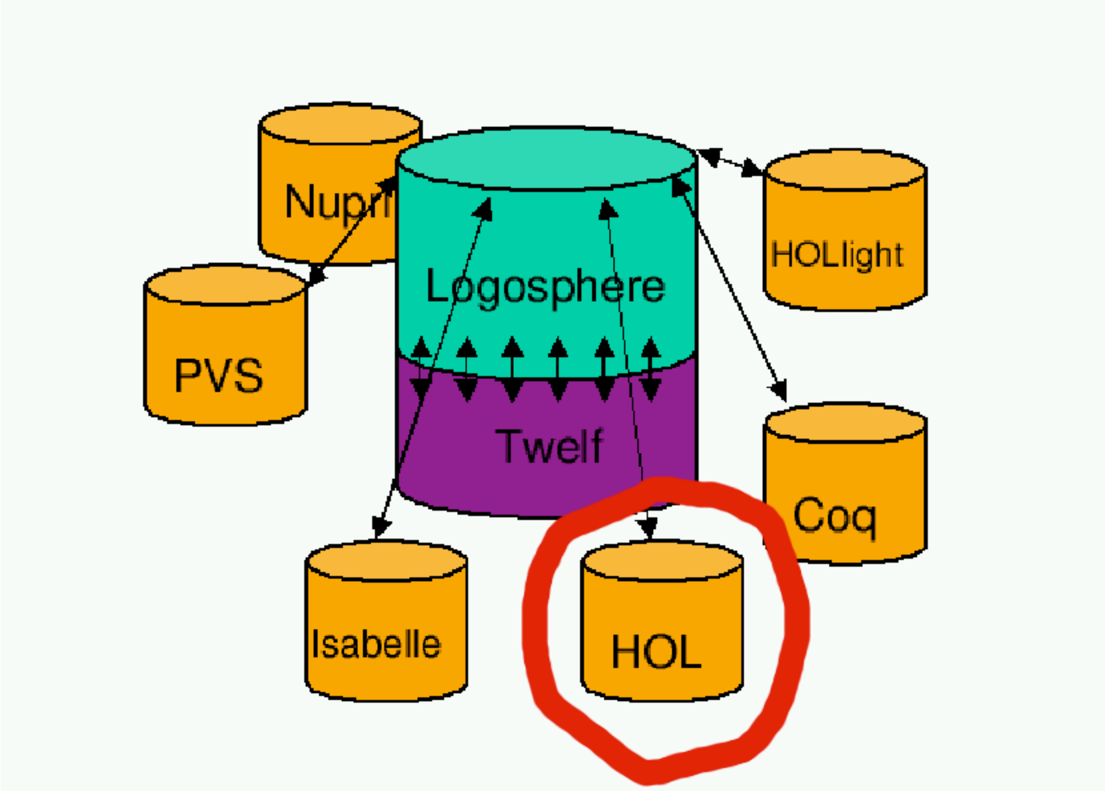
[The Economist, May 2005]

Rest of this talk

joint work with Mark-Oliver Stehr



- The logic HOL.
- Logical framework LF.
- Nuprl type theory.
- HOL - Nuprl connection.
- Open questions.


Nuprl
PVS
Logosphere
Twelf
HOLlight
Coq
Isabelle
HOL

HOL

- Higher-order logic [Church ‘40]
- HOL theorem prover [Gordon ‘85]
- Flavor: Isabelle/HOL [Paulson, Gordon ‘92]

Terms: $e_1, e_2 ::= x \;|{=}|{\supset}|\; e_1\ e_2 \mid \lambda x : \tau . e$

Types: $\tau \quad ::= o \mid \tau_1 \rightarrow \tau_2$

HOL (Typing)

Judgments: $e : \tau$

Rules: $$\frac{}{\supset : o \to o \to o}\,\textsf{imp} \qquad \frac{}{= : \tau \to \tau \to o}\,\textsf{eq}$$

$$\frac{e_1 : \tau_2 \to \tau_1 \qquad e_2 : \tau_2}{e_1\ e_2 : \tau_1}\,\textsf{app} \qquad \frac{\begin{array}{c}\overline{x : \tau_1}^{\,u} \\ \vdots \\ e : \tau_2\end{array}}{\lambda x : \tau_1 . e : \tau_1 \to \tau_2}\,\textsf{lam}^u$$

HOL (Proofs)

Judgments: $\vdash P$

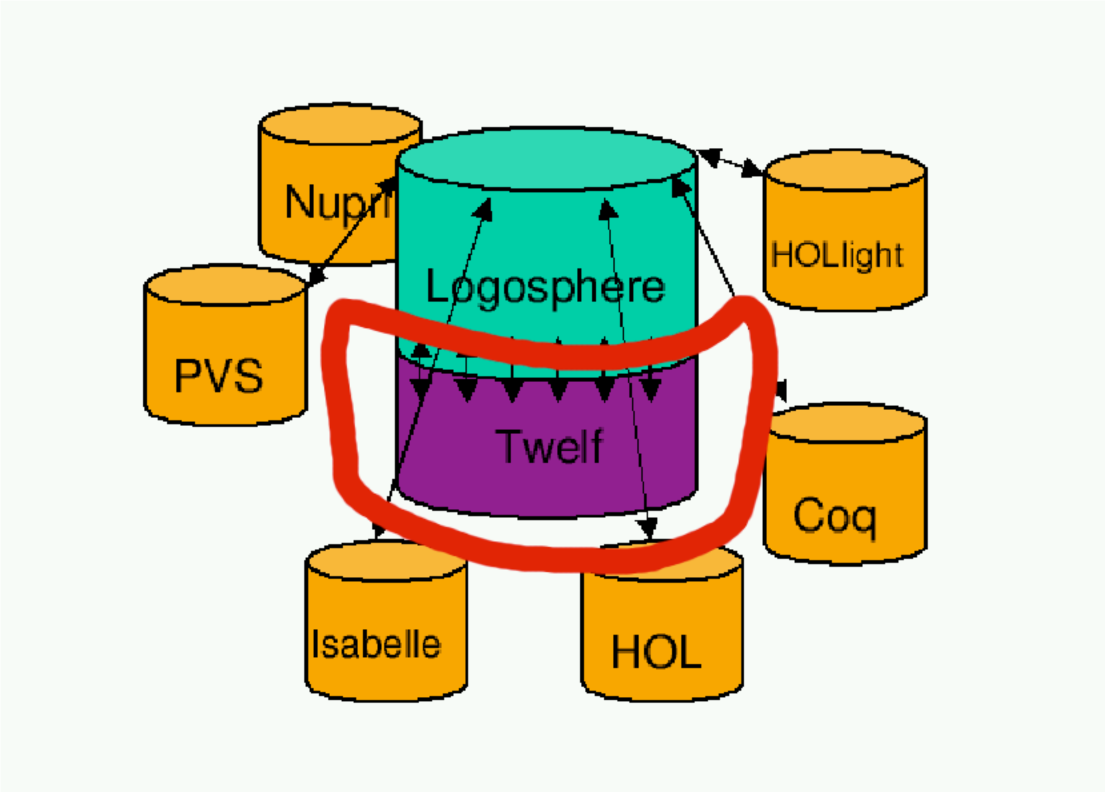
Rules:

$$\dfrac{\vdash P \qquad \vdash P \supset Q}{\vdash Q}\,\text{mp} \qquad \dfrac{\begin{array}{c}\overline{\vdash P}\\ \vdots \\ \vdash Q\end{array}}{\vdash P \supset Q}\,\text{disch}$$

$$\dfrac{}{\vdash P = P}\,\text{refl} \qquad \dfrac{}{\vdash (\lambda x : \tau . P)Q = [Q/x]P}\,\text{beta}$$

HOL (Booleans)

$$
\begin{array}{rcl}
\text{bool} & \hat{=} & o \\
\text{true} & \hat{=} & \lambda x : \text{bool}.x = \lambda x : \text{bool}.\, x \\
\text{all } P & \hat{=} & P = \lambda x : \tau.\, \text{true} \\
\text{false} & \hat{=} & \text{all } (\lambda x : \text{bool}.x) \\
\text{neg } P & \hat{=} & P \supset \text{false} \\
P \text{ and } Q & \hat{=} & \text{all } (\lambda R : \text{bool}.(P \supset Q \supset R) \supset R) \\
\text{the } P & & \text{(newly declared)} \\
\text{ex } P & \hat{=} & P\ (\text{the } P)
\end{array}
$$


Nuprl
Logosphere
HOLlight
PVS
Twelf
Coq
Isabelle
HOL

Twelf

- Logical framework LF. [Harper ‘93]
- Meta-language for deductive systems.
- Judgments-as-types, derivations-as-objects.
- Representation methodology.
  - Higher-order abstract syntax.
  - Captures variable binding.

Twelf (cont'd)

Representing numbers in BS (binary strings).

$$\ulcorner 79 \urcorner = *, 1, 0, 0, 1, 1, 1, 1$$

Representing judgments in LF.

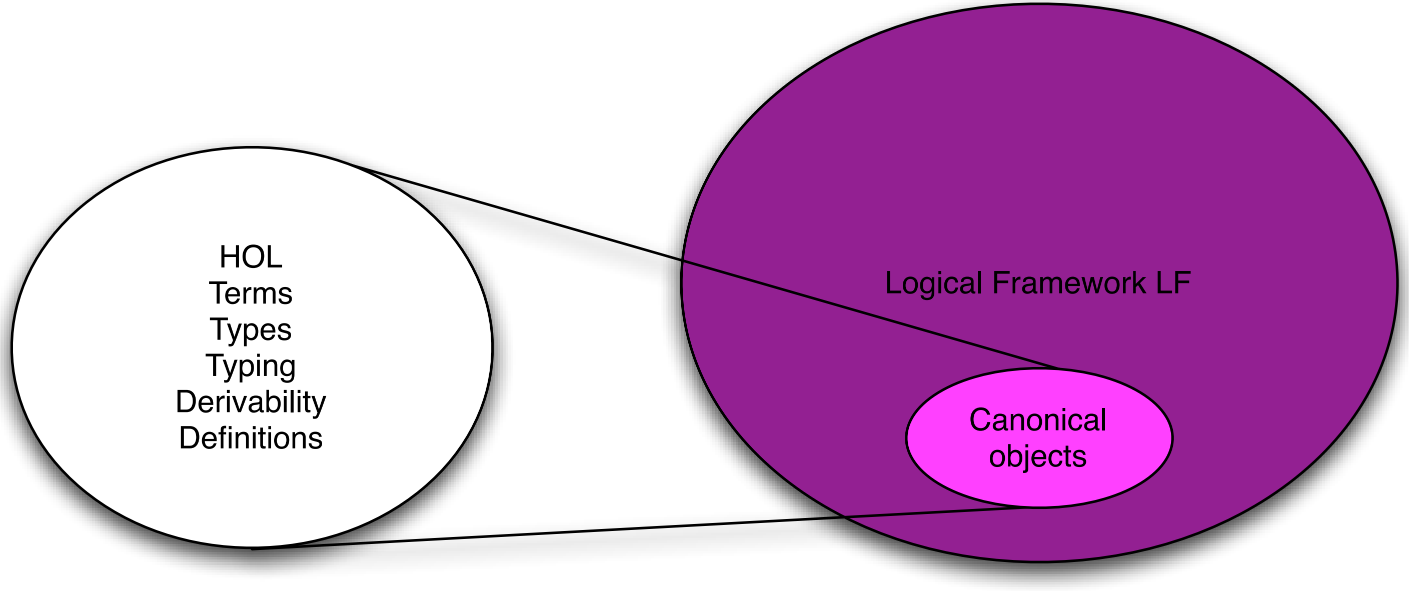
$$\ulcorner \vdash P \urcorner : \textsf{type} = \vdash \ulcorner P \urcorner$$

Representing derivations in LF.

$$\begin{array}{rll} \ulcorner \dfrac{\begin{array}{c}\mathcal{H}_1 \\ \vdash P \supset Q\end{array} \qquad \begin{array}{c}\mathcal{H}_2 \\ \vdash P\end{array}}{\vdash Q}\,\textsf{mp} \urcorner & : & \vdash \ulcorner Q \urcorner \\ & = & \textsf{mp}\ \ulcorner P \urcorner\ \ulcorner Q \urcorner\ \ulcorner \mathcal{H}_1 \urcorner\ \ulcorner \mathcal{H}_2 \urcorner \end{array}$$

Twelf's Strength

Adequacy Theorem: Every HOL derivation $\mathcal{D}$ of $P_1, \ldots, P_n \vdash Q$ can be represented in LF as a canonical object $\ulcorner \mathcal{D} \urcorner : \ulcorner Q \urcorner$ in context $u_1 :\vdash \ulcorner P_1 \urcorner, \ldots u_n :\vdash \ulcorner P_n \urcorner$.



Twelf (cont'd)

- Edinburgh Logical Framework.
- Signature declares object/type constants.
- Dependent types.

$$
\begin{array}{lcl}
K & ::= & \textsf{type} \mid \Pi x : A.\, K \mid A \rightarrow K \\
A & ::= & a \mid A\ M \mid \Pi x : A_1.\, A_2 \mid A_1 \rightarrow A_2 \\
M & ::= & c \mid \lambda x : A.\, M \mid M_1\ M_2
\end{array}
$$

[Pfenning, Schürmann '98]

Twelf Encoding of HOL

```
tp : type.                     %name tp (A B).
--> : tp -> tp -> tp.          %infix right 10 -->.
o  : tp.

tm : tp -> type.               %name tm (H G) (x y P Q R).
=>: tm (o --> o --> o).
== : tm (A --> A --> o).
@ : tm (A --> B) -> tm A -> tm B.     %infix left 15 @.
\ : (tm A -> tm B) -> tm (A --> B).
==> = [H:tm o] [G:tm o] => @ H @ G.     %infix right 13 ==>.
=== = [H:tm A] [G:tm A] == @ H @ G.     %infix left 14 ===.


|-    : tm o -> type.          %prefix 10 |-.  %name |- D u.
mp    : |- H -> |- H ==> G -> |- G.
disch : (|- H -> |- G) -> |- H ==> G.
refl  : |- H === H.
beta  : |- (\ H) @ G === (H G).
sub   : {G:tm A -> tm o} |- H1 === H2 -> |- G H1 -> |- G H2.
abs   : |- \ H === \ G
          <- ({x} |- H x === G x).
```

```
bool  = o.
true  : tm bool = (\ [x : tm bool] x) === (\ [x: tm bool] x).
all|  : tm ((A --> bool) --> bool)
      = \ [P:tm (A --> bool)] P === \ [x] true.
all   = [P] all| @ P.
false : tm bool = all (\ [P] P).
neg   : tm (bool --> bool) = \ [P:tm bool] P ==> false.
/|\   : tm (bool --> bool --> bool)
      = \ [P:tm bool] \ [Q:tm bool]
        all (\ [R:tm bool] (P ==> Q ==> R) ==> R).
/\    = [P] [Q] /|\ @ P @ Q.              %infix right 12 /\.
\|/   : tm (bool --> bool --> bool)
      = \ [P:tm bool] \ [Q:tm bool]
        all (\ [R:tm bool] (P ==> R) ==> (Q ==> R) ==> R).
\/    = [P] [Q] \|/ @ P @ Q.              %infix right 11 \/.
the|  : tm ((A --> bool) --> A).
the   = [P] the| @ P.
ex|   : tm ((A --> bool) --> bool)
      = \ [P:tm (A --> bool)] P @ (the (\ [x] P @ x)).
ex    = [P] ex| @ P.
```

Applications of Twelf

- Foundational Proof-Carrying Code. [Appel '99]
- Typed Assembly Language. [Crary '02]
- POPLmark Challenge. [UPenn ... '05]
- Logosphere Digital Library.

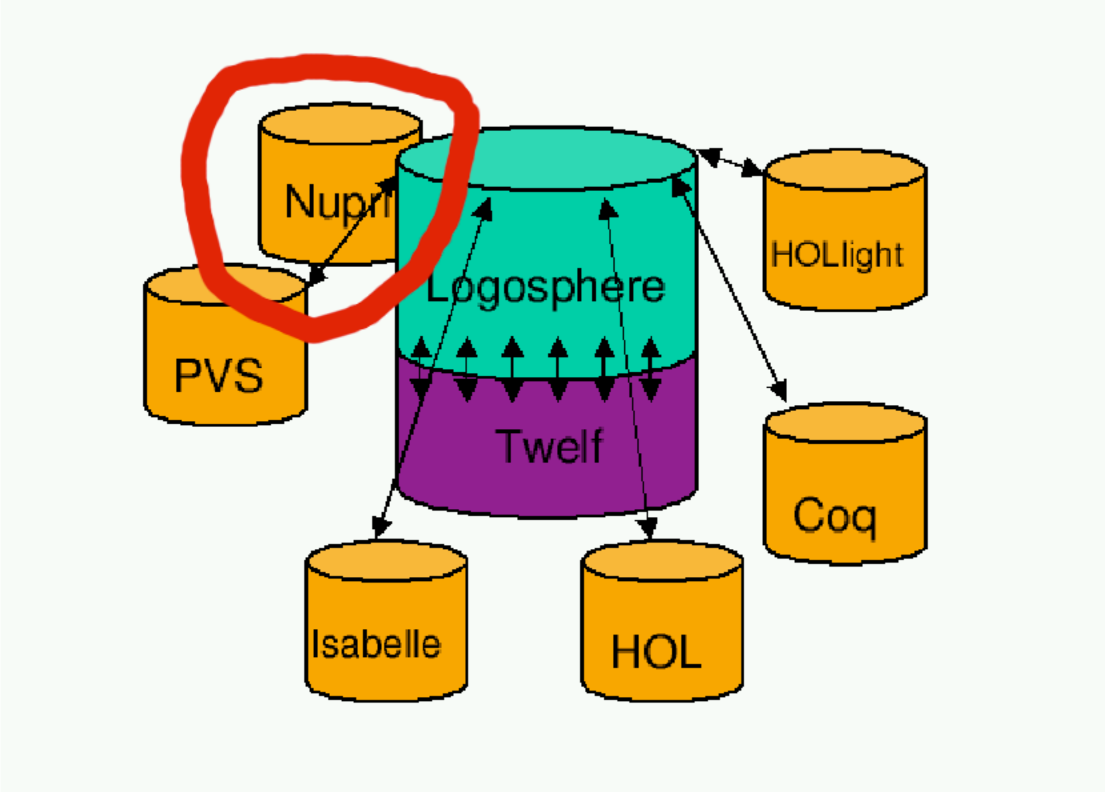
Alternative Logical Frameworks

Hereditary Harrop Formulas. [Isabelle, λProlog]

Substructural logical frameworks. [LLF, OLF]

Equational logic, rewrite logic. [Maude, Elan]

Constructive type theory. [AGDA, Coq, Nuprl]


Nuprl
PVS
Logosphere
Twelf
HOLlight
Coq
Isabelle
HOL

Nuprl

- Polymorphic extensional type theory.

  [Constable '86]

- Judgments establishes equality among terms.
- A type is *true* iff it is *inhabited*.
- Many applications.
  - Ensemble (TCP/IP stack). [Kreitz '04]
  - Protocol Verification. [Felty et al '98]

Nuprl Functions

$H \vdash S \rightarrow T \ \texttt{type}$ `funR`

$\quad H \vdash S \ \texttt{type}$

$\quad H \vdash T \ \texttt{type}$

$H \vdash \lambda x.e = \lambda x'.e' \in S \rightarrow T$ `lamR`

$\quad H, \ x{:}S \vdash e = e'[x/x'] \in T$

$\quad H \vdash S \ \texttt{type}$

$H \vdash f \ e = f' \ e' \in T$ `appR` $S \rightarrow T$

$\quad H \vdash f = f' \in S \rightarrow T$

$\quad H \vdash e = e' \in S$

$H \vdash (\lambda x.e) \ e' = e^* \in T$ `compute 1`

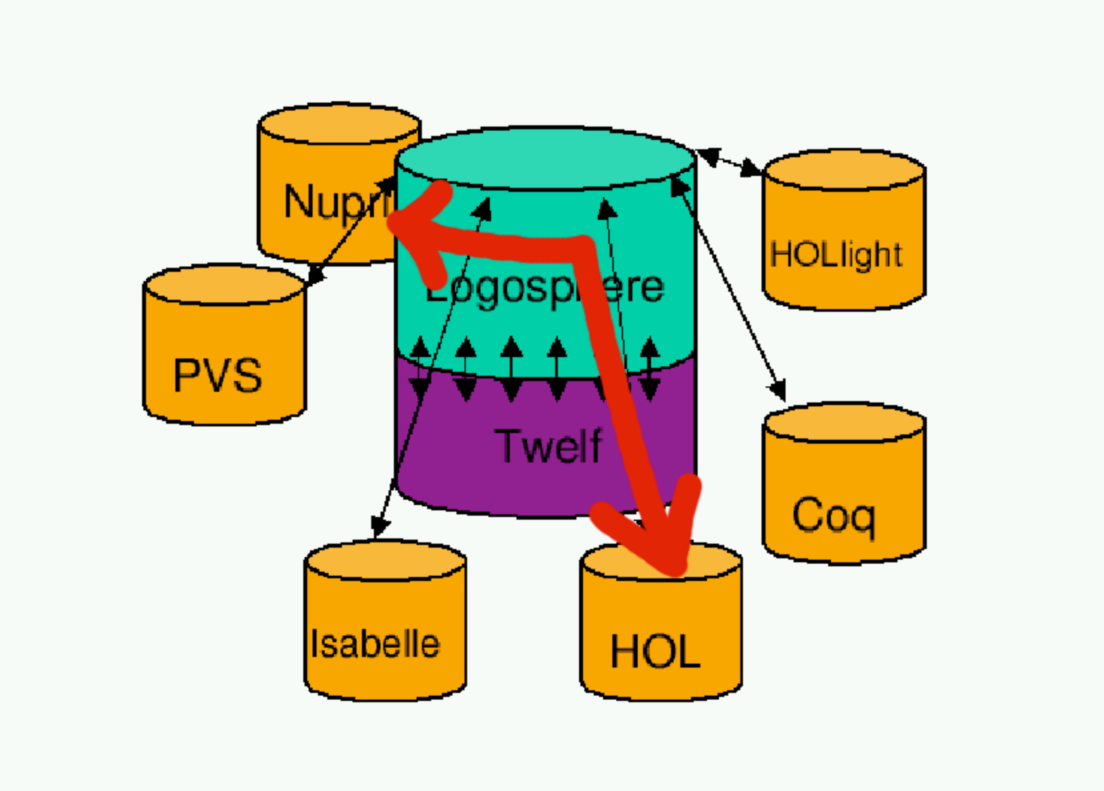
$\quad H \vdash e'[e/x] = e^* \in T$

[Courtesy Kreitz]

Note: $e{=}e \in T$ *is usually abbreviated by* $e \in T$

Nuprl (cont'd)

- Also: Dependent Sums, Functions, Quotient types, Universes, Substitution principles.
- Judgments, rules form deductive system.
- Variable binding and hypotheses modeled using higher-order abstract syntax.
- Implemented in Twelf.
- Details omitted here.


Nuprl
PVS
Logosphere
Twelf
HOLlight
Coq
Isabelle
HOL

Translation

- Original idea. [Howe ‘98]
- Syntactic argument. [Meseguer, Stehr ‘01]
- Implemented in Nuprl, replay of proof scripts. [Naumov ‘01]
- Formalized and executable specification.

  [Schürmann, Stehr ‘05]

Translation (cont'd)

- Booleans.

$$\begin{aligned} \textsf{boolean} &= \textsf{unit} + \textsf{unit} \\ \textsf{tt} &= \textsf{inl bullet} \\ \textsf{ff} &= \textsf{inr bullet} \\ \textsf{if}\ e\ e_1\ e_2 &= \textsf{decide}\ e\ (\lambda z.\, e_1)\ (\lambda z.\, e_2) \end{aligned}$$

- Propositions-as-types.

$$\begin{aligned} \textsf{BOOLEAN} &= \mathcal{U}_1 \\ \textsf{TRUE} &= \textsf{unit} \\ \textsf{FALSE} &= \textsf{void} \\ \textsf{ALL} &= \Pi \\ \textsf{=n=>} &= \Pi \end{aligned}$$

Howe's Observation

- Axiom of the excluded middle.

$$\frac{}{\vdash \textsf{inh}\ \#\ \Pi x : \textsf{BOOLEAN}.\ x + (x \longrightarrow \textsf{void})}\ \textsf{inhI}$$

- Lift Booleans to propositions.

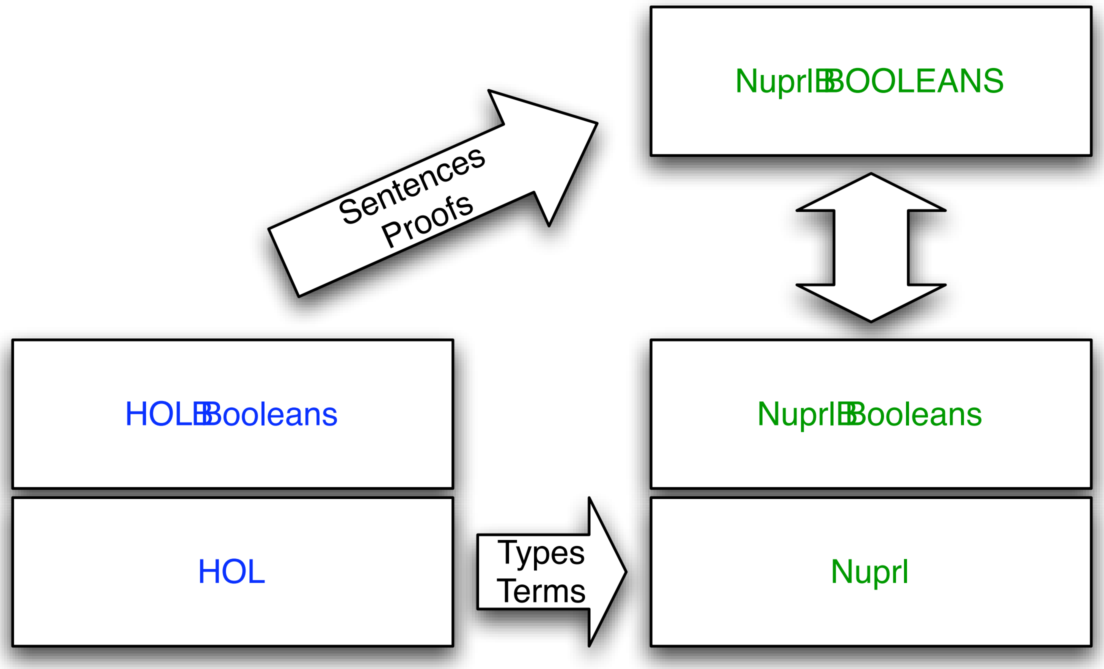
$$\uparrow (e) = \textsf{if}\ e\ \textsf{TRUE FALSE}.$$

- Lower propositions to Booleans.

$$\downarrow (P) = \textsf{decide}\ (\textsf{inh}\ P)\ (\lambda x.\,\textsf{tt})\ (\lambda y.\,\textsf{ff}).$$

- All important laws verifiable within Nuprl.

Translation (cont'd)



Translations-as-Relations

- Relations in Twelf.

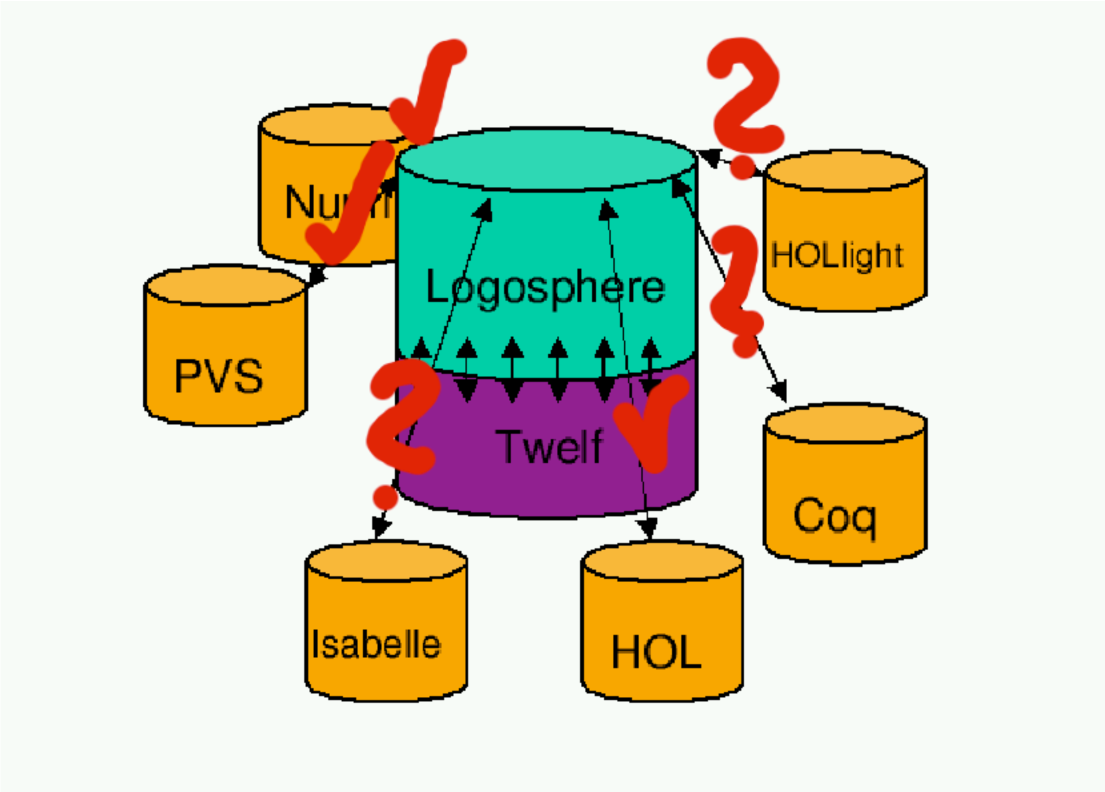
  trans-tp : tp $\longrightarrow$ nuprlterm $\longrightarrow$ type

  trans-tm : tm A $\longrightarrow$ nuprlterm $\longrightarrow$ type

  trans-sentence : tm o $\longrightarrow$ nuprlterm $\longrightarrow$ type

  trans-proof : $\vdash P$ $\longrightarrow$ trans-sentence $P\ T$ $\longrightarrow \vdash M\#T$ $\longrightarrow$ type

- Defining declarations omitted.
- Executable within Twelf.
- We can transform HOL proofs into Nuprl.


Nuprl
PVS
Logosphere
Twelf
HOLlight
Coq
Isabelle
HOL
✓
✓
?
?
?
✓

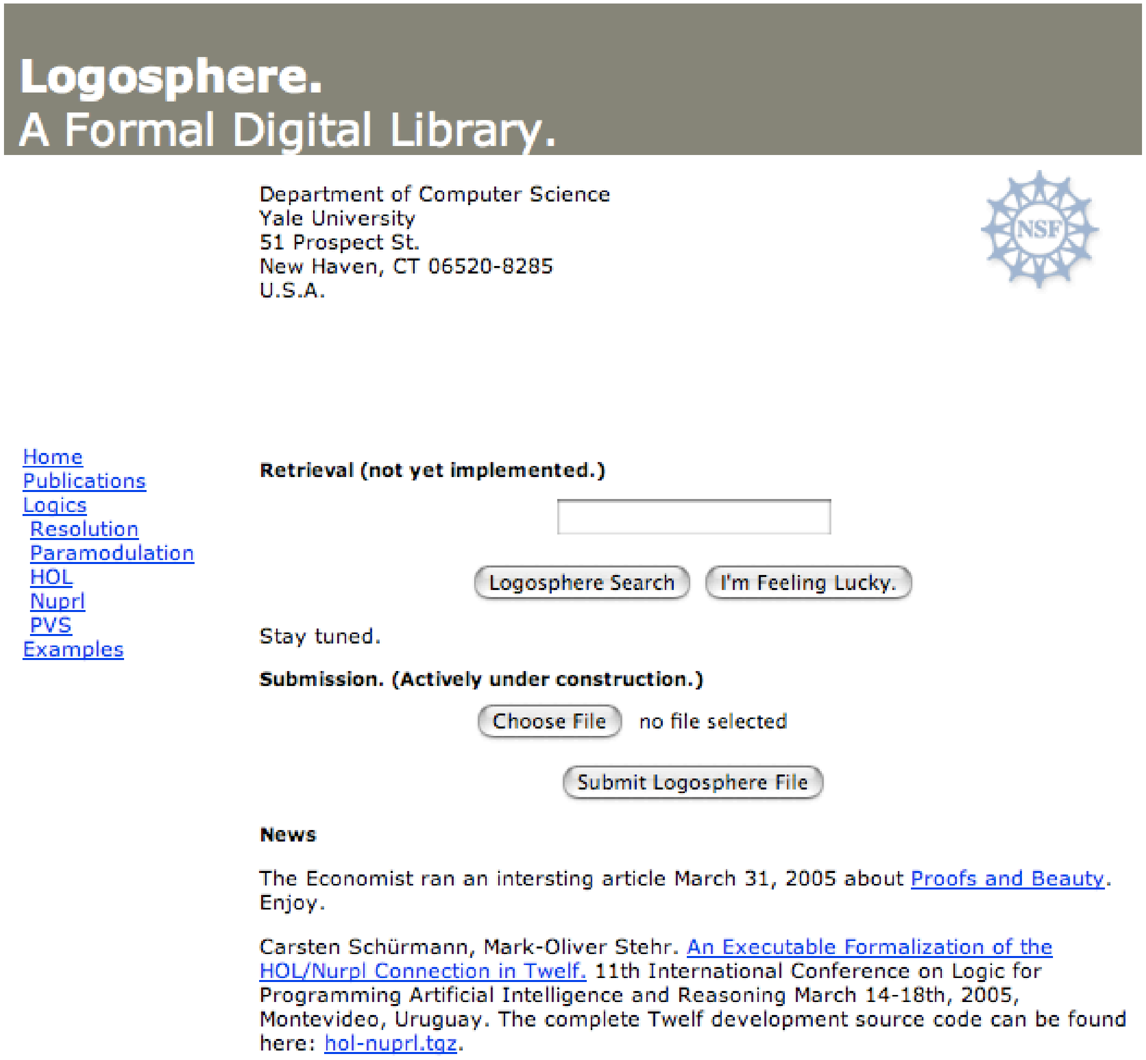
Conclusion

- There is a true need to share mathematical knowledge in form of proofs.
- Proof-theory: syntax instead semantics.
- Logical framework technology important.
- Proof conversion between HOL and Nuprl.
- For other systems (PVS), work in progress.

Open Questions

- Design of a query language.
- Design of the database.
- Shared domains, integers, natural numbers, complex numbers.
- Partial transformations.
- Connection to OMDOC. [Kohlhase 2001]
- Formalization of other logics.

www.logosphere.org



Logosphere.
A Formal Digital Library.

Department of Computer Science
Yale University
51 Prospect St.
New Haven, CT 06520-8285
U.S.A.

Retrieval (not yet implemented.)

Stay tuned.

Submission. (Actively under construction.)

News

The Economist ran an intersting article March 31, 2005 about Proofs and Beauty. Enjoy.

Carsten Schürmann, Mark-Oliver Stehr. An Executable Formalization of the HOL/Nurpl Connection in Twelf. 11th International Conference on Logic for Programming Artificial Intelligence and Reasoning March 14-18th, 2005, Montevideo, Uruguay. The complete Twelf development source code can be found here: hol-nuprl.tgz.

Thank you!