CS 671 Automated Reasoning

Introduction to NuPRL

1. **NuPRL Features**
2. **NuPRL Architecture**
3. **Interactive Theorem Proving in NuPRL**
   - Decomposition & Computation
   - Defining new constructs

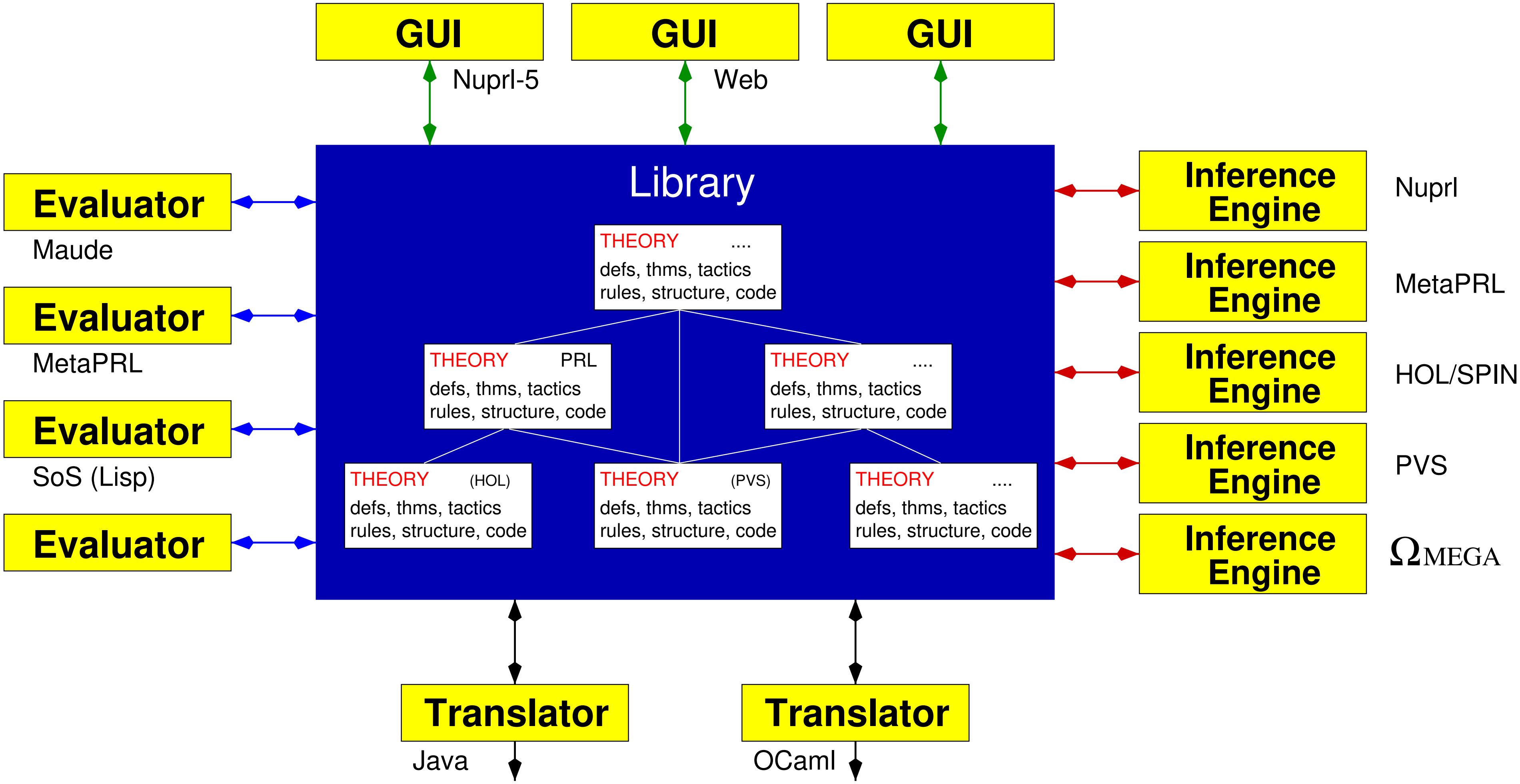
The Nuprl System

- **Beginnings in 1984**
  - Nuprl 1 (Symbolics): proof & program refinement in Type Theory
  - Book: *Implementing Mathematics ...* (1986)
  - Nuprl 2: Unix Version
- Nuprl 3: **Mathematical Problem Solving**
  - Machine proof for unsolved problems (Girard's paradox) (Howe 1987)
    (Higman's Lemma) (Murthy 1990)
- Nuprl 4: **System Verification and Optimization**
  - Verification of a logic synthesis tool (Aagaard & Leeser 1993)
  - Verification of the SCI cache coherency protocol (Howe 1996)
  - Optimization of the Ensemble group communication system (Kreitz, Hayden & Hickey 1999)
  - Verification of Ensemble protocol layers (Bickford 1999)

Nuprl 4 System Features

- **Interactive Proof Editor** $\rightsquigarrow$ readable proofs
- **Flexible definition mechanism** $\rightsquigarrow$ user-defined terms
- **Customizable Term Display** $\rightsquigarrow$ flexible notation
- **Structure Editor for Terms** $\rightsquigarrow$ no ambiguities
- **Tactics** $\rightsquigarrow$ user-defined inferences
- **Decision Procedures**
- **Proof objects, Program Extraction** $\rightsquigarrow$ program synthesis
- **Program Evaluation**
- **Library mechanism** $\rightsquigarrow$ user-theories
  - Large mathematical libraries
  - Large tactics collection
- **HTML output generator** $\rightsquigarrow$ web accessibility

Nuprl 5: An Open Logical Environment



Platform for Cooperating Reasoning Systems

Nuprl 5: Additional System Features

- **Collection of Cooperating Processes**
  – Centered around a common knowledge base
  – Refiners, interfaces, evaluators, etc. connect as independent processes
  – Processes can connect and disconnect at any time
- **Ability to Connect to External Systems**
  – MetaPRL, JProver, HOL, ...
- **Library Organized as Persistent Data Base**
  – Transaction model + Version control + Dependency tracking
- **Reflective System Structure**
  – System designed within the system's library $\leadsto$ customizable structure
- **Cooperating Inference Engines**
  – Asynchronous and distributed theorem proving
- **Multiple User Interfaces**
  – Structure editor, Web front end, ...

Refinement Rules for Natural Numbers

$H \vdash \mathbb{N}\ \texttt{type}$ `natR`

$H \vdash \texttt{0=0} \in \mathbb{N}$ `zeroR`

$H \vdash \texttt{suc}(e)\texttt{=suc}(e') \in \mathbb{N}$ `sucR`

$\quad H \vdash e\texttt{=}e' \in \mathbb{N}$

$H \vdash \texttt{ind}(e;\, base;\, n,x.\,up) = \texttt{ind}(e';\, base';\, n',x'.\,up') \in T$ `indR`

$\quad H \vdash e\texttt{=}e' \in \mathbb{N}$

$\quad H \vdash base\texttt{=}base' \in T$

$\quad H,\ n{:}\mathbb{N},\ x{:}T \vdash up\texttt{=}up'[n,x\,/\,n',x'] \in T$

$H_1,\ x{:}T,\ H_2 \vdash x\texttt{=}x \in T$ `hypotheses`

$H \vdash \texttt{ind}(\texttt{0};\, base;\, n,x.\,up) = e' \in T$ `compute 1`

$\quad H \vdash base = e' \in T$

$H \vdash \texttt{ind}(\texttt{suc}(e);\, base;\, n,x.\,up) = e' \in T$ `compute 1`

$\quad H \vdash up[e, \texttt{ind}(e;\, base;\, x.n,up)\,/\,n,x] = e' \in T$

Refinement Rules for Function Spaces

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

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

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

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

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

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

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

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

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

Refinement Rules for First-Order Logic

	left		right	
andL i	$H, A \wedge B, H' \vdash G$ $H, A, B, H' \vdash G$	$H \vdash A \wedge B$ $H \vdash A$ $H \vdash B$	andR
orL i	$H, A \vee B, H' \vdash G$ $H, A, H' \vdash G$ $H, B, H' \vdash G$	$H \vdash A \vee B$ $H \vdash A$ $H \vdash A \vee B$ $H \vdash B$	orR1 orR2
impL i	$H, A \Rightarrow B, H' \vdash G$ $H, A \Rightarrow B, H' \vdash A$ $H, H', B \vdash G$	$H \vdash A \Rightarrow B$ $H, A \vdash B$	impR
notL i	$H, \neg A, H' \vdash G$ $H, \neg A, H' \vdash A$	$H \vdash \neg A$ $H, A \vdash \texttt{false}$	notR
exL i	$H, \exists x{:}T.B, H' \vdash G$ $H, x{:}T, B, H' \vdash G$	$H \vdash \exists x{:}T.B$ $H \vdash B[t/x]$	exR t
allL i t	$H, \forall x{:}T.B, H' \vdash G$ $H, \forall x{:}T.B, B[t/x], H' \vdash G$	$H \vdash \forall x{:}T.B$ $H, x{:}T \vdash B$	allR

Note: an unlabelled hypotheses A is an abbreviation for `%:A`