The Nuprl Open Logical Environment

Stuart Allen, Robert Constable, Richard Eaton, Christoph Kreitz, Lori Lorigo

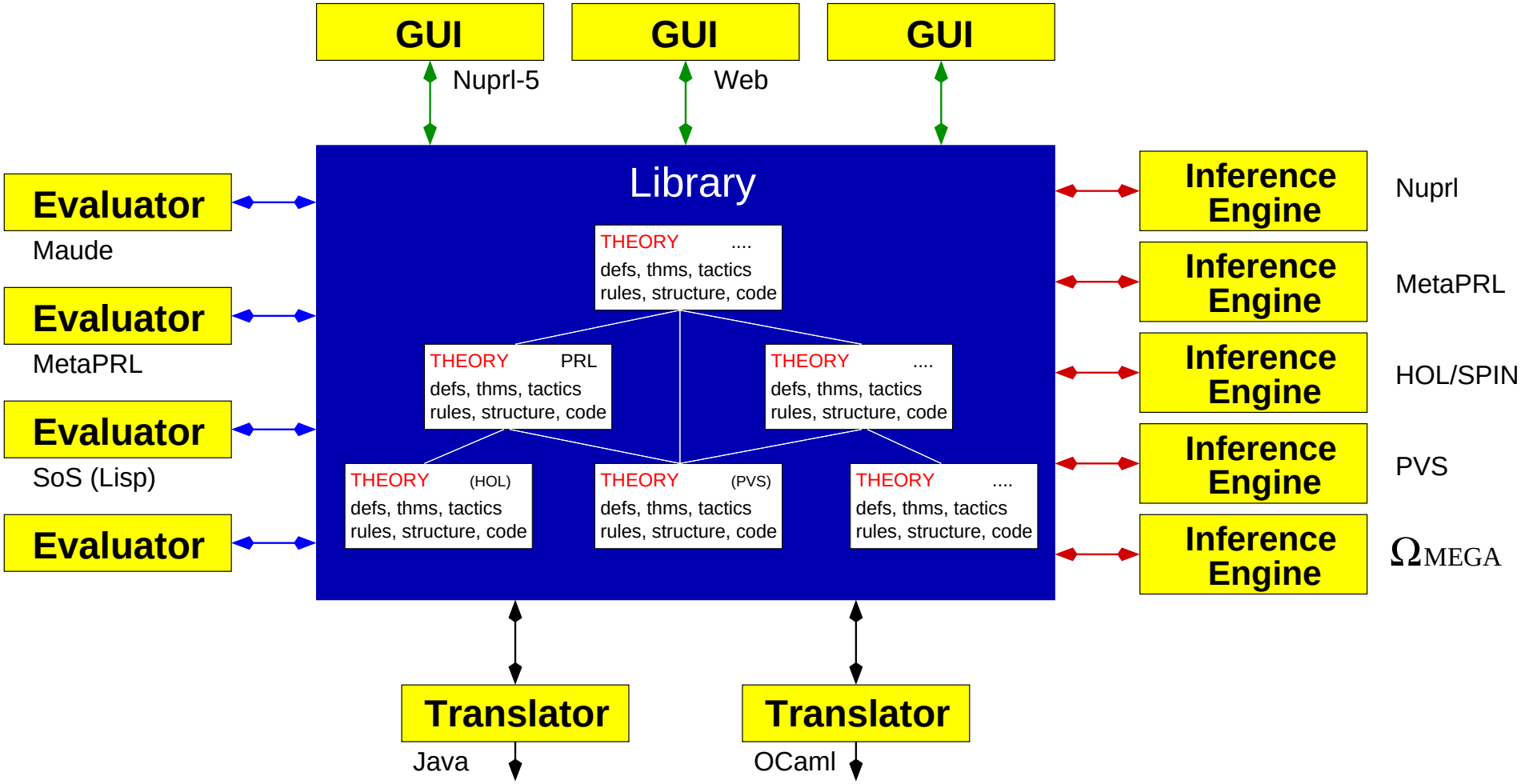
Department of Computer Science, Cornell University

Ithaca, NY 14853

Nuprl History

- **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 5: Open Distributed Architecture**

The Nuprl Architecture



Key Features I

- **Collection of Cooperating Processes**
  - Centered around a common knowledge base
  - Refiners, editors, evaluators, etc. connect as independent processes
  - Several users can work in parallel on the same formal theory
  - A user can start several refiners in parallel
- **Ability to Connect to External Systems**
  - MetaPRL (modularized PRL, multiple logics) (Hickey & Nogin, 1999)
  - Jprover (a matrix-based intuitionistic theorem prover) (Schmitt & Lorigo, 2000)
  - HOL (classical higher order logic) (Howe, 1998, Stehr & Naumov, 1999)
  - Mathematica (Benzinger, 2000)

  ⋮
- **Library Organized as Persistent Data Base**
  - Transaction model (preserves data even in case of crashes)
  - Version control mechanism
  - Dependency tracking

Key Features II

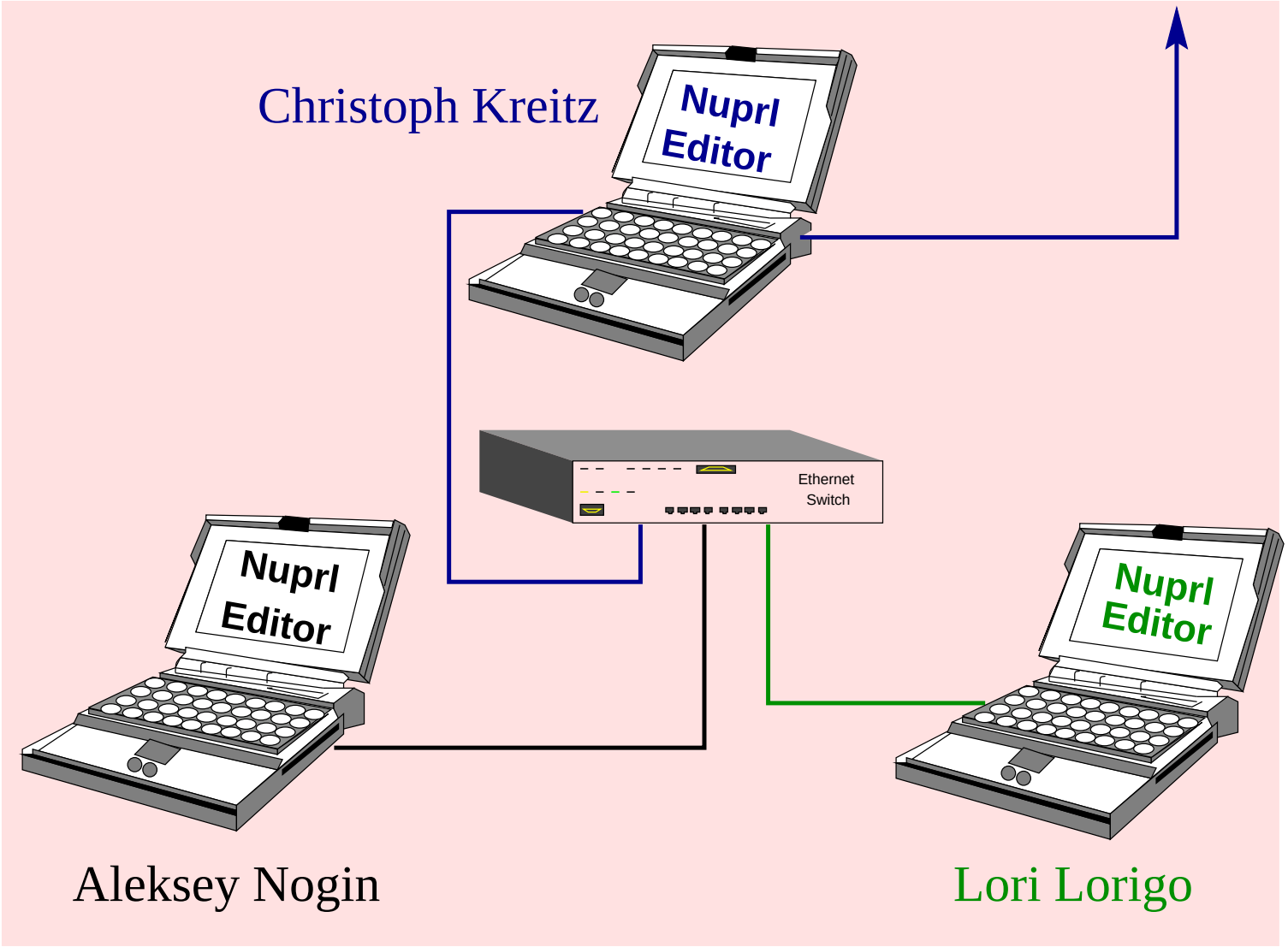
- **Reflective System Structure**
  - System designed within the system's library
  - Customizable structure
- **Cooperating Inference Engines**
  - Asynchronous refinement
  - Distributed theorem proving
- **Multiple User Interfaces**
  - Collaborative proving while using favorite editor
  - Web front end will allow external users to browse the library
- **Nuprl 4 Capabilities**
  - Readable proofs
  - Structure editor
  - Large tactics collection
  - Definition mechanism
  - Customizable term display
  - HTML output generator

`http://www.cs.cornell.edu/Info/Projects/NuPrl/nuprl.html`

Demonstrations

- **Nuprl 5 Basics** (Christoph Kreitz, Lori Lorigo)
  - How to use the new system
- **Cooperative Theorem Proving** **(McConomy Auditorium TODAY)**
  - Multiple users work on the same theorem at the same time
- **Application to Software** (Christoph Kreitz)
  - Optimization of the Ensemble group communication system
  - Automatic complexity analysis (Ralph Benzinger)
- **MetaPRL** (Alexey Nogin)
  - Inferences at 100+ times the speed of ordinary tactic provers

Cooperative Theorem Proving – Setup



- 3 laptops connected via ethernet, one connected to projector
- 1 Nuprl library process, 3 Nuprl user interfaces
- 3 users work simultaneously on the integer square root problem