KAT-ML
An Interactive Theorem Prover for Kleene Algebra w/Tests

Kamal Aboul-Hosn
Dexter Kozen
Cornell University

Goals

- Interactively develop proofs in KAT
- Manage proofs and theorems in a reusable fashion
- Formally verify proof already in the literature

System Description

- Written in Standard ML (with SML Tk)
- Works on unix-based OSes, Windows
- Fundamental Commands:
  - ***Publish***: Create a new theorem (without a proof!)
  - ***Cite***: Incorporates previous proofs into current proof

Representing Proofs

- A term abstracted over
  - Term variables `p,q,r`... and boolean variables `A,B,C`.... in the theorem
  - Proof variables $\texttt{P}_0, \texttt{P}_1$,..., representing proofs of premises
  - Task variables $\texttt{T}_0, \texttt{T}_1$,... for incomplete tasks

Representing Proofs

$$\forall x_1 \ldots \forall x_m \quad \phi_1 \rightarrow \phi_2 \rightarrow \cdots \rightarrow \phi_n \rightarrow \psi$$

Proof term is well-typed

$$\lambda x_1 \ldots \lambda x_m . \lambda P_1 \ldots \lambda P_n . (T P_1 \cdots P_n)$$

By Curry-Howard isomorphism, the type of term is the proof

A Sample Proof

- From Tuesday: All of the following are equivalent

$$\begin{aligned} Up &= UpV \\ Up\overline{V} &= 0 \\ Up &\leq pV \end{aligned}$$

Verified Proofs

- Hoare While rule:

$$\frac{\{B;C\}p\{C\}}{\{C\}\text{while } B \text{ do } p\{C;\overline{B}\}}$$

- Need to show:

$$B;C;p = B;C;p;C \rightarrow C;(B;p)^*;\overline{B} = C;(B;p)^*;\overline{B};C;\overline{B}$$

Future Additions

- First-order constructs
  - Schematic part almost complete
- "Adaptive" heuristics
- Readable printing of proofs
- Online database of proofs