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 $P_0, P_1, ...$, representing proofs of premises
- Task variables $T_0, T_1, ...$ for incomplete tasks
Representing Proofs

∀x_1 \ldots ∀x_m \quad φ_1 \rightarrow φ_2 \rightarrow \cdots \rightarrow φ_n \rightarrow ψ

Proof term is well-typed

λx_1 \ldots λx_m.λP_1 \ldots λP_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

\[ U_p = U_p V \]
\[ U_p \overline{V} = 0 \]
\[ U_p \leq p V \]
Verified Proofs

- **Hoare While rule:**

\[
\begin{align*}
\{B; C\}p\{C\} \\
\{C\} \text{while } B \text{ do } p\{C; \overline{B}\}
\end{align*}
\]

- **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