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

Kamal Aboul-Hosn
Dexter Kozen
Kleene Algebra (KA)

- The algebra of regular expressions

pq + qp

pq*
K is an idempotent semiring under $+, \cdot, 0, 1$

\[
(p + q) + r = p + (q + r) \quad (1) \quad (pq)r = p(qr) \quad (2)
\]
\[
p + q = q + p \quad (3) \quad p1 = 1p = p \quad (4)
\]
\[
p + 0 = p + p = p \quad (5) \quad 0p = p0 = 0 \quad (6)
\]
\[
p(q + r) = pq + pr \quad (7) \quad (p + q)r = pr + qr \quad (8)
\]
\[
1 + pp^* \leq p^* \quad (9) \quad q + pr \leq r \quad \rightarrow p^*q \leq r \quad (10)
\]
\[
1 + p^*p \leq p^* \quad (11) \quad q + rp \leq r \quad \rightarrow qp^* \leq r \quad (12)
\]

- $p^*q = \text{least } x \text{ such that } q + px \leq x$
- $qp^* = \text{least } x \text{ such that } q + xp \leq x$

\[x \leq y \iff x + y = y\]
Standard Interpretation

Regular sets over $\Sigma$

$A+B = A \cup B$

$AB = \{xy \mid x \in A, y \in B\}$

$A^* = \bigcup_{n \geq 0} A^n = A^0 \cup A^1 \cup A^2 \cup \ldots$

$1 = \{\varepsilon\}$

$0 = \emptyset$

$p \in \Sigma$ interpreted as $\{p\}$
Useful Properties

\[
\begin{align*}
1 + pp^* &= 1 + p^*p = p^* \\
p^*p^* &= p** = p^* \\
(pq)^*p &= p(qp)^* \quad \text{sliding} \\
(p^*q)^*p^* &= (p + q)^* \quad \text{denesting} \\
px = xp &\Rightarrow p^*x = xq^* \quad \text{bisimulation} \\
qp = 0 &\Rightarrow (p + q)^* = p^*q^*
\end{align*}
\]
Applications of KA

- Automata and regular expressions
- Relational algebra
- Design and analysis of algorithms
  - shortest paths
  - connectivity
  - computational geometry
Kleene Algebra w/Tests (KAT)

\((K, B, +, \cdot, *, -, 0, 1)\)

- \((K, +, \cdot, *, 0, 1)\) is a Kleene algebra
- \((B, +, \cdot, -, 0, 1)\) is a Boolean algebra

\(B \subseteq K\)

- \(p, q, r\) range over \(K\)
- \(A, B, C\) range over \(B\)
KAT-ML

- Written in Standard ML (with SML Tk)
- Works on unix-based OSes, Windows
- Goals:
  - Interactively develop proofs in KAT
  - Manage proofs and theorems in a reusable fashion
  - Formally verify proof already in the literature
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

\[ \forall x_1 \ldots \forall x_m \phi_1 \rightarrow \phi_2 \rightarrow \cdots \rightarrow \phi_n \rightarrow \psi \]

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

- All of the following are equivalent

\[
U_p = U_p V \\
U_p V = 0 \\
U_p \leq pV
\]
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:

\[
B; C; p = B; C; p; C \rightarrow C; (B; p)^*; \overline{B} = C; (B; p)^*; \overline{B}; C; \overline{B}
\]
Modeling Programs

[Fischer + Ladner 74]

\[ x := e \equiv a \]
\[ e < f \equiv A \]
\[ \text{if } B \text{ then } p \text{ else } q \equiv Bp + \overline{B}q \]
\[ \text{while } B \text{ do } p \equiv (Bp)^*\overline{B} \]
Schematic KAT

\[ x := s; \ y := t \quad = \quad y := t[x/s]; \ x := s \quad y \notin FV(s) \]
\[ x := s; \ y := t \quad = \quad x := s; \ y := t[x/s] \quad x \notin FV(s) \]
\[ x := s; \ x := t \quad = \quad x := t[x/s] \]
\[ \varphi[x/t]; \ x := t \quad = \quad x := t; \varphi \]
\[ x := x \quad = \quad 1 \]
Future Additions

- First-order constructs
  - Add interpreted level
- “Adaptive” heuristics
- Readable printing of proofs
- Online database of proofs
Download

http://www5.cs.cornell.edu/~kamal/kat