Introduction to Kleene Algebra	**Lecture 23**
CS786 Spring 2002	**Thursday, April 18, 2002**

Completeness of KAT for the Hoare Theory of Relational Models

Theorem **??** of Lecture **??** says that for any proof rule of PHL, or more generally, for any rule of the form

$$\frac{\{b_1\}\,p_1\,\{c_1\},\ \ldots,\ \{b_n\}\,p_n\,\{c_n\}}{\{b\}\,p\,\{c\}}$$

derivable in PHL, the corresponding equational implication (universal Horn formula)

$$b_1p_1\overline{c}_1 = 0 \wedge \cdots \wedge b_np_n\overline{c}_n = 0 \quad\to\quad bp\overline{c} = 0 \tag{1}$$

is a theorem of KAT. In this lecture we strengthen this result to show (Corollary 0.2) that *all* universal Horn formulas of the form

$$r_1 = 0 \wedge \cdots \wedge r_n = 0 \quad\to\quad p = q \tag{2}$$

that are relationally valid (true in all relational models) are theorems of KAT; in other words, KAT is complete for universal Horn formulas of the form (2) over relational interpretations. This result subsumes Theorem **??** of Lecture **??**, since the Hoare rules are relationally valid. Corollary 0.2 is trivially false for PHL; for example, the rule

$$\frac{\{c\}\ \textbf{if}\ b\ \textbf{then}\ p\ \textbf{else}\ p\ \{c\}}{\{c\}\,p\,\{c\}}$$

is not derivable, since the Hoare rules only increase the length of programs. The results of this lecture are from [1].

To prove this result we generalize Cohen's theorem (Lecture **??**) in two ways: to handle tests and to show completeness over relational models. The deductive completeness of KAT over relationally valid formulas of the form (2) will follow as a corollary.

Let $\mathsf{RExp}_{\mathsf{P},\mathsf{B}}$ denote the set of terms of the language of KAT over primitive propositions $\mathsf{P} = \{p_1, \ldots, p_m\}$ and primitive tests $\mathsf{B} = \{b_1, \ldots, b_k\}$. Let $r_1, \ldots, r_n, p, q \in \mathsf{RExp}_{\mathsf{P},\mathsf{B}}$. Let u be the *universal expression* $u = (p_1 + \cdots + p_m)^*$ and let $r = \sum_i r_i$. The formula (2) is equivalent to $r = 0 \to p = q$.

Recall the definition of the algebra $\mathsf{Reg}_{\mathsf{P},\mathsf{B}}$ of regular sets of guarded strings over P, B and the standard interpretation $G : \mathsf{RExp}_{\mathsf{P},\mathsf{B}} \to \mathsf{Reg}_{\mathsf{P},\mathsf{B}}$ from Lecture **??**. We showed in

Lecture **??** that $\mathsf{Reg}_{\mathsf{P},\mathsf{B}}$ is the free KAT on generators P,B in the sense that for any terms $s,t \in \mathsf{RExp}_{\mathsf{P},\mathsf{B}}$,

$$\vDash s = t \quad \Leftrightarrow \quad G(s) = G(t). \tag{3}$$

Note that $G(u)$ is the set of all guarded strings over P,B.

Theorem 0.1 *The following four conditions are equivalent:*

(i) $\mathsf{KAT} \vDash r = 0 \to p = q$

(ii) $\mathsf{KAT}^* \vDash r = 0 \to p = q$

(iii) $\mathsf{REL} \vDash r = 0 \to p = q$

(iv) $\vDash\ p + uru = q + uru$.

It does not matter whether (iv) is preceded by KAT, KAT^*, or REL, since the equational theories of these classes coincide, as shown in Lecture **??**.

Proof. Since $\mathsf{REL} \subseteq \mathsf{KAT}^* \subseteq \mathsf{KAT}$, the implications (i) $\to$ (ii) $\to$ (iii) hold trivially. Also, it is clear that

$$\mathsf{KAT} \ \vDash \ p + uru = q + uru \to (r = 0 \to p = q),$$

therefore (iv) $\to$ (i) as well. It thus remains to show that (iii) $\to$ (iv). Writing equations as pairs of inequalities, it suffices to show

$$\mathsf{REL} \vDash r = 0 \to p \le q \quad \Rightarrow \quad \vDash p \le q + uru. \tag{4}$$

To show (4), we construct a relational model R on states $G(u) - G(uru)$. Note that if $x, y, z \in G(u)$ such that $xyz \in G(u) - G(uru)$, then $y \in G(u) - G(uru)$. If $G(u) \subseteq G(uru)$, then we are done, since in that case $G(p) \subseteq G(u) \subseteq G(uru)$ and the right-hand side of (4) follows immediately from (3). Similarly, if $G(1) \subseteq G(uru)$, then $G(u) \subseteq G(uuru) \subseteq G(uru)$ and the same argument applies. We can therefore assume without loss of generality that both $G(u) - G(uru)$ and $G(1) - G(uru)$ are nonempty.

The atomic symbols are interpreted in R as follows:

$$\begin{aligned} R(a) &\stackrel{\text{def}}{=} \{(x, xa\beta) \mid xa\beta \in G(u) - G(uru)\}, \quad a \in \mathsf{P} \\ R(b) &\stackrel{\text{def}}{=} \{(x, x) \mid x = x\beta \in G(u) - G(uru),\ \beta \le b\}, \quad b \in \mathsf{B}. \end{aligned}$$

The interpretations of compound expressions are defined inductively in the standard way for relational models.

We now show that for any $t \in \mathsf{RExp}_{\mathsf{P,B}}$,

$$R(t) = \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(t)\} \tag{5}$$

by induction on the structure of t. For primitive programs a and tests b,

$$\begin{aligned}
R(a) &= \{(x,xa\beta) \mid xa\beta \in G(u) - G(uru)\} \\
&= \{(x,x\alpha a\beta) \mid x\alpha a\beta \in G(u) - G(uru)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(a)\}, \\
R(b) &= \{(x,x) \mid x = x\beta \in G(u) - G(uru),\ \beta \in G(b)\} \\
&= \{(x,x\beta) \mid x\beta \in G(u) - G(uru),\ \beta \in G(b)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(b)\}.
\end{aligned}$$

For the constants 0 and 1, we have

$$\begin{aligned}
R(0) &= \varnothing \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(0)\}, \\
R(1) &= \{(x,x) \mid x \in G(u) - G(uru)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(1)\}.
\end{aligned}$$

For compound expressions,

$$\begin{aligned}
R(s+t) &= R(s) \cup R(t) \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(s)\} \\
&\quad \cup \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(t)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(s) \cup G(t)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(s+t)\}, \\
R(st) &= R(s) \circ R(t) \\
&= \{(x,xz) \mid xz \in G(u) - G(uru),\ z \in G(s)\} \\
&\quad \circ \{(y,yw) \mid yw \in G(u) - G(uru),\ w \in G(t)\} \\
&= \{(x,xzw) \mid xzw \in G(u) - G(uru),\ z \in G(s),\ w \in G(t)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(st)\}, \\
R(t^*) &= \bigcup_n R(t^n) \\
&= \bigcup_n \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(t^n)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in \bigcup_n G(t^n)\} \\
&= \{(x,xy) \mid xy \in G(u) - G(uru),\ y \in G(t^*)\}.
\end{aligned}$$

We now show (4). Suppose the left-hand side holds. By (5),

$$R(r) \quad \stackrel{\text{def}}{=} \quad \{(x, xy) \mid xy \in G(u) - G(uru),\ y \in G(r)\} \quad = \quad \varnothing.$$

By the left-hand side of (4), $R(p) \subseteq R(q)$. In particular, for any $x \in G(p) - G(uru)$, $(\mathsf{first}\, x, x) \in R(p)$, therefore $(\mathsf{first}\, x, x) \in R(q)$ as well, thus $x \in G(q) - G(uru)$. But this says $G(p) - G(uru) = G(q) - G(uru)$, thus $G(p) \subseteq G(q) \cup G(uru) = G(q + uru)$. It follows from (3) that the right-hand side of (4) holds. □

Corollary 0.2 KAT *is deductively complete for formulas of the form* (2) *over relational models.*

Proof. If the formula (2) is valid over relational models, then by Theorem 0.1, (iv) holds. Since KAT is complete for valid equations,

$$\mathsf{KAT} \quad \vdash \quad p + uru = q + uru.$$

But clearly

$$\mathsf{KAT} \quad \vdash \quad p + uru = q + uru \wedge r = 0 \to p = q,$$

therefore

$$\mathsf{KAT} \quad \vdash \quad r = 0 \to p = q.$$

□

References

[1] Dexter Kozen. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic*, 1(1):60–76, July 2000.