Introduction to Kleene Algebra	**Lecture 11**
CS786 Spring 2002	**Thursday, February 28, 2002**

Equational Implications

In many applications of Kleene algebra, one needs to reason in the presence of extra conditions. For example, the fact that two atomic actions cannot affect each other and can be done in either order might be represented by a commutativity condition $pq = qp$. The fact that an atomic program p does not affect the truth value of a test b might be represented similarly as $pb = bp$. It is therefore of interest to study universally quantified equational implications or *Horn formulas*, which are formulas of the form

$$s_1 = t_1 \wedge \cdots \wedge s_n = t_n \quad \rightarrow \quad s = t.$$

In general, the universal Horn theory is much more complex than the equational theory. For unrestricted premises, the universal Horn theory of Kleene algebras is Σ_1^0-complete (r.e. complete) and that of star-continuous Kleene algebras is Π_1^1-complete [2].

However, there is an interesting and useful subclass of Horn formulas in which the problem is no less tractable than the equational theory and that actually arises quite often in practice. The subclass consists of Horn formulas in which all premises are of the form $r = 0$. For example, the premise $pb = bp$ mentioned above is equivalent (under Boolean algebra axioms for tests b) to $bp\bar{b} + \bar{b}pb = 0$. Formulas of this form are sufficient to encode Hoare logic, a classical logic for program correctness. We call Horn formulas satisfying this restriction *Hoare formulas* after C. A. R. Hoare, the inventor of Hoare logic. Thus a *Hoare formula* is a Horn formula of the form

$$r_1 = 0 \wedge \cdots \wedge r_n = 0 \quad \rightarrow \quad s = t. \tag{1}$$

In this lecture we prove a result of Cohen [1] that shows how to eliminate premises of the form $r = 0$. Specifically, we show that any Hoare formula reduces efficiently to a single equation that is valid iff the original Hoare formula was. The Hoare formula and the resulting equation are not equivalent under all interpretations, but one is valid iff the other is.

Let $p, q, r \in \mathsf{RExp}_\Sigma$. Let u be the *universal expression* $(a_1 + \cdots + a_m)^*$, where $\Sigma = \{a_1, \ldots, a_m\}$. Under the standard interpretation R_Σ in Reg_Σ, the term u represents the set of all strings over Σ. It is not difficult to show that for any $x \in \mathsf{RExp}_\Sigma$, $x \leq u$ is a theorem of Kleene algebra.

Let us write $\mathsf{KA} \vDash \varphi$ or $\mathsf{KA}^* \vDash \varphi$ to indicate that a Horn formula φ is a theorem of Kleene algebra or star-continuous Kleene algebra, respectively. If φ is an equation, these two notions coincide, in which case we write $\vDash \varphi$.

First we observe that the conjunction of the premises $r_1 = 0 \wedge \cdots \wedge r_n = 0$ in (1) is equivalent to the single premise $r_1 + \cdots + r_n = 0$, so we can without loss of generality restrict our attention to Hoare formulas of the form

$$r = 0 \quad \rightarrow \quad s = t. \tag{2}$$

Theorem 0.1 (Cohen [1]) *The following are equivalent:*

(i) $\mathsf{KA} \models r = 0 \rightarrow p = q$

(ii) $\mathsf{KA}^* \models r = 0 \rightarrow p = q$

(iii) $\models p + uru = q + uru.$

In (iii), we do not need to write KA or KA^*, since we have shown that the equational theories coincide. Note that the equivalence of (i) and (ii) does not follow immediately from Theorem **??**, since they are not equations but equational implications.

Proof. We first define a congruence on regular expressions in RExp_Σ. For $s, t \in \mathsf{RExp}_\Sigma$, define

$$s \equiv t \quad \overset{\text{def}}{\Longleftrightarrow} \quad \vDash s + uru = t + uru.$$

The relation $\equiv$ is an equivalence relation. We show that it is a star-continuous Kleene algebra congruence.

If $s = t$ is a theorem of Kleene algebra, then $s \equiv t$, since $\vDash s = t$ implies $\vDash s + uru = t + uru$.

To show $\equiv$ is a congruence with respect to $+$, we need to show that $s \equiv t$ implies $s + w \equiv t + w$. But this says only that $\vDash s + uru = t + uru$ implies $\vDash s + w + uru = t + w + uru$, which is immediately apparent.

To show $\equiv$ is a congruence with respect to $\cdot$, we need to show that $s \equiv t$ implies $sw \equiv tw$ and $ws \equiv wt$. We establish the former; the latter follows by symmetry.

$$\begin{aligned}
&\vDash s + uru = t + uru \\
&\quad \Rightarrow \quad \vDash (s + uru)w = (t + uru)w \\
&\quad \Rightarrow \quad \vDash sw + uruw = tw + uruw \\
&\quad \Rightarrow \quad \vDash sw + uruw + uru = tw + uruw + uru \\
&\quad \Rightarrow \quad \vDash sw + uru = tw + uru.
\end{aligned}$$

To show $\equiv$ is a congruence with respect to *, we need to show that $s \equiv t$ implies $s^* \equiv t^*$.

$$
\begin{aligned}
& \vDash s + uru = t + uru \\
& \quad \Rightarrow \;\; \vDash (s + uru)^* = (t + uru)^* \\
& \quad \Rightarrow \;\; \vDash s^*(urus^*)^* = t^*(urut^*)^* \\
& \quad \Rightarrow \;\; \vDash s^*(1 + urus^*(urus^*)^*) = t^*(1 + urut^*(urut^*)^*) \\
& \quad \Rightarrow \;\; \vDash s^* + s^*urus^*(urus^*)^* = t^* + t^*urut^*(urut^*)^* \\
& \quad \Rightarrow \;\; \vDash s^* + s^*urus^*(urus^*)^* + uru = t^* + t^*urut^*(urut^*)^* + uru \\
& \quad \Rightarrow \;\; \vDash s^* + uru = t^* + uru.
\end{aligned}
$$

Finally, to show that $\equiv$ respects star-continuity condition, we need only show that if $st^nv \leqq y$ for all n, then $st^*v \leqq y$, where $p \leqq q$ is an abbreviation for $p + q \equiv q$.

$$
\begin{aligned}
& \vDash (st^nv + y) + uru = y + uru \text{ for all } n \\
& \quad \Rightarrow \;\; \vDash st^nv + (y + uru) = y + uru \text{ for all } n \\
& \quad \Rightarrow \;\; \vDash st^*v + (y + uru) = y + uru \qquad (3) \\
& \quad \Rightarrow \;\; \vDash (st^*v + y) + uru = y + uru.
\end{aligned}
$$

The crucial step (3) follows from the fact that if $st^nv \leq y + uru$ for all n in all star-continuous Kleene algebras, then $st^*v \leq y + uru$ in all star-continuous Kleene algebras.

Since $\equiv$ is a KA^* congruence on RExp_Σ, we can form the quotient $\mathsf{RExp}_\Sigma/\equiv$ and canonical interpretation $s \mapsto [s]$, where $[s]$ denotes the $\equiv$-congruence class of s, and this structure is a star-continuous Kleene algebra. The equation $r = 0$ is satisfied under this interpretation, since

$$\vDash r + uru \;\; = \;\; uru \;\; = \;\; 0 + uru,$$

so $r \equiv 0$.

Now we are ready to prove the equivalence of the three conditions in the statement of the theorem.

(i) $\Rightarrow$ (ii)   Any formula true in all Kleene algebras is certainly true in all star-continuous Kleene algebras.

(ii) $\Rightarrow$ (iii)   If $\mathsf{KA}^* \models r = 0 \to p = q$, then since $\mathsf{RExp}_\Sigma/\equiv$ is a star-continuous Kleene algebra and $\mathsf{RExp}_\Sigma/\equiv, [\;] \vDash r = 0$, we have $\mathsf{RExp}_\Sigma/\equiv, [\;] \vDash p = q$. By definition, $p \equiv q$, which is what we wanted to show.

(iii) $\Rightarrow$ (i)   Suppose $\models p + uru = q + uru$. Let K be an arbitrary Kleene algebra and let I be an arbitrary interpretation over K such that $K, I \models r = 0$. Then $K, I \models p = p + uru = q + uru = q$. Since K and I were arbitrary, $\mathsf{KA} \models r = 0 \to p = q$. $\square$

References

[1] Ernie Cohen. Hypotheses in Kleene algebra. Unpublished, April 1994.

[2] Dexter Kozen. On the complexity of reasoning in Kleene algebra. In *Proc. 12th Symp. Logic in Comput. Sci.*, pages 195–202, Los Alamitos, Ca., June 1997. IEEE.