Introduction to Kleene Algebra	**Lecture 21**
CS786 Spring 2002	**Tuesday, April 16, 2002**

Completeness of KAT

In this lecture we show that the equational theories of the Kleene algebras with tests and the star-continuous Kleene algebras with tests coincide. Combined with the results of the previous lecture, this says that KAT is complete for the equational theory of relational models and $\mathsf{Reg}_{\mathsf{P},\mathsf{B}}$ forms the free KAT on generators P and B. This result is analogous to the completeness result of Lecture **??**, which states that the regular sets over a finite alphabet P form the free Kleene algebra on generators P. The results of this lecture are from [5].

Theorem 0.1 *Let* REL *denote the class of all relational Kleene algebras with tests. Let* $p, q \in \mathsf{RExp}_{\mathsf{P},\mathsf{B}}$. *The following are equivalent:*

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

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

(iii) $G(p) = G(q)$

(iv) $\mathsf{REL} \vDash p = q$.

The statements (ii)–(iv) were shown to be equivalent in Theorem **??** of Lecture **??**. Here we have added (i) to the list. Thus, for the purpose of deriving identities, the infinitary star-continuity condition provides no extra power over the finitary axiomatization KAT. However, it does entail more Horn formulas (equational implications).

One possible approach might be to modify the completeness proof of Lecture **??** for KA to handle tests. We take a different approach here, showing that every term p can be transformed into a KAT-equivalent term $\widehat{p}$ such that $G(\widehat{p})$, the set of guarded strings represented by $\widehat{p}$, is the same as $R(\widehat{p})$, the set of strings represented by $\widehat{p}$ under the ordinary interpretation of regular expressions. The Boolean algebra axioms are not needed in equivalence proofs involving such terms, so we can apply the completeness result of Lecture **??** directly. This idea is ultimately due to Kaplan [3].

Consider the set $\overline{\mathsf{B}} = \{\overline{b} \mid b \in \mathsf{B}\}$, the set of negated atomic tests. We can view $\overline{\mathsf{B}}$ as a separate set of primitive symbols disjoint from B and P. Using the DeMorgan laws and the law $\overline{\overline{b}} = b$ of Boolean algebra, every term p can be transformed to a KAT-equivalent term

p' in which $^{-}$ is applied only to primitive test symbols, thus we can view p' as a regular expression over the alphabet $\mathsf{P} \cup \mathsf{B} \cup \overline{\mathsf{B}}$. As such, it represents a set of strings

$$R(p') \quad \subseteq \quad (\mathsf{P} \cup \mathsf{B} \cup \overline{\mathsf{B}})^*$$

under the standard interpretation R of regular expressions as regular sets.

In general, the sets $R(p')$ and $G(p')$ may differ. For example, $R(q) = \{q\}$ for primitive action q, but $G(q) = \{\alpha q \beta \mid \alpha, \beta \in \mathsf{Atoms}_\mathsf{B}\}$.

Our main task will be to show how to further transform p' to another KAT-equivalent string $\widehat{p}$ such that all elements of $R(\widehat{p})$ are guarded strings and $R(\widehat{p}) = G(\widehat{p})$. We can then use the completeness result of [4], since p and q will be KAT-equivalent iff $\widehat{p}$ and $\widehat{q}$ are equivalent as regular expressions over $\mathsf{P} \cup \mathsf{B} \cup \overline{\mathsf{B}}$; that is, if they can be proved equivalent in pure Kleene algebra.

Example 0.2 Consider the two terms

$$\begin{aligned} p &= (q + b + \overline{b})^* br \\ \widehat{p} &= (bq + \overline{b}q)^* br(b + \overline{b}), \end{aligned}$$

where $\mathsf{P} = \{q, r\}$ and $\mathsf{B} = \{b\}$. There are certainly strings in $R(p)$, $qq\overline{b}bbqbr$ for example, that are not guarded strings. However, p and $\widehat{p}$ represent the same set of guarded strings under the interpretation G, and all strings in $R(\widehat{p})$ are guarded strings; that is, $G(p) = G(\widehat{p}) = R(\widehat{p})$. $\square$

In our inductive proof, it will be helpful to maintain terms in the following special form. Call a term *externally guarded* if it is of the form α or $\alpha q \beta$, where α and β are atoms of B. For an externally guarded term $\alpha q \beta$, define $\mathsf{first}\, p = \alpha$ and $\mathsf{last}\, p = \beta$. For an externally guarded term α, define $\mathsf{first}\, p = \mathsf{last}\, p = \alpha$. Define a special multiplication operation $\diamond$ on externally guarded terms as follows:

$$r\alpha \diamond \beta s \quad \stackrel{\text{def}}{=} \quad \begin{cases} r\alpha s, & \text{if } \alpha = \beta, \\ 0, & \text{if } \alpha \neq \beta. \end{cases}$$

This is much like fusion product on guarded strings as defined in Lecture **??**, except that for incompatible pairs of guarded strings, fusion product is undefined, whereas $\diamond$ is defined and has value 0.

For any two externally guarded terms q and r, $q \diamond r$ is externally guarded, and $q \diamond r = qr$ is a theorem of KAT; in particular,

$$G(q \diamond r) \quad = \quad G(q) \cdot G(r).$$

If $\sum_i q_i$ and $\sum_j r_j$ are sums of zero or more externally guarded terms, define

$$(\sum_i q_i) \diamond (\sum_j r_j) \quad \stackrel{\mathrm{def}}{=} \quad \sum_{i,j} q_i \diamond r_j.$$

As above, for any two sums q and r of externally guarded terms, $q \diamond r = qr$ is a theorem of KAT; in particular,

$$G(q \diamond r) \quad = \quad G(q) \cdot G(r),$$

and $q \diamond r$ is a sum of externally guarded terms.

Lemma 0.3 *For every term p, there is a term $\widehat{p}$ such that*

(i) $\mathsf{KAT} \models p = \widehat{p}$

(ii) $R(\widehat{p}) = G(\widehat{p})$

(iii) *$\widehat{p}$ is a sum of zero or more externally guarded terms.*

Proof. As argued above, we can assume without loss of generality that all occurrences of $^-$ in p are applied to primitive tests only, thus we may view p as a term over the alphabet $\mathsf{P} \cup \mathsf{B} \cup \overline{\mathsf{B}}$.

We define $\widehat{p}$ by induction on the structure of p. For the basis, take

$$\begin{array}{lllllll} \widehat{p} & \stackrel{\mathrm{def}}{=} & \sum_{\alpha,\beta \in \mathsf{Atoms}_\mathsf{B}} \alpha p \beta, \quad p \in \mathsf{P} & \qquad & \widehat{1} & \stackrel{\mathrm{def}}{=} & \sum_{\alpha \in \mathsf{Atoms}_\mathsf{B}} \alpha \\ \widehat{b} & \stackrel{\mathrm{def}}{=} & \sum_{\alpha \leq b} \alpha, \quad b \in \mathsf{B} \cup \overline{\mathsf{B}} & & \widehat{0} & \stackrel{\mathrm{def}}{=} & 0. \end{array}$$

In each of these cases, it is straightforward to verify (i), (ii), and (iii).

For the induction step, suppose we have terms p and q satisfying (ii) and (iii). We take

$$\widehat{p+q} \quad \stackrel{\mathrm{def}}{=} \quad p + q \qquad\qquad \widehat{pq} \quad \stackrel{\mathrm{def}}{=} \quad p \diamond q.$$

These constructions are easily shown to satisfy (i), (ii), and (iii).

It remains to construct $\widehat{p^*}$. We proceed by induction on the number of externally guarded terms in the sum p.

For the basis, we define

$$\begin{array}{rcll} \widehat{0^*} & \stackrel{\mathrm{def}}{=} & \widehat{1} & \\ \widehat{\alpha^*} & \stackrel{\mathrm{def}}{=} & \widehat{1} & \\ \widehat{(\alpha q \beta)^*} & \stackrel{\mathrm{def}}{=} & \widehat{1} + \alpha q \beta, \quad \alpha \neq \beta & \qquad (1) \\ \widehat{(\alpha q \alpha)^*} & \stackrel{\mathrm{def}}{=} & \widehat{1} + \alpha q (\alpha q)^* \alpha. & \qquad (2) \end{array}$$

For the induction step, let $p = q+r$, where r is an externally guarded term and q is a sum of externally guarded terms, one fewer in number than in p. By the induction hypothesis, we can construct $q' = \widehat{q^*}$ with the desired properties. Suppose the initial atom of the externally guarded term r is α. Then $\mathsf{KAT} \models r = \alpha r$. Moreover, the expression $(rq'\alpha)^*$ is KAT-equivalent to $(r \diamond q' \diamond \alpha)^*$, which by distributivity can be put into a form in which (1) or (2) applies, yielding a term q'' satisfying (ii) and (iii).

Reasoning in KAT,

$$\begin{array}{rcll}
p^* & = & (q+r)^* & \\
& = & q^*(rq^*)^* & \text{by the denesting rule} \\
& = & q'(rq')^* & \\
& = & q' + q'rq'(rq')^* & \text{by unwinding and distributivity} \\
& = & q' + q'rq'(\alpha rq')^* & \\
& = & q' + q'(rq'\alpha)^* rq' & \text{by the sliding rule} \\
& = & q' + q'q''rq' & \\
& = & q' + q' \diamond q'' \diamond r \diamond q', &
\end{array}$$

which is of the desired form. □

Theorem 0.4

$$\mathsf{KAT} \models p = q \quad \Leftrightarrow \quad G(p) = G(q).$$

In other words, the equational theories of the Kleene algebras with tests and the star-continuous Kleene algebras with tests coincide.

Proof. The forward implication is immediate, since $\mathsf{Reg}_{\mathsf{P},\mathsf{B}}$ is a Kleene algebra with tests.

For the reverse implication, suppose $G(p) = G(q)$. By Lemma 0.3(i) and Theorem **??** of Lecture **??**, $G(\widehat{p}) = G(\widehat{q})$. By Lemma 0.3(ii), $R(\widehat{p}) = R(\widehat{q})$. By the completeness of KA (Lecture **??**), $\mathsf{KA} \models \widehat{p} = \widehat{q}$. Combining this with Lemma 0.3(i), we have $\mathsf{KAT} \models p = q$. □

Since we have shown that the equational theories of the Kleene algebras with tests and the star-continuous Kleene algebras with tests coincide, we can henceforth write $\models p = q$ unambiguously in place of $\mathsf{KAT}^* \models p = q$ or $\mathsf{KAT} \models p = q$.

Decidability

Once we have Theorem 0.1, the decidability of the equational theory of Kleene algebra with tests follows almost immediately from a simple reduction to Propositional Dynamic Logic

(PDL). Any term in the language of KAT is a program of PDL (after replacing Boolean terms b with PDL tests $b?$), and it is known that two such terms p and q represent the same binary relation in all relational structures iff

$$\mathsf{PDL} \models \mathsf{<}p\mathsf{>}c \leftrightarrow \mathsf{<}q\mathsf{>}c,$$

where c is a new primitive proposition symbol [1] (see [2]). By Theorems 0.1 and 0.4, this is tantamount to deciding KAT-equivalence.

PDL is known to be exponential time complete [1, 6], thus the equational theory of KAT is decidable in no more than exponential time. It is at least *PSPACE*-hard, since the equational theory of Kleene algebra is [7].

We will show in Lecture **??** by different methods that the equational theory of KAT is *PSPACE*-complete.

References

[1] Michael J. Fischer and Richard E. Ladner. Propositional dynamic logic of regular programs. *J. Comput. Syst. Sci.*, 18(2):194–211, 1979.

[2] David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic.* MIT Press, Cambridge, MA, 2000.

[3] Donald M. Kaplan. Regular expressions and the equivalence of programs. *J. Comput. Syst. Sci.*, 3:361–386, 1969.

[4] Dexter Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Infor. and Comput.*, 110(2):366–390, May 1994.

[5] Dexter Kozen and Frederick Smith. Kleene algebra with tests: Completeness and decidability. In D. van Dalen and M. Bezem, editors, *Proc. 10th Int. Workshop Computer Science Logic (CSL'96)*, volume 1258 of *Lecture Notes in Computer Science*, pages 244–259, Utrecht, The Netherlands, September 1996. Springer-Verlag.

[6] V. R. Pratt. Models of program logics. In *Proc. 20th Symp. Found. Comput. Sci.*, pages 115–122. IEEE, 1979.

[7] L. J. Stockmeyer and A. R. Meyer. Word problems requiring exponential time. In *Proc. 5th Symp. Theory of Computing*, pages 1–9, New York, 1973. ACM.