In the next few lectures we will show that KAT is complete over relational and language models, and that the regular sets of guarded strings form the free KAT generated by the primitive action and test symbols. We will not have to redo the proof for KA, but we will be able to use it as a lemma.

Completeness of KAT* over Reg P, B

First we show that the result holds in the presence of the star-continuity axiom. Later, we will be able to relax this assumption and fall back on the KAT axioms without star-continuity. But for now, let us show that an equation $p = q$ with primitive symbols in P and B is a theorem of KAT* iff it holds under the standard interpretation $G : \mathsf{Exp}\,\mathsf{P},\mathsf{B} \to \mathsf{Reg}\,\mathsf{P},\mathsf{B}$. Thus Reg P, B is the free star-continuous Kleene algebra with tests on generators P and B.

Theorem 1. *Let $p, q \in \mathsf{Exp}\,\mathsf{P},\mathsf{B}$. Then $\mathsf{KAT}^* \vDash p = q$ if and only if $G(p) = G(q)$.*

Thus the equational theory of Reg P, B under the interpretation G the same as the set of equations that hold under all interpretations of P and B in all star-continuous Kleene algebras with tests.

The forward implication is easy, since Reg P, B is a star-continuous Kleene algebra. The converse is a consequence of the following lemma, which is analogous to a similar lemma proved earlier for KA.

Lemma 2. *For any star-continuous Kleene algebra with tests K, interpretation $I : \mathsf{Exp}\,\mathsf{P},\mathsf{B} \to K$, and $p, q, r \in \mathsf{Exp}\,\mathsf{P},\mathsf{B}$,*

$$I(pqr) = \sup_{x \in G(q)} I(pxr)$$

where the supremum is with respect to the natural order in K. In particular,

$$I(q) = \sup_{x \in G(q)} I(x).$$

This result is analogous to the same result for star-continuous Kleene algebras proved in Lecture **??** and the proof is similar. Note that the star-continuity axiom is a special case.

As before, we are most interested in the second statement, but there is a slight subtlety that requires the stronger first statement as the induction hypothesis. In addition to the existence of the supremum, the more general statement provides a kind of infinite distributivity law over existing suprema. The need for this arises mainly in the induction case for multiplication.

Proof of Lemma 2. We proceed by induction on the structure of q. The basis consists of cases for primitive tests, primitive actions, 0 and 1. We argue the case for primitive actions and primitive tests explicitly.

For a primitive action $q \in \mathsf{P}$, recall that $G(q) = \{\alpha q \beta \mid \alpha, \beta \in \mathsf{At}\}$. Then

$$\begin{aligned} I(pqr) &= I(p)I(1)I(q)I(1)I(r) = \sup\{I(p)I(\alpha)I(q)I(\beta)I(r) \mid \alpha, \beta \in \mathsf{At}\} \\ &= \sup\{I(p\alpha q \beta r) \mid \alpha, \beta \in \mathsf{At}\} = \sup\{I(pxr) \mid x \in G(q)\}. \end{aligned}$$

where $I(1) = \sum \mathsf{At}$. Finite distributivity was used in the second step.

For a primitive test $b \in B$, recall that $G(b) = \{\alpha \mid \alpha \le b\}$. Then

$$\begin{aligned} I(pbr) &= I(p)I(b)I(r) = \sup\{I(p)I(\alpha)I(r) \mid \alpha \le b\} \\ &= \sup\{I(p\alpha r) \mid \alpha \le b\} = \sup\{I(pxr) \mid x \in G(b)\}. \end{aligned}$$

Again, finite distributivity was used in the second step.

The induction step consists of cases for $+$, $\cdot$, *, and $^-$. The cases other than $\cdot$ and $^-$ are the same as in the earlier proof for KA.

For the case $\cdot$, recall that

$$G(qq') = G(q) \cdot G(q') = \{y \diamond z \mid y \in G(q),\ z \in G(q'),\ y \diamond z \text{ exists}\} = \{y\alpha z \mid y\alpha \in G(q),\ \alpha z \in G(q')\}.$$

Applying the induction hypothesis twice,

$$\begin{aligned} I(pqq'r) &= \sup\{I(pqvr) \mid v \in G(q')\} \\ &= \sup\{\sup\{I(puvr) \mid u \in G(q)\} \mid v \in G(q')\} \\ &= \sup\{I(puvr) \mid u \in G(q),\ v \in G(q')\}. \end{aligned}$$

The last step follows from a purely lattice-theoretic argument: if all the suprema in question on the left hand side exist, then the supremum on the right hand side exists and the two sides are equal. Now

$$\begin{aligned} &\sup\{I(puvr) \mid u \in G(q),\ v \in G(q')\} \\ &\quad = \sup\{I(py\alpha\beta zr) \mid y\alpha \in G(q),\ \beta z \in G(q')\} \\ &\quad = \sup\{I(py\alpha\alpha zr) \mid y\alpha \in G(q),\ \alpha z \in G(q')\} \qquad (1) \\ &\quad = \sup\{I(py\alpha zr) \mid y\alpha \in G(q),\ \alpha z \in G(q')\} \\ &\quad = \sup\{I(pxr) \mid x \in G(qq')\}. \end{aligned}$$

The justification for step (1) is that if $\alpha \neq \beta$, then the product in K is 0 and does not contribute to the supremum.

For the case $^-$, recall that

$$G(\bar{b}) = \mathsf{At} \setminus G(b) = \{\alpha \mid \alpha \not\leq b\} = \{\alpha \mid \alpha \leq \bar{b}\}.$$

Then

$$I(p\bar{b}r) = \sup\{I(p\alpha r) \mid \alpha \leq \bar{b}\} = \sup\{I(p\alpha r) \mid \alpha \in G(\bar{b})\}. \qquad \square$$

Proof of Theorem 1. If $\mathsf{KAT}^* \vDash p = q$ then $G(p) = G(q)$, since $\mathsf{Reg}\,\mathsf{P},\mathsf{B}$ is a star-continuous Kleene algebra with tests. Conversely, if $G(p) = G(q)$, then by Lemma 2, for any star-continuous Kleene algebra with tests K and any interpretation I over K, $I(p) = I(q)$. Therefore $\mathsf{KAT}^* \vDash p = q$. $\square$

Completeness over Relational Models

In this section we show completeness of KAT^* over relational interpretations. It will suffice to construct a relational model isomorphic to $\mathsf{Reg}\,\mathsf{P},\mathsf{B}$. This construction is similar to a construction we have seen before for KA.

Lemma 3. *The language-theoretic model* 2^{GS} *and its submodel* $\mathsf{Reg}\,\mathsf{P},\mathsf{B}$ *are isomorphic to relational models.*

Proof. Define

$$h : 2^{\mathsf{GS}} \to 2^{\mathsf{GS}\times\mathsf{GS}} \qquad\qquad h(A) \stackrel{\text{def}}{=} \{(x, x \diamond y) \mid x \in \mathsf{GS},\ y \in A,\ \mathsf{last}\,x = \mathsf{first}\,y\}.$$

We show that h embeds 2^{GS} isomorphically onto a subalgebra of the Kleene algebra of all binary relations on GS.

It is not difficult to verify that h is a homomorphism:

$$\begin{aligned}
h(AB) &= \{(z, z \diamond r) \mid z \in \mathsf{GS},\ r \in AB,\ \mathsf{last}\, z = \mathsf{first}\, r\} \\
&= \{(z, z \diamond p \diamond q) \mid z \in \mathsf{GS},\ p \in A,\ q \in B,\ \mathsf{last}\, p = \mathsf{first}\, q,\ \mathsf{last}\, z = \mathsf{first}\,(p \diamond q)\} \\
&= \{(z, z \diamond p) \mid z \in \mathsf{GS},\ p \in A,\ \mathsf{last}\, z = \mathsf{first}\, p\} \ ;\ \{(y, y \diamond q) \mid y \in \mathsf{GS},\ q \in B,\ \mathsf{last}\, y = \mathsf{first}\, q\} \\
&= h(A) \ ;\ h(B)
\end{aligned}$$

$$h(A \cup B) = h(A) \cup h(B) \qquad\qquad h(A^*) = h(\bigcup_{n \geq 0} A^n) = \bigcup_{n \geq 0} h(A)^n = h(A)^*$$

$$h(\mathsf{At}) = \{(x, x \diamond \alpha) \mid x \in \mathsf{GS},\ \alpha \in \mathsf{At},\ \mathsf{last}\, x = \alpha\} = \{(x, x) \mid x \in \mathsf{GS}\} = \mathsf{id} \qquad\qquad h(0) = \varnothing$$

$$\begin{aligned}
h(\overline{B}) &= h(\{\alpha \mid \alpha \notin B\}) = \{(x, x \diamond \alpha) \mid \alpha \notin B,\ \mathsf{last}\, x = \alpha\} \\
&= \{(x, x) \mid \mathsf{last}\, x \notin B\} = \mathsf{id} \setminus \{(x, x) \mid \mathsf{last}\, x \in B\} = \mathsf{id} \setminus h(B).
\end{aligned}$$

The function h is injective, since A can be uniquely recovered from $h(A)$:

$$A = \{y \mid \exists \alpha\ (\alpha, y) \in h(A)\}.$$

The submodel $\mathsf{Reg}\,\mathsf{P}, \mathsf{B}$ is perforce isomorphic to a relational model on GS, namely the image of $\mathsf{Reg}\,\mathsf{P}, \mathsf{B}$ under h. □

Combining Theorem 1, Lemma 3, and the fact that all relational models are star-continuous Kleene algebras with tests, we have

Theorem 4. *Let* REL *denote the class of all relational Kleene algebras with tests. Let* $p, q \in \mathsf{Exp}\,\mathsf{P}, \mathsf{B}$. *The following are equivalent:*

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

(ii) $G(p) = G(q)$

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

Completeness of KAT

In this segment we show that the equational theories of the Kleene algebras with tests and the star-continuous Kleene algebras with tests coincide. Combined with previous results, 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 for KA, which states that the regular sets over a finite alphabet P form the free Kleene algebra on generators P. The results of this segment are from [6].

Theorem 5. *Let* REL *denote the class of all relational Kleene algebras with tests. Let* $p, q \in \mathsf{Exp}\,\mathsf{P}, \mathsf{B}$. *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 previously shown to be equivalent. Here we add (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). Note that $\mathsf{KAT} \vDash p = q$ iff $\mathsf{KAT} \vdash p = q$ and $\mathsf{KAT}^* \vDash p = q$ iff $\mathsf{KAT}^* \vdash p = q$ by the completeness of equational logic.

One possible approach might be to modify the completeness proof 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 for KA directly.

Consider the set $\overline{\mathsf{B}} = \{\bar{b} \mid b \in \mathsf{B}\}$, 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 De Morgan laws and the law $\bar{\bar{b}} = b$ 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

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

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 $G(q) = \{\alpha q \beta \mid \alpha, \beta \in \mathsf{At}\}$.

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 6. *Consider the two terms*

$$p = (q + b + \bar{b})^* br \qquad\qquad \widehat{p} = (bq + \bar{b}q)^* br(b + \bar{b}),$$

where $\mathsf{P} = \{q, r\}$ and $\mathsf{B} = \{b\}$. There are certainly strings in $R(p)$, $qq\bar{b}bbqbr$ 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, $G(p) = G(\widehat{p}) = R(\widehat{p})$.

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 $\alpha q \beta$, let $\mathsf{first}\, p = \alpha$ 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:

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

This is much like fusion product on guarded strings as defined previously, except that for incompatible pairs of guarded strings, fusion product is undefined, whereas here $\diamond$ 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,

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

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

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

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

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

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

Lemma 7. *For every term p, there is a term $\widehat{p}$ such that*

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

(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

$$\widehat{p} \stackrel{\text{def}}{=} \sum_{\alpha,\beta \in \mathsf{At}} \alpha p \beta, \quad p \in \mathsf{P} \qquad\qquad \widehat{1} \stackrel{\text{def}}{=} \sum_{\alpha \in \mathsf{At}} \alpha$$

$$\widehat{b} \stackrel{\text{def}}{=} \sum_{\alpha \leq b} \alpha, \quad b \in \mathsf{B} \cup \overline{\mathsf{B}} \qquad\qquad \widehat{0} \stackrel{\text{def}}{=} 0.$$

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

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

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

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 $\widehat{p}$. For the basis, we define

$$\widehat{0^*} \stackrel{\text{def}}{=} \widehat{1} \qquad\qquad \widehat{\alpha^*} \stackrel{\text{def}}{=} \widehat{1} \qquad\qquad \widehat{(\alpha q \beta)^*} \stackrel{\text{def}}{=} \begin{cases} \widehat{1} + \alpha q \beta, & \text{if } \alpha \neq \beta, \\ \widehat{1} + \alpha q (\alpha q)^* \alpha, & \text{if } \alpha = \beta. \end{cases} \tag{2}$$

For the induction step, consider a sum $q + r$, where r is an externally guarded term and q is a sum of one fewer externally guarded terms. By the induction hypothesis, we can construct

$$\widehat{q^*} = \sum_i \alpha_i q_i \beta_i$$

with the desired properties. Suppose that $\mathsf{first}\, r = \alpha$. Then $\mathsf{KAT} \vDash r = \alpha r$. Moreover, the following equations are provable in KAT:

$$r\widehat{q^*}\alpha = r(\sum_i \alpha_i q_i \beta_i)\alpha = \sum_i (r \diamond \alpha_i q_i \beta_i \diamond \alpha) = \sum_{\substack{\mathsf{last}\, r = \alpha_i \\ \beta_i = \alpha}} r q_i \alpha = r(\sum_{\substack{\mathsf{last}\, r = \alpha_i \\ \beta_i = \alpha}} q_i)\alpha,$$

and the expression on the right-hand side is externally guarded and satisfies (ii). We can therefore apply (2) to this expression, yielding an expression q' equivalent to $(r\widehat{q^*}\alpha)^*$ and satisfying (ii) and (iii).

Now reasoning in KAT,

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

which is of the desired form. □

The next theorem shows that the equational theories of the Kleene algebras with tests and the star-continuous Kleene algebras with tests coincide, thus the KAT axioms are complete for the equational theory of Reg P, B under the canonical interpretation.

Theorem 8. KAT $\vdash p = q$ *if and only if* $G(p) = G(q)$.

Proof. The forward implication is immediate, since Reg P, B is a Kleene algebra with tests.

For the reverse implication, suppose $G(p) = G(q)$. By Lemma 7(ii) and the soundness of the KAT axioms,

$$R(\widehat{p}) = G(\widehat{p}) = G(p) = G(q) = G(\widehat{q}) = R(\widehat{q}).$$

By the completeness theorem for KA, KA $\vdash \widehat{p} = \widehat{q}$. Combining this with Lemma 7(i), KAT $\vdash p = q$. □

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 $\vDash p = q$ unambiguously in place of KAT$^* \vDash p = q$ or KAT $\vDash p = q$.

Decidability

Once we have Theorem 5, 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

$$\text{PDL} \vDash \langle p\rangle c \;\Leftrightarrow\; \langle q\rangle c,$$

where c is a new primitive proposition symbol [2] (see [3]). By Theorems 5 and 8, this is tantamount to deciding KAT-equivalence.

PDL is known to be exponential time complete [2, 7], 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 [8]. We will show later by different methods that the equational theory of KAT is PSPACE-complete.

KAT and the Hoare Theory of Relational Models

We have previously shown that for any proof rule of PHL, or more generally, for any rule of the form

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

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

$$b_1p_1\bar{c}_1 = 0 \wedge \cdots \wedge b_np_n\bar{c}_n = 0 \;\Rightarrow\; bp\bar{c} = 0 \tag{3}$$

is a theorem of KAT. In this lecture we strengthen this result to show (Corollary 10) that *all* universal Horn formulas of the form

$$r_1 = 0 \wedge \cdots \wedge r_n = 0 \;\Rightarrow\; p = q \tag{4}$$

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 (4) over relational interpretations. Corollary 10 is trivially false for PHL; for example, the rule

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

cannot be proved in PHL for the simple reason that the Hoare rules only increase the length of programs. The results of this lecture are from [5].

Cohen [1] proved this result for KA. Here we generalize Cohen's result in two ways: to handle tests and to show completeness over relational models and KAT. The deductive completeness of KAT over relationally valid formulas of the form (4) will follow as a corollary. Later we will show how to handle some other specific types of premises as well.

Let $\mathsf{Exp}\,\mathsf{P},\mathsf{B}$ 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 $r_1,\ldots,r_n,p,q \in \mathsf{Exp}\,\mathsf{P},\mathsf{B}$. Let $\top$ be the *universal expression*

$$\top = (p_1 + \cdots + p_m)^*.$$

Note that $G(\top) = \mathsf{GS}$, the set of all guarded strings over P,B. The formula (4) is equivalent to $r = 0 \Rightarrow p = q$, where $r = \sum_i r_i$.

Recall the algebra $\mathsf{Reg}\,\mathsf{P},\mathsf{B}$ of regular sets of guarded strings over P,B and the standard interpretation $G : \mathsf{Exp}\,\mathsf{P},\mathsf{B} \to \mathsf{Reg}\,\mathsf{P},\mathsf{B}$. We showed earlier that $\mathsf{Reg}\,\mathsf{P},\mathsf{B}$ is the free KAT on generators P,B in the sense that for any terms $s,t \in \mathsf{Exp}\,\mathsf{P},\mathsf{B}$,

$$\vDash s = t \;\Leftrightarrow\; G(s) = G(t). \tag{5}$$

Theorem 9. *The following four conditions are equivalent:*

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

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

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

(iv) $\vDash\; p + \top r \top = q + \top r \top$.

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

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

$$\mathsf{KAT} \vDash p + \top r \top = q + \top r \top \;\Rightarrow\; (r = 0 \;\Rightarrow\; p = q),$$

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

$$\text{if} \quad \mathsf{REL} \vDash r = 0 \;\Rightarrow\; p \le q \quad \text{then} \quad \vDash p \le q + \top r \top. \tag{6}$$

To show (6), we construct a relational interpretation M on states $S = \mathsf{GS} \setminus G(\top r \top)$, where G is the standard interpretation of expressions as sets of guarded strings. This is the set of guarded strings containing no substring in $G(r)$. Note that if $x, y, z \in \mathsf{GS}$ and $x \diamond y \diamond z \in S$, then $y \in S$. If $\mathsf{GS} \subseteq G(\top r \top)$, that is, if $S = \varnothing$, then we are done, since in that case $G(p) \subseteq \mathsf{GS} \subseteq G(\top r \top)$ and the right-hand side of (6) follows immediately from (5). Similarly, if $G(1) \subseteq G(\top r \top)$, then $\mathsf{GS} = G(\top)G(1) \subseteq G(\top\top r \top) \subseteq G(\top r \top)$ and the same argument applies. We can therefore assume without loss of generality that both S and $G(1) \setminus G(\top r \top)$ are nonempty.

The atomic symbols are interpreted in M as follows:

$$M(p) \stackrel{\text{def}}{=} \{(x, xp\beta) \mid xp\beta \in S\},\ p \in \mathsf{P} \qquad M(b) \stackrel{\text{def}}{=} \{(x, x) \mid x \in S,\ \mathsf{last}\, x \leq b\},\ b \in \mathsf{B}.$$

The interpretations $M(p)$ of KAT expressions p as binary relations are defined inductively in the standard way for relational models.

We now show that for any $e \in \mathsf{Exp}\,\mathsf{P}, \mathsf{B}$,

$$M(e) = \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(e)\} \tag{7}$$

by induction on the structure of e. For primitive programs p and tests b,

$$M(p) = \{(x, xp\beta) \mid xp\beta \in S\} = \{(x, x \diamond \alpha p\beta) \mid x \diamond \alpha p\beta \in S\} = \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(p)\},$$
$$M(b) = \{(x, x) \mid x \in S,\ \mathsf{last}\, x \in G(b)\} = \{(x, x \diamond \beta) \mid x \diamond \beta \in S,\ \beta \in G(b)\} = \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(b)\}.$$

For the constants 0 and 1, we have

$$\begin{aligned}
M(0) &= \varnothing = \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(0)\},\\
M(1) &= \{(x, x) \mid x \in S\} = \{(x, x \diamond \beta) \mid x \diamond \beta \in S,\ \beta \in G(1)\}.
\end{aligned}$$

For compound expressions,

$$\begin{aligned}
M(s + t) &= M(s) \cup M(t)\\
&= \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(s)\} \cup \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(t)\}\\
&= \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(s) \cup G(t)\}\\
&= \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(s + t)\}
\end{aligned}$$

$$\begin{aligned}
M(st) &= M(s) \mathbin{;} M(t)\\
&= \{(x, x \diamond z) \mid x \diamond z \in S,\ z \in G(s)\} \mathbin{;} \{(y, y \diamond w) \mid y \diamond w \in S,\ w \in G(t)\}\\
&= \{(x, x \diamond z \diamond w) \mid x \diamond z \diamond w \in S,\ z \in G(s),\ w \in G(t)\}\\
&= \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(st)\}
\end{aligned}$$

$$\begin{aligned}
M(t^*) = \bigcup_n M(t^n) &= \bigcup_n \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(t^n)\}\\
&= \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in \bigcup_n G(t^n)\}\\
&= \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(t^*)\}.
\end{aligned}$$

We now show (6). Suppose the left-hand side holds. By (7),

$$M(r) = \{(x, x \diamond y) \mid x \diamond y \in S,\ y \in G(r)\} = \varnothing.$$

By the left-hand side of (6), $M(p) \subseteq M(q)$. In particular, for any $x \in G(p) \setminus G(\top r \top)$, $(\mathsf{first}\, x, x) \in M(p)$, therefore $(\mathsf{first}\, x, x) \in M(q)$ as well, thus $x \in G(q) \setminus G(\top r \top)$. But this says $G(p) \setminus G(\top r \top) \subseteq G(q) \setminus G(\top r \top)$, thus $G(p) \subseteq G(q) \cup G(\top r \top) = G(q + \top r \top)$. It follows from (5) that the right-hand side of (6) holds. $\square$

Corollary 10. KAT *is deductively complete for formulas of the form* (4) *over relational models.*

Proof. If the formula (4) is valid over relational models, then by Theorem 9, (iv) holds. Since KAT is complete for valid equations,

$$\mathsf{KAT} \vdash p + \top r \top = q + \top r \top.$$

But clearly

$$\mathsf{KAT} \vdash p + \top r \top = q + \top r \top \wedge r = 0 \;\Rightarrow\; p = q,$$

therefore

$$\mathsf{KAT} \vdash r = 0 \;\Rightarrow\; p = q.$$

□

Ideals

The elimination of hypotheses of the form $q = 0$ rests on the concept of an *ideal*. An *ideal* in an idempotent semiring K is a nonempty subset $I \subseteq K$ such that

(i) if $x, y \in I$, then $x + y \in I$

(ii) if $x \in I$ and $r \in K$, then $xr \in I$ and $rx \in I$

(iii) if $x \leq y$ and $y \in I$, then $x \in I$.

It follows that $0 \in I$. If desired, we might also postulate $1 \notin I$ to rule out the degenerate case $I = K$. This definition is in slight contrast to ideals in rings, where there is no analogue of (iii).

For $A \subseteq K$, define

$$\langle A \rangle \stackrel{\text{def}}{=} \{y \mid \exists n\ \exists a_1, \ldots, a_n \in A\ \exists u, v \in K\ y \leq u(a_1 + \cdots + a_n)v\}. \tag{8}$$

Lemma 11. *$\langle A \rangle$ is an ideal containing A, and is the smallest such ideal.*

Proof. Surely $A \subseteq \langle A \rangle$, since for $a \in A$, we can take $n = 1$, $y = a_1 = a$, and $u = v = 1$ in (8).

To show $\langle A \rangle$ is an ideal, we must show that it is closed under the operations (i)-(iii). For (i), if

$$y_1 \leq u_1(a_1 + \cdots + a_n)v_1 \qquad\qquad y_2 \leq u_2(b_1 + \cdots + b_m)v_2$$

with $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$, then

$$\begin{aligned} y_1 + y_2 &\leq u_1(a_1 + \cdots + a_n)v_1 + u_2(b_1 + \cdots + b_m)v_2 \\ &\leq (u_1 + u_2)(a_1 + \cdots + a_n)(v_1 + v_2) + (u_1 + u_2)(b_1 + \cdots + b_m)(v_1 + v_2) \\ &\leq (u_1 + u_2)(a_1 + \cdots + a_n + b_1 + \cdots + b_m)(v_1 + v_2). \end{aligned}$$

For (ii), if $y \leq u(a_1 + \cdots + a_n)v$ and $r \in K$, then

$$ry \leq ru(a_1 + \cdots + a_n)v \qquad\qquad yr \leq u(a_1 + \cdots + a_n)vr.$$

Finally, for (iii), if $x \leq y \leq u(a_1 + \cdots + a_n)v$, then $x \leq u(a_1 + \cdots + a_n)v$.

To show that $\langle A \rangle$ is the smallest ideal containing A, we only need to show that all ideals that contain A also contain $\langle A \rangle$. If I is an ideal containing A, then since I is closed under (i), it contains all elements $a_1 + \cdots + a_n$ for $a_1, \ldots, a_n \in A$. Since it is closed under (ii), it must contain all $u(a_1 + \cdots + a_n)v$ for $a_1, \ldots, a_n \in A$ and $u, v \in K$. Finally, since it is closed under (iii), it must contain all y such that $y \leq u(a_1 + \cdots + a_n)v$, $a_1, \ldots, a_n \in A$, and $u, v \in K$. But this is all of $\langle A \rangle$. $\square$

Given an ideal I, define

$$x \leq_I y \overset{\text{def}}{\Leftrightarrow} \exists z \in I \; x \leq y + z \qquad\qquad x \equiv_I y \overset{\text{def}}{\Leftrightarrow} x \leq_I y \wedge y \leq_I x. \tag{9}$$

Alternatively and with the same effect, we could define

$$x \equiv_I y \overset{\text{def}}{\Leftrightarrow} \exists z \in I \; x + z = y + z \qquad\qquad x \leq_I y \overset{\text{def}}{\Leftrightarrow} x + y \equiv_I y. \tag{10}$$

Lemma 12. *Let $h : K_1 \to K_2$ be any semiring homomorphism between idempotent semirings. Then the kernel of h,*

$$\ker h \overset{\text{def}}{=} \{s \mid h(s) = 0\},$$

is an ideal. Conversely, any ideal is the kernel of a semiring epimorphism.

Proof. Let $h : K_1 \to K_2$ be a semiring homomorphism. We argue that $\ker h$ satisfies the properties (i)-(iii) in the definition of ideals. For (i), if $h(x) = h(y) = 0$, then $h(x + y) = h(x) + h(y) = 0 + 0 = 0$, since h is a homomorphism. Similarly, for (ii), if $h(x) = 0$ and $r \in K_1$ is any other element, Then $h(xr) = h(x)h(r) = 0 \cdot h(r) = 0$ and $h(rx) = h(r)h(x) = h(r) \cdot 0 = 0$. Finally, for (iii), if $x \leq y$ and $h(y) = 0$, then $x + y = y$, so $h(x) = h(x) + 0 = h(x) + h(y) = h(x + y) = h(y) = 0$.

For the other direction, consider the relations $\equiv_I$ and $\leq_I$ defined in (9) and (10). One can show easily that the order $\leq_I$ is a preorder (reflexive and transitive) and $\equiv_I$ is an equivalence relation. Denote by K/I the quotient of K modulo $\equiv_I$ and let $[\cdot] : K \to K/I$ be the canonical map. The relation $\leq_I$ is well-defined on K/I:

$$x \equiv_I y \leq_I z \Rightarrow x \leq_I y \leq_I z \Rightarrow x \leq_I z,$$

and is a partial order (reflexive, transitive, and antisymmetric), and $I = [0]$:

$$x \equiv_I 0 \Leftrightarrow x \leq_I 0 \Leftrightarrow \exists z \in I \; x \leq z \Leftrightarrow x \in I.$$

Now we wish to show that $\equiv_I$ is a congruence with respect to addition and multiplication; that is,

$$x \equiv_I y \Rightarrow x + z \equiv_I y + z \qquad\qquad y \equiv_I y' \Rightarrow xyz \equiv_I xy'z.$$

These are quite easy to verify:

$$\begin{aligned} x \leq_I y \;&\Rightarrow\; \exists w \in I \; x \leq y + w \Rightarrow \; \exists w \in I \; x \leq y + w \\ &\Rightarrow\; \exists w \in I \; x + z \leq y + z + w \;\Rightarrow\; x + z \leq_I y + z, \end{aligned}$$

and similarly $y \leq_I x \Rightarrow y + z \leq_I x + z$, therefore

$$x \equiv_I y \;\Rightarrow\; x \leq_I y \qquad y \leq_I x \;\Rightarrow\; x + z \leq_I y + z \qquad y + z \leq_I x + z \;\Rightarrow\; x + z \equiv_I y + z.$$

Thus the operations are well defined on $\equiv_I$-classes and K/I is an idempotent semiring, and the canonical map $x \mapsto [x]$ is a semiring epimorphism $[\cdot] : K \to K/I$ with kernel I. $\square$

Quite fortuitously, and more than a little surprisingly, if K is a KAT, then the congruence $\equiv_I$ defined in (9) turns out to be a KAT-congruence, and the quotient K/I is a KAT.

Lemma 13. *If K is a* KAT*, then the relation $\equiv_I$ is a* KAT*-congruence and K/I is a* KAT*. If $I = \langle A \rangle$, then K/I, $[\cdot]$ is initial among all homomorphic images of K in which the image of A vanishes; that is, given any homomorphism $h : K \to K'$ such that $h(a) = 0$ for all $a \in A$, there exists a homomorphism $h' : K/I \to K'$ such that $h = h' \circ [\cdot]$.*

Proof. We must first show that $\equiv_I$ is a congruence with respect to * and $^-$ in order to verify that those operators are well defined on K/I. Note that, since I is closed under addition, to verify $x \equiv_I y$ it suffices to find $z, w \in I$ such that $x + z = y + w$, as this implies that $x + z + w = y + z + w$ and $z + w \in I$.

For *, we wish to show that if $x \equiv_I y$ then $x^* \equiv_I y^*$. Reasoning in KAT, we have

$$(x + z)^* = x^*(zx^*)^* = x^* + x^*zx^*(zx^*)^*, \tag{11}$$

and similarly for $(y + z)^*$. If $x + z = y + z$ with $z \in I$, then $(x + z)^* = (y + z)^*$, thus by (11),

$$x^* + x^*zx^*(zx^*)^* = y^* + y^*zy^*(zy^*)^*,$$

and both $x^*zx^*(zx^*)^*$ and $y^*zy^*(zy^*)^*$ are in I, therefore $x^* \equiv_I y^*$.

For negation, we show that the ideal I behaves like a Boolean algebra ideal on Boolean elements; that is, $c \equiv_I d$ iff $c\overline{d} + \overline{c}d \in I$. Suppose $c + z = d + z$ with $z \in I$. Multiplying on the left by $\overline{c}$, we have $\overline{c}z = \overline{c}d + \overline{c}z$, so $\overline{c}d \in I$. Similarly, multiplying on the right by $\overline{d}$ gives $c\overline{d} \in I$, therefore $c\overline{d} + \overline{c}d \in I$. Conversely, if $c\overline{d} + \overline{c}d \in I$, then $c + c\overline{d} + \overline{c}d = c + d = d + c\overline{d} + \overline{c}d$, so $c \equiv_I d$. By the symmetry of $c\overline{d} + \overline{c}d$, $c \equiv_I d$ implies that $\overline{c} \equiv_I \overline{d}$, thus $\equiv_I$ is a congruence with respect to negation.

We have shown that $\equiv_I$ is a congruence with respect to all the KAT operations, thus the KAT operations are well defined on the quotient K/I and the canonical map $x \mapsto [x]$ is a homomorphism. However, we have yet to show that K/I is a KAT. We know that it satisfies all equations, because the epimorphism $[\cdot]$ preserves all equations, and K is a KAT. However, we must also verify that the equational implications

$$ax \le x \;\Rightarrow\; a^*x \le x \qquad\qquad xa \le x \;\Rightarrow\; xa^* \le x$$

hold modulo $\equiv_I$ as well. We show the former; the latter follows from symmetry.

To show that $ax \le x \Rightarrow a^*x \le x$ holds modulo $\equiv_I$, we must show that if $ax \le_I x$, then $a^*x \le_I x$. If $ax \le_I x$, then $ax \le x + z$ for some $z \in I$. Reasoning in KAT,

$$a(x + a^*z) = ax + aa^*z \le x + z + aa^*z = x + a^*z.$$

Applying the same rule in K, we have $a^*(x + a^*z) \le x + a^*z$, thus $a^*x \le x + a^*z$. Since $a^*z \in I$, $a^*x \le_I x$.

Finally, to argue the last statement of the lemma, we wish to show that any homomorphism $h : K \to K'$ under which A vanishes factors through $K/\langle A \rangle$ via the canonical homomorphism $[\cdot]$. In other words, if $h(a) = 0$ for all $a \in A$, then there exists a homomorphism $h' : K/\langle A \rangle \to K'$ such that $h = h' \circ [\cdot]$.

$$\begin{tikzcd} & K/\langle A \rangle \arrow[d, "h'"] \\ K \arrow[ur, "{[\cdot]}"] \arrow[r, "h"'] & K' \end{tikzcd}$$

We need only observe that the condition that A vanishes under h means that $\langle A \rangle$ is contained in $\ker h$, thus if $x \equiv_I y$ then $h(x) = h(y)$, so h is well defined on $\equiv_I$ classes and reduces to a map $h' : K/\langle A \rangle \to K'$. $\square$

We have shown that if K is a KAT, then for any ideal I, the quotient K/I is a KAT, the canonical map $[\cdot] : K \to K/I$ is an epimorphism, and $I = [0]$. Moreover, K/I is initial among all homomorphic images of K such that $I = [0]$.

Another unusual fact is that, unlike the case of groups or rings, the ideal $[0]$ does not uniquely determine the homomorphic image up to isomorphism. For example, consider the free KA on one generator a. Modulo the inequality $a \le 1$, the resulting algebra is isomorphic to the *tropical semiring* used in shortest path algorithms; but the kernel of the canonical map to this algebra is $\{0\}$, the same as the identity.

If the KAT K has a top element $\top$, then any Horn formula of the form

$$s_1 = 0 \wedge \cdots \wedge s_n = 0 \;\Rightarrow\; s = t \tag{12}$$

reduces to a single equation in K. For instance, if K is finitely generated with generators $p_1, \ldots, p_k$, as is the case with all finitely generated free algebras such as $\mathsf{Reg}\,\mathsf{P},\mathsf{B}$, we can take $\top = (p_1 + \cdots + p_k)^*$. To reduce the Horn formula (12) to an equation, let $z = \top(s_1 + \cdots + s_n)\top$. Then z is the maximum element of the ideal generated by $s_1, \ldots, s_n$. Thus (12) is equivalent to the equation $s + z = t + z$.

References

[1] Ernie Cohen. Hypotheses in Kleene algebra. Technical Report TM-ARH-023814, Bellcore, 1993. `http://citeseer.nj.nec.com/1688.html`.

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

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

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

[6] 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.

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

[8] 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.