Kleene Algebra and Kleene Algebra with Tests

Part II

December 8, 2015

Today – Completeness and Complexity

- Introduction to KAT
- Encoding Hoare logic
- Completeness for the equational theory
- Completeness for the Hoare theory (reasoning under assumptions)
- Completeness and incompleteness results for PHL
- Complexity (PSPACE completeness)
- Typed KA and KAT and relation to type theory

Kleene Algebra with Tests (KAT)

Axioms of Boolean Algebra

$$a + (b + c) = (a + b) + c \qquad a(bc) = (ab)c$$

$$a + b = b + a \qquad ab = ba$$

$$a + 0 = a \qquad a1 = a$$

$$a + a = a \qquad aa = a$$

$$a(b + c) = ab + ac \qquad (a + b)c = ac + bc$$

$$a0 = 0 \qquad a + 1 = 1$$

$$\overline{a + b} = \overline{a}\,\overline{b} \qquad \overline{ab} = \overline{a} + \overline{b}$$

$$\overline{\overline{a}} = a$$

$(K, B, +, \cdot, ^*, ^-, 0, 1), \quad B \subseteq K$

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

- $p, q, r, \ldots$ range over K
- $a, b, c, \ldots$ range over B

$+, \cdot, 0, 1$ serve double duty

- applied to actions, denote choice, composition, fail, and skip, resp.
- applied to tests, denote disjunction, conjunction, falsity, and truth, resp.
- these usages do not conflict!

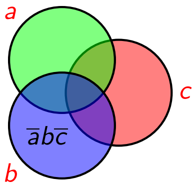
$$bc = b \wedge c \qquad\qquad b + c = b \vee c$$

Models of KAT

- Relational models
  - K = binary relations on a set X
  - B = subsets of the identity relation
- Trace models
  - K = sets of traces $s_0 p_0 s_1 p_1 s_2 \cdots s_{n-1} p_{n-1} s_n$
  - B = traces of length 0
- Language-theoretic models
  - K = sets of guarded strings over Σ, T
  - B = free Boolean algebra generated by T
- $n \times n$ matrices over K, B

Guarded Strings over Σ, T [Kaplan 69]

Σ action symbols $\qquad$ T test symbols



B = free Boolean algebra generated by T
At = atoms of $B = \{\alpha, \beta, \ldots\}$

E.g. if $T = \{a, b, c\}$, then $\overline{a}b\overline{c}$ is an atom

Guarded strings $\alpha_0 p_0 \alpha_1 p_1 \alpha_2 \cdots \alpha_{n-1} p_{n-1} \alpha_n \in (\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At}$

Guarded strings are the join-irreducible elements of the free KAT on generators Σ, T

Standard Interpretation of KAT

Regular sets of guarded strings over Σ, T

$$
\begin{aligned}
A + B &= A \cup B \\
AB &= \{x\alpha y \mid x\alpha \in A,\ \alpha y \in B\} \\
A^* &= \bigcup_{n \geq 0} A^n \quad = \quad A^0 \cup A^1 \cup A^2 \cup \cdots \\
1 &= \mathrm{At} \\
0 &= \varnothing
\end{aligned}
$$

- $p \in \Sigma$ interpreted as $\{\alpha p \beta \mid \alpha, \beta \in \mathrm{At}\}$
- $b \in T$ interpreted as $\{\alpha \mid \alpha \leq b\}$
- $\mathrm{GS}(e) = \{$guarded strings represented by $e\}$

Modeling While Programs

$$p; q \stackrel{\text{def}}{=} pq$$

$$\textbf{if } b \textbf{ then } p \textbf{ else } q \stackrel{\text{def}}{=} bp + \overline{b}q$$

$$\textbf{while } b \textbf{ do } p \stackrel{\text{def}}{=} (bp)^*\overline{b}$$

KAT Subsumes Hoare Logic

$$\begin{aligned}\{b\}\,p\,\{c\} &\stackrel{\text{def}}{\iff} bp \le pc \\ &\iff bp = bpc \\ &\iff bp\overline{c} = 0\end{aligned}$$

The Hoare while rule

$$\frac{\{bc\}\,p\,\{c\}}{\{c\}\ \textbf{while}\ b\ \textbf{do}\ p\,\{\overline{b}c\}}$$

becomes the universal Horn sentence

$$bcp\overline{c} = 0 \;\Rightarrow\; c(bp)^*\overline{b}\,\overline{\overline{b}c} = 0$$

Deductive Completeness and Complexity

- The regular sets of guarded strings over Σ, T form the free KAT on generators Σ, T
- KAT is deductively complete over relational and trace models
- Subsumes propositional Hoare logic (PHL)
- KAT is deductively complete for all relationally valid Hoare-style rules

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

  (PHL is not!)

- PSPACE-complete (thus no harder to decide than KA or PHL)

Automata with Tests

aka Automata on Guarded Strings

- A generalization of classical automata theory to include Booleans
- An ε-transition is really a 1-transition (i.e., an ordinary automaton with ε-transitions is an automaton with tests over the two-element Boolean algebra)
- Classical constructions of ordinary finite-state automata generalize readily
    - determinization
    - state minimization
    - Kleene's theorem

Deductive Completeness

The Equational Theory

We have defined several different but related classes of algebras:

- Kleene algebras (KA)
- star-continuous Kleene algebras (KA^*)
- closed semirings (CS)
- complete semirings or S-algebras (SA)
- relational models (Rel)
- trace models (Tr)
- language-theoretic models (Lan)
- Reg_Σ.

Will show: All these classes of models have the same equational theory over the signature $+$, $\cdot$, *, 0, 1 of Kleene algebra, and it is the same as the equational theory of the regular sets.

What are we talking about?

Let σ denote the signature $+$, $\cdot$, *, 0, 1 of Kleene algebra. A σ-algebra is any structure of signature σ. (Need not satisfy the axioms of Kleene algebra.)

Example: RExp_Σ can be regarded as a σ-algebra. The distinguished operations are defined syntactically; for example, $+$ takes regular expressions s and t and produces the regular expression $s + t$.

Homomorphisms and Interpretations

For σ-algebras C, C', a homomorphism from $C \to C'$ is a map $h : C \to C'$ that commutes with all the distinguished operations and constants of σ; that is, for all $x, y \in C$,

$$\begin{aligned} h(x+y) &= h(x)+h(y) \\ h(xy) &= h(x)\cdot h(y) \\ h(x^*) &= h(x)^* \\ h(0) &= 0 \\ h(1) &= 1. \end{aligned}$$

Operators and constants on the left-hand side are interpreted in C and on the right-hand side in C'.

An interpretation is a homomorphism with domain RExp_Σ. Interpretations are uniquely determined by their values on Σ.

Equational Theories

Let s, t be regular expressions and $I : \mathrm{RExp}_\Sigma \to C$ an interpretation.

We write $C, I \vDash s = t$ and say that $s = t$ holds under I and if $I(s) = I(t)$.

If $\mathcal{A}$ is a family of interpretations C, I, we write $\mathcal{A} \vDash s = t$ and say that $s = t$ holds in $\mathcal{A}$ if $C, I \vDash s = t$ for all $C, I \in \mathcal{A}$.

The equational theory of $\mathcal{A}$, denoted $\mathcal{E}(\mathcal{A})$, is the set of equations that hold in $\mathcal{A}$.

Equational Theories

Theorem

The following classes of algebras all have the same equational theory:

- *Kleene algebras* (KA)
- *star-continuous Kleene algebras* (KA^*)
- *closed semirings* (CS)
- *complete semirings or S-algebras* (SA)
- *relational models (Rel)*
- *trace models (Tr)*
- *language-theoretic models (Lan).*

Moreover, for $s, t \in \mathrm{RExp}_\Sigma$, $s = t$ is a member of this theory iff $R(s) = R(t)$, where $R : \mathrm{RExp}_\Sigma \to \mathrm{Reg}_\Sigma$ is the standard interpretation.

Equational Theories

Inclusions easy in one direction: since

$$\mathsf{KA} \supseteq \mathsf{KA}^* \supseteq \mathsf{CS} \supseteq \mathsf{SA} \supseteq \mathsf{Rel} \supseteq \mathsf{Tr} \supseteq \mathsf{Lan} \supseteq \{R\}$$

we have

$$\begin{aligned} \mathcal{E}(\mathsf{KA}) \subseteq \mathcal{E}(\mathsf{KA}^*) \subseteq \mathcal{E}(\mathsf{CS}) \subseteq \mathcal{E}(\mathsf{SA}) \subseteq \mathcal{E}(\mathsf{Rel}) \\ \subseteq \mathcal{E}(\mathsf{Tr}) \subseteq \mathcal{E}(\mathsf{Lan}) \subseteq \mathcal{E}(\{\mathcal{R}\}). \end{aligned}$$

Completeness of Star-Continuity

We have argued

$$\begin{aligned}\mathcal{E}(\mathsf{KA}) \;\subseteq\; \mathcal{E}(\mathsf{KA}^*) \;\subseteq\; \mathcal{E}(\mathsf{CS}) \;\subseteq\; \mathcal{E}(\mathsf{SA}) \;\subseteq\; \mathcal{E}(\mathsf{Rel})\\ \subseteq\; \mathcal{E}(\mathsf{Tr}) \;\subseteq\; \mathcal{E}(\mathsf{Lan}) \;\subseteq\; \mathcal{E}(\{\mathcal{R}\}).\end{aligned}$$

We now show that

$$\mathcal{E}(\{\mathcal{R}\}) \;\subseteq\; \mathcal{E}(\mathsf{KA}^*);$$

that is, if $\mathsf{RExp}_\Sigma, R \vDash s = t$, then $\mathsf{KA}^* \vDash s = t$. Thus

$$\begin{aligned}\mathcal{E}(\mathsf{KA}^*) \;=\; \mathcal{E}(\mathsf{CS}) \;=\; \mathcal{E}(\mathsf{SA}) \;=\; \mathcal{E}(\mathsf{Rel})\\ =\; \mathcal{E}(\mathsf{Tr}) \;=\; \mathcal{E}(\mathsf{Lan}) \;=\; \mathcal{E}(\{\mathcal{R}\}).\end{aligned}$$

(The proof for KA is harder.)

Completeness of Star-Continuity

Lemma

For any $s, t, u \in \mathrm{RExp}_\Sigma$*, the following holds in any star-continuous Kleene algebra* K*:*

$$stu \quad = \quad \sup_{x \in R(t)} sxu.$$

In other words, if K *is star-continuous, then under any interpretation* $I : \mathrm{RExp}_\Sigma \to K$*, the supremum of the set*

$$\{I(sxu) \mid x \in R(t)\}$$

exists and is equal to $I(stu)$*.*

Completeness of Star-Continuity

Proof: Induction on the structure of t. For the case *, we use the *-continuity axiom:

$$\begin{aligned}
st^*u &= \sup_{n\geq 0} st^n u \\
&= \sup_{n\geq 0} \sup_{x\in R(t^n)} sxu \\
&= \sup_{x \in \bigcup_{n\geq \mathbf{0}} R(t^n)} sxu \\
&= \sup_{x \in R(t^*)} sxu.
\end{aligned}$$

Completeness of Star-Continuity

Theorem

$\mathrm{KA}^* \vDash s = t$ *iff* $R(s) = R(t)$.

Proof.

$(\Rightarrow)$ is immediate, since Reg_Σ is a star-continuous Kleene algebra.
Conversely, by two applications of the Lemma, if $R(s) = R(t)$, then under any interpretation in any star-continuous Kleene algebra,

$$s = \sup_{x \in R(s)} x = \sup_{x \in R(t)} x = t.$$

$\square$

Free Algebras

Another way of saying this is that Reg_Σ is the free star-continuous Kleene algebra on generators Σ. The term free intuitively means that Reg_Σ is free from any equations except those that it is forced to satisfy in order to be a star-continuous Kleene algebra.

Formally, an algebra A of a class of algebras $\mathcal{C}$ of the same signature is said to be free on generators X for the class $\mathcal{C}$ if

- A is generated by X;
- any function h from X into another algebra $B \in \mathcal{C}$ extends to a homomorphism $\widehat{h} : A \to B$.

The extension is necessarily unique, since a homomorphism is completely determined by its action on a generating set.

Equivalently, every interpretation $I : \mathrm{RExp}_\Sigma \to K$, where $K \in \mathrm{KA}^*$, factors through R; that is, there exists a homomorphism $h : \mathrm{Reg}_\Sigma \to K$ such that $I = h \circ R$.

Completeness of KA

To show completeness of KA, we will encode some classical combinatorial constructions of the theory of finite automata algebraically:

- construction of a transition matrix representing a finite automaton equivalent to a given regular expression (Kleene 1956, Conway 1971)
- elimination of ε-transitions (Kuich and Salomaa 1986, Sakarovitch 1987)

We will add two other fundamental constructions:

- determinization of an automaton via the subset construction, and
- state minimization via equivalence modulo a Myhill-Nerode equivalence relation.

We then use the uniqueness of the minimal deterministic finite automaton to obtain completeness.

Finite Automata over a KA

A finite automaton over a KA K is represented by a triple $\mathcal{A} = (u, A, v)$, where $u, v \in \{0, 1\}^n$ and A is an $n \times n$ matrix over K for some n.

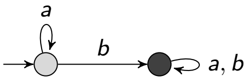
The states are the row and column indices. A start state is an index i for which $u(i) = 1$. A final state is an index i for which $v(i) = 1$. The matrix A is called the transition matrix.

The language accepted by $\mathcal{A}$ is the element $u^T A^* v \in K$.

For automata over the free KA on generators Σ, this is essentially equivalent to the classical combinatorial definition. A similar definition can be found in (Conway 1971).

Example

Consider the two-state automaton



Classically, this automaton accepts the set of strings over $\Sigma = \{a, b\}$ containing at least one occurrence of b. In our formalism,

$$\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} a & b \\ 0 & a+b \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right).$$

Modulo the axioms of KA,

$$\begin{aligned} & \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & a+b \end{bmatrix}^* \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ = \quad & \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a^* & a^* b(a+b)^* \\ 0 & (a+b)^* \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ = \quad & a^* b(a+b)^*. \end{aligned}$$

Simple Automata

Definition

Let $\mathcal{A} = (u, A, v)$ be an automaton over $\mathcal{F}_\Sigma$, the free Kleene algebra on free generators Σ. $\mathcal{A}$ is said to be simple if A can be expressed as a sum

$$A = J + \sum_{a \in \Sigma} a \cdot A_a$$

where J and the A_a are 0-1 matrices. In addition, $\mathcal{A}$ is said to be ε-free if J is the zero matrix. Finally, $\mathcal{A}$ is said to be deterministic if it is simple and ε-free, and u and all rows of A_a have exactly one 1.

The automaton of the previous example is simple, ε-free, and deterministic.

Completeness

The first lemma asserts that Kleene's theorem is a theorem of KA.

Lemma

For every regular expression s over Σ (or more accurately, its image in the free KA *under the canonical interpretation), there is a simple automaton (u, A, v) such that*

$$s \quad = \quad u^T A^* v$$

is a theorem of KA.

Proof: By induction on the structure of s.

Completeness

For $a \in \Sigma$, the automaton

$$\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right)$$

suffices, since

$$\begin{aligned} & \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}^* \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ = \quad & \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ = \quad & a. \end{aligned}$$

Completeness

For $s + t$, let $\mathcal{A} = (u, A, v)$ and $\mathcal{B} = (x, B, y)$ be automata such that

$$s = u^T A^* v \qquad\qquad t = x^T B^* y.$$

Consider the automaton with transition matrix

$$\left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right]$$

and start and final state vectors

$$\left[\begin{array}{c} u \\ \hline x \end{array}\right] \quad \text{and} \quad \left[\begin{array}{c} v \\ \hline y \end{array}\right],$$

respectively. (Corresponds to a disjoint union construction.)

Completeness

Then

$$\left[\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right]^* \quad = \quad \left[\begin{array}{c|c} A^* & 0 \\ \hline 0 & B^* \end{array}\right],$$

and

$$\begin{aligned} & \left[\begin{array}{c|c} u^T & x^T \end{array}\right] \cdot \left[\begin{array}{c|c} A^* & 0 \\ \hline 0 & B^* \end{array}\right] \cdot \left[\begin{array}{c} v \\ \hline y \end{array}\right] \\ & = \quad u^T A^* v + x^T B^* y \\ & = \quad s + t. \end{aligned}$$

Completeness

For st, let $\mathcal{A} = (u, A, v)$ and $\mathcal{B} = (x, B, y)$ be automata such that

$$s = u^T A^* v \qquad\qquad t = x^T B^* y.$$

Consider the automaton with transition matrix

$$\left[\begin{array}{c|c} A & vx^T \\ \hline 0 & B \end{array}\right]$$

and start and final state vectors

$$\left[\begin{array}{c} u \\ \hline 0 \end{array}\right] \quad \text{and} \quad \left[\begin{array}{c} 0 \\ \hline y \end{array}\right],$$

respectively. (Corresponds to forming the disjoint union and connecting the accept states of $\mathcal{A}$ to the start states of $\mathcal{B}$.)

Completeness

Then

$$\left[\begin{array}{c|c} A & vx^T \\ \hline 0 & B \end{array}\right]^* = \left[\begin{array}{c|c} A^* & A^* vx^T B^* \\ \hline 0 & B^* \end{array}\right],$$

and

$$\begin{aligned} \left[\begin{array}{c|c} u^T & 0 \end{array}\right] \cdot \left[\begin{array}{c|c} A^* & A^* vx^T B^* \\ \hline 0 & B^* \end{array}\right] \cdot \left[\begin{array}{c} 0 \\ \hline y \end{array}\right] \\ = \quad & u^T A^* vx^T B^* y \\ = \quad & st. \end{aligned}$$

Completeness

For s^*, let $\mathcal{A} = (u, A, v)$ be an automaton such that $s = u^T A^* v$. First produce an automaton equivalent to the expression ss^*. Consider the automaton

$$(u,\ A + vu^T,\ v).$$

This construction corresponds to the combinatorial construction of adding ε-transitions from the final states of $\mathcal{A}$ back to the start states. Using denesting and sliding,

$$\begin{aligned} u^T(A + vu^T)^* v &= u^T A^*(vu^T A^*)^* v \\ &= u^T A^* v(u^T A^* v)^* \\ &= ss^*. \end{aligned}$$

Once we have an automaton for ss^*, we can get an automaton for $s^* = 1 + ss^*$ by the construction for $+$ given above, using a trivial one-state automaton for 1.

Removing ε-Transitions

This construction models ε-closure.

Lemma

For every simple automaton (u, A, v) *over the free* KA, *there is a simple* ε*-free automaton* (s, B, t) *such that*

$$u^T A^* v \quad = \quad s^T B^* t.$$

Proof.

Write A as a sum $A = J + A'$ where J is 0-1 and A' is ε-free. Then

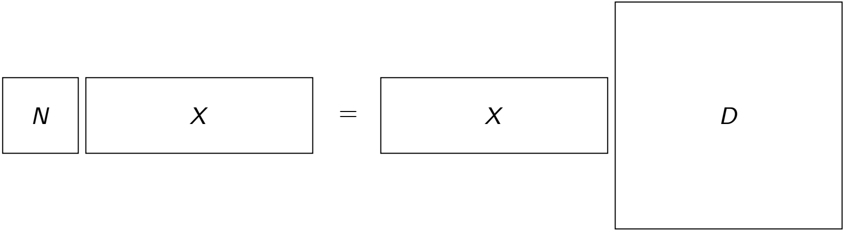
$$u^T A^* v \quad = \quad u^T (A' + J)^* v \quad = \quad u^T J^* (A' J^*)^* v$$

by denesting, so we can take

$$s^T = u^T J^* \qquad B = A' J^* \qquad t = v.$$

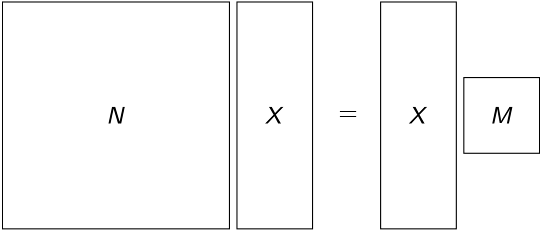
Then J^* is 0-1 and B is ε-free. $\square$

Determinization



$$NX = XD \quad \Rightarrow \quad N^*X = XD^*$$

Minimization via a Myhill–Nerode Relation



$$NX = XM \quad \Rightarrow \quad N^*X = XM^*$$

Isomorphic Automata

$$\boxed{P^{-1}}\,\boxed{A}\,\boxed{P} \quad = \quad \boxed{B}$$

$$(P^{-1}AP)^* = P^{-1}A^*P$$

Putting the Steps Together...

$$
\begin{tikzcd}
s \arrow[d, "\text{build automaton}"'] & & & t \arrow[d, "\text{build automaton}"] \\
N_s \arrow[d, "\text{determinize}"'] & & & N_t \arrow[d, "\text{determinize}"] \\
D_s \arrow[dr, "\text{minimize}"'] & & & D_t \arrow[dl, "\text{minimize}"] \\
& M_s \arrow[r, dash, "\text{permute}"'] & M_t &
\end{tikzcd}
$$

Completeness of KAT

Let $T = \{b_1, \ldots, b_n\}$ be the set of atomic tests. Let $\overline{T} = \{\overline{b}_1, \ldots, \overline{b}_n\}$. Represent atoms as $c_1 c_2 \cdots c_n$, where each $c_i \in \{b_i, \overline{b}_i\}$, $1 \leq i \leq n$. Then a guarded string can be regarded as a string in $(\Sigma \cup T \cup \overline{T})^*$.

Lemma

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

- KAT $\vDash p = \widehat{p}$,
- $G(\widehat{p}) = R(\widehat{p})$.

Theorem

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

Proof.

$(\Rightarrow)$ Immediate, since $\mathcal{G}$ is a KAT.
$(\Leftarrow)$ Suppose $G(p) = G(q)$. Since KAT $\vDash p = \widehat{p}$ and $\mathcal{G}$ is a KAT, $G(\widehat{p}) = G(\widehat{q})$. By the Lemma, $R(\widehat{p}) = R(\widehat{q})$. By the completeness of KA, KA $\models \widehat{p} = \widehat{q}$. By transitivity, KAT $\models p = q$. □

Eliminating Assumptions $s = 0$

An ideal of a KA or KAT is a subset $I \subseteq K$ such that

1. $0 \in I$
2. if $x, y \in I$, then $x + y \in I$
3. if $x \in I$ and $r \in K$, then xr and rx are in I
4. if $x \leq y$ and $y \in I$, then $x \in I$.

Given I, define $x \lesssim y$ if there exists $z \in I$ such that $x \leq y + z$, and define $x \approx y$ if $x \lesssim y$ and $y \lesssim x$. Equivalently, we could define $x \approx y$ if there exists $z \in I$ such that $x + z = y + z$, and $x \lesssim y$ if $x + y \approx y$.

$\lesssim$ is a preorder and $\approx$ is an equivalence relation. Let $[x]$ denote the $\approx$-equivalence class of x and let K/I denote the set of all $\approx$-equivalence classes. The relation $\lesssim$ is well-defined on K/I and is a partial order. Note also that $I = [0]$.

Eliminating Assumptions $s = 0$

Theorem

$\approx$ is a KAT congruence and K/I is a KAT. If $A \subseteq K$ and $I = <A>$, then K/I is initial among all homomorphic images of K satisfying $x = 0$ for all $x \in A$.

To show $ax \lesssim x \Rightarrow a^*x \lesssim x$:

If $ax \lesssim x$, then $ax \leq x + z$ for some $z \in I$. Then

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

Applying the same rule in K, we have $a^*(x + a^*z) \leq x + a^*z$, therefore $a^*x \leq x + a^*z$. Since $a^*z \in I$, $a^*x \lesssim x$.

Eliminating Assumptions $s = 0$

Corollary

Let $\Sigma = \{a_1, \ldots, a_n\}$*,* $u = (a_1 + \cdots + a_n)^*$*. Then* KAT $\models r = 0 \Rightarrow s = t$ *iff* KAT $\models s + uru = t + uru$*.*

Proof sketch: $\{y \mid y \leq uru\}$ is the ideal generated by r, so $s + uru = t + uru$ iff $s \approx t$ iff $s = t$ in $\mathcal{G}/I$.

Tomorrow

Automata and coalgebras!

Exercises

1. Prove that **while** b **do** $(p\,;$ **while** c **do** $q) =$
   if b **then** $(p\,;$ **while** $b + c$ **do if** c **then** q **else** $p)$ **else skip**.
2. Prove that the following KAT equations and inequalities are equivalent:
   1. $bp = bpc$
   2. $bp\overline{c} = 0$
   3. $bp \leq pc$
3. Prove that the expression $bp = pc$ is equivalent to the two Hoare partial correctness assertions $\{b\}\,p\,\{c\}$ and $\{\overline{b}\}\,p\,\{\overline{c}\}$.

Exercises

4. Let Σ be a finite alphabet and K a Kleene algebra. A power series in noncommuting variables Σ with coefficients in K is a map $\sigma : \Sigma^* \to K$. The power series σ is often written as a formal sum

$$\sum_{x \in \Sigma^*} \sigma(x) \cdot x.$$

The set of all such power series is denoted $K\langle\langle\Sigma\rangle\rangle$. Addition on $K\langle\langle\Sigma\rangle\rangle$ is defined pointwise, and multiplication is defined as follows:

$$(\sigma \cdot \tau)(x) \stackrel{\text{def}}{=} \sum_{x=yz} \sigma(y) \cdot \tau(z).$$

Define 0 and 1 appropriately and argue that $K\langle\langle\Sigma\rangle\rangle$ forms an idempotent semiring. Then define * as follows:

$$\sigma^*(x) \stackrel{\text{def}}{=} \sum_{x=y_1\cdots y_n} \sigma(\varepsilon)^*\sigma(y_1)\sigma(\varepsilon)^*\sigma(y_2)\sigma(\varepsilon)^* \cdots \sigma(\varepsilon)^*\sigma(y_n)\sigma(\varepsilon)^*$$

where ε is the null string and the sum is over all ways of expressing x as a product of strings $y_1, \ldots, y_n$. Show that $K\langle\langle\Sigma\rangle\rangle$ forms a KA.

Exercises

5. Strassen's matrix multiplication algorithm can be used to multiply two $n \times n$ matrices over a ring using approximately $n^{\log_2 7} = n^{2.807\cdots}$ multiplications in the underlying ring. The best known result of this form is by Coppersmith and Winograd, who achieve $n^{2.376\cdots}$. Show that over arbitrary semirings, n^3 multiplications are necessary in general. (*Hint*. Interpret over Reg_Σ, where $\Sigma = \{a_{ij}, b_{ij} \mid 1 \leq i, j \leq n\}$. What semiring expressions could possibly be equivalent to $\sum_{j=1}^{n} a_{ij} b_{jk}$?)