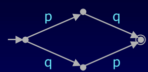
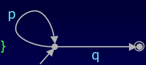
Kleene Algebra (KA)

is the algebra of regular expressions

pq + qp
{pq,qp}

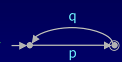


p*q
{q,pq,p^2q,p^3q, ...}

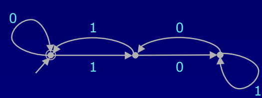


(p + q)* = (p*q)*p*
{all strings over p,q}

(pq)*p = p(qp)*
{p,pqp,pqpqp,...}



(0 + 1(01*0)*1)*
{multiples of 3 in binary}



Standard Interpretation

Regular sets over Σ

$A+B = A \cup B$
$AB = \{xy \mid x \in A, y \in B\}$
$A^* = \bigcup_{n\geq 0} A^n = A^0 \cup A^1 \cup A^2 \cup \ldots$
$1 = \{\varepsilon\}$
$0 = \emptyset$

$p \in \Sigma$ interpreted as $\{p\}$

Binary Relations

R, S binary relations on a set X

$R+S = R \cup S$
$RS = R \circ S = \{(u,v) \mid \exists w\ (u,w) \in R, (w,v) \in S\}$
R^* = reflexive transitive closure of R
$= \bigcup_{n\geq 0} R^n = R \cup R^1 \cup R^2 \cup \ldots$
1 = identity relation $= \{(u,u) \mid u \in X\}$
$0 = \emptyset$

Applications

- Automata and formal languages
  - regular expressions
- Relational algebra
- Program logic and verification
  - Dynamic Logic
  - program analysis
  - optimization
- Design and analysis of algorithms
  - shortest paths
  - connectivity

Fundamental Questions

- Axiomatization of equational theory
  [Salomaa 66]
- ...but no finite equational axiomatization
  [Redko 64]
- Complexity = PSPACE complete
  [(Stock+1)Meyer 74]

Axioms of KA [K91]

- K is an idempotent semiring under +, ·, 0, 1

$(p + q) + r = p + (q + r)$ $\quad (pq)r = p(qr)$
$p + q = q + p$ $\quad p1 = 1p = p$
$p + p = p$ $\quad p0 = 0p = 0$
$p + 0 = p$

$p(q + r) = pq + pr$
$(p + q)r = pr + qr$

- p*q = least x such that $q + px \leq x$
- qp* = least x such that $q + xp \leq x$

$$x \leq y \overset{def}{\leftrightarrow} x + y = y$$

This is a universal Horn axiomatization

- p^*q = least x such that $q + px \le x$
  $q + p(p^*q) \le p^*q$
  $q + px \le x \rightarrow p^*q \le x$
- qp^* = least x such that $q + xp \le x$
  $q + p(p^*q) \le p^*q$
  $q + px \le x \rightarrow p^*q \le x$

Every system of linear inequalities

$$a_{11}x_1 + \ldots + a_{n1}x_n + b_1 \le x_1$$
$$\vdots$$
$$a_{n1}x_1 + \ldots + a_{nn}x_n + b_n \le x_n$$

has a unique least solution

Alternative Characterizations of *

Complete semirings

$\sum_{i \in I} p_i$ = supremum of $\{p_i \mid i \in I\}$ with respect to $\le$

*-continuity

$$pq^*r = \sup_{n \ge 0} pq^n r$$

- infinitary
- same equational theory Eq(KA) = Eq(KA*)

Some Useful Properties

$1 + pp^* = 1 + p^*p = p^*$	
$p^*p^* = p^{**} = p^*$	
$(pq)^*p = p(qp)^*$	sliding
$(p^*q)^*p^* = (p + q)^*$	denesting
$px = xq \rightarrow p^*x = xq^*$	bisimulation
$qp = 0 \rightarrow (p + q)^* = p^*q^*$	loop distribution

Proof of the Sliding Rule

$(ab)^*a \le a(ba)^*$

$a + aba(ba)^* = a(1 + ba(ba)^*)$	distributivity
$= a(ba)^*$	$1 + pp^* = p^*$.
$a + aba(ba)^* \le a(ba)^*$	
$(ab)^*a \le a(ba)^*$	$q + px \le x \rightarrow p^*q \le x$

The reverse inequality $\ge$ is symmetric.

Equational Completeness [K91]

- Reg_Σ, the KA regular sets over Σ, is the free KA on generators Σ

$p \equiv q$ as regular sets
$\Leftrightarrow$
$p = q$ is a consequence of the KA axioms

- KA is complete over relational models

Eq(REL) = Eq(KA) = Eq(Reg_Σ)

Matrices over a KA

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

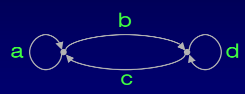
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

$$0 \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad 1 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* \stackrel{\text{def}}{=} \begin{pmatrix} (a+bd^*c)^* & (a+bd^*c)^*bd^* \\ (d+ca^*b)^*ca^* & (d+ca^*b)^* \end{pmatrix}$$

Matrices over a KA

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* \stackrel{\text{def}}{=} \begin{bmatrix} (a+bd^*c)^* & (a+bd^*c)^*bd^* \\ (d+ca^*b)^*ca^* & (d+ca^*b)^* \end{bmatrix}$$



Matrices over a KA

- Representation of finite automata
- Construction of regular expressions
- Solution of linear equations over a KA
- Connectivity and shortest path algorithms

Solution of Linear Inequalities

$$a_{11}x_1 + \ldots + a_{n1}x_n + b_1 \le x_1$$
$$\vdots$$
$$a_{n1}x_1 + \ldots + a_{nn}x_n + b_n \le x_n$$

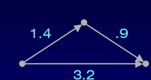
$$\begin{bmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \le \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Shortest Paths

The min,+ algebra

$R_+ \cup \{\infty\}$

$r + s$ = min r,s
rs = $r + s$
r^* = 0
0 = ∞
1 = 0
$\le$ = $\ge$

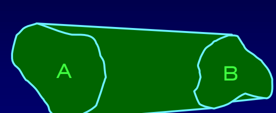


$$\begin{bmatrix} 0 & 1.4 & 3.2 \\ \infty & 0 & .9 \\ \infty & \infty & 0 \end{bmatrix}^* = \begin{bmatrix} 0 & 1.4 & 2.3 \\ \infty & 0 & .9 \\ \infty & \infty & 0 \end{bmatrix}$$

Other Models

Convex polyhedra [Iwano & Steiglitz 90]

$AB = \{ax + by \mid x \in A, y \in B\}$



A^* = convex hull of A

Kleene Algebra with Tests (KAT)

$(K, B, +, \cdot, ^*, \bar{\ }, 0, 1)$

- $(K, +, \cdot, ^*, 0, 1)$ is a Kleene algebra
- $(B, +, \cdot, \bar{\ }, 0, 1)$ is a Boolean algebra
- $B \subseteq K$

- p,q,r,... range over K
- a,b,c,... range over B

Kleene Algebra with Tests (KAT)

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

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

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

Models

- Relational models
  - K = binary relations on a set X
  - B = subsets of the identity relation
- Trace models
  - K = sets of traces $u_0 p_0 u_1 p_1 u_2 \dots u_{n-1} p_{n-1} u_n$
  - B = sets of traces of length 0
- Language-theoretic models
  - K = regular sets of guarded strings over Σ
  - B = atoms of a finite free Boolean algebra

Kripke Frames

$K = (K, m_K)$

$m_K : \{\text{atomic programs}\} \to 2^{K \times K}$

$m_K : \{\text{atomic tests}\} \to 2^K$

Relational Models

$K = (K, m_K)$

$m_K : \{\text{atomic programs}\} \to 2^{K \times K}$

$m_K : \{\text{atomic tests}\} \to 2^K$

$[p]_K = m_K(p)$, p atomic

$[b]_K = \{(u,u) \mid u \in m_K(b)\}$, b atomic

$[pq]_K = [p]_K \circ [q]_K = \{(u,v) \mid \exists w\ (u,w) \in [p]_K, (w,v) \in [q]_K\}$

$[p + q]_K = [p]_K \cup [q]_K$

$[p^*]_K$ = reflexive transitive closure of $[p]_K = \bigcup_{n\geq 0} [p]_K^n$

$[\bar{b}]_K = \{(u,u) \mid u \in K\} - [b]_K$

Trace Models

$K = (K, m_K)$

$m_K : \{\text{atomic programs}\} \to 2^{K \times K}$

$m_K : \{\text{atomic tests}\} \to 2^K$

A trace is a sequence

$x = u_0 p_0 u_1 p_1 u_2 \dots u_{n-1} p_{n-1} u_n$, $n \geq 0$, $(u_i, u_{i+1}) \in m_K(p_i)$

$\text{first}(x) = u_0$, $\text{last}(x) = u_n$

Product xy exists iff $\text{last}(x) = \text{first}(y)$

$(u_0 p_0 u_1 \dots u_{n-1} p_{n-1} u_n) \cdot (u_n p_n u_{n+1} \dots u_{m-1} p_{m-1} u_m)$

$= u_0 p_0 u_1 \dots p_{n-1} u_n p_n \dots u_{m-1} p_{m-1} u_m$

Trace Models

$K = (K, m_K)$

$m_K : \{\text{atomic programs}\} \to 2^{K \times K}$

$m_K : \{\text{atomic tests}\} \to 2^K$

$[[p]]_K = \{upv \mid (u,v) \in m_K(p)\}$, p atomic

$[[b]]_K = m_K(b)$, b atomic

$[[pq]]_K = [[p]]_K \cdot [[q]]_K = \{xy \mid x \in [[p]]_K, y \in [[q]]_K, xy \text{ exists}\}$

$[[p + q]]_K = [[p]]_K \cup [[q]]_K$

$[[p^*]]_K = \bigcup_{n\geq 0} [[p]]_K^n$

$[[\bar{b}]]_K = K - [[b]]_K$

Guarded Strings [Kaplan 69]

P atomic programs B atomic tests

$\alpha, \beta, \ldots$ atoms (minimal nonzero elements) of the free Boolean algebra on generators B

e.g. if B = $\{b_1, \ldots, b_6\}$, then $\bar{b}_1 b_2 b_3 \bar{b}_4 \bar{b}_5 b_6$ is an atom

guarded strings $\alpha_0 p_0 \alpha_1 p_1 \alpha_2 p_2 \alpha_3 \ldots \alpha_{n-1} p_{n-1} \alpha_n$

$A+B = A \cup B$

$AB = \{x\alpha y \mid x\alpha \in A, \alpha y \in B\}$

$A^* = \bigcup_{n \geq 0} A^n$

$1 = \{\text{atoms}\}$

$0 = \varnothing$

Theorem [Kozen & Smith 96]

The family of regular sets of guarded strings over P,B is the free KAT on generators P,B.

Corollary

KAT is complete over relational models.

Eq(GS) = Eq(KAT) = Eq(KAT*) = Eq(REL)

Matrices over a KAT

The n x n matrices over a KAT (K,B) forms a KAT (K',B')

B' = diagonal matrices over B

Modeling Programs

same as in PDL [Fischer & Ladner 79]

p;q	≡	pq
if b then p else q	≡	$bp + \bar{b}q$
while b do p	≡	$(bp)^*\bar{b}$

Propositional Hoare Logic (PHL)

Hoare Logic without the assignment rule

{b[x/t]} x := t {b}

Is a given rule

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

- a logical consequence of the composition, conditional, while, and weakening rules?
- relationally valid?

KAT subsumes PHL

{b}p{c} modeled by bp = bpc or $bp\bar{c} = 0$

[Manes & Arbib 86]

$bp = bpc \quad \Leftrightarrow \quad bp\bar{c} = 0$

$(\Rightarrow) \quad bp\bar{c} = bpc\bar{c} = bp0 = 0$

$(\Leftarrow) \quad bp = bp1 = bp(c+\bar{c}) = bpc + bp\bar{c} = bpc + 0 = bpc$

$$\frac{\{b\}p\{c\},\ \{c\}q\{d\}}{\{b\}pq\{d\}}$$

composition rule

$\equiv \ bp\bar{c} = 0 \wedge cq\bar{d} = 0 \ \rightarrow \ bpq\bar{d} = 0$

$$\frac{\{bc\}p\{d\},\ \{\bar{b}c\}q\{d\}}{\{c\}\text{if } b \text{ then } p \text{ else } q\{d\}}$$

conditional rule

$\equiv \ bcp\bar{d} = 0 \wedge \bar{b}cq\bar{d} = 0 \ \rightarrow \ c(bp+\bar{b}q)\bar{d} = 0$

$$\frac{\{bc\}p\{c\}}{\{c\}\text{while } b \text{ do } p\{\bar{b}c\}}$$

while rule

$\equiv \ bcp\bar{c} = 0 \ \rightarrow \ c(bp)^*\bar{b}\,\overline{\bar{b}c} = 0$

Theorem

These are all theorems of KAT

Completeness Theorem [K 99]

All relationally valid rules of the form

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

are derivable in KAT (not so for PHL)

Counterexample

$$\frac{\{c\}\text{if } b \text{ then } p \text{ else } p\{c\}}{\{c\}p\{c\}}$$

is trivially unprovable in Hoare Logic, but

$c(bp + \bar{b}p)\bar{c} = 0 \ \rightarrow \ cp\bar{c} = 0$

is easily provable in KAT

Hoare formulas

$p_1 = 0 \wedge p_2 = 0 \wedge \ldots \wedge p_n = 0 \ \rightarrow \ q = r$

Theorem

KAT is complete for the Hoare theory of relational algebras

... not for the Horn theory!

Counterexample: $p \leq 1 \ \rightarrow \ p^2 = p$

Complexity of KAT and PHL

Theorem [Cohen 94]

The Hoare theory of KA (Horn formulas with premises $p = 0$) is PSPACE-complete

Theorem [Cohen, Kozen & Smith 96]

The Hoare theory of KAT is PSPACE-complete

Theorem

PHL is PSPACE-complete

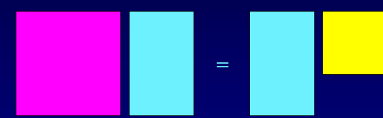
Typed KAT

- Extend the type discipline of KA to KAT
  test ⇒ typecast or coercion operator
- Hoare Logic is subsumed by the type discipline of typed KAT

Thus Hoare-style reasoning with partial correctness assertions is just typechecking

Typed Kleene Algebra [K 98]

$ax = xb \rightarrow a^*x = xb^*$



Typed Kleene Algebra

$$\frac{p:b \to c \quad q:b \to c}{p + q:b \to c} \qquad \frac{p:b \to c \quad q:c \to d}{pq:b \to d}$$

$$0:b \to c \qquad 1:b \to b \qquad \frac{p:b \to b}{p^*:b \to b}$$

Typed KAT

$$\frac{p:b \to c \quad q:b \to c}{p + q:b \to c} \qquad \frac{p:b \to c \quad q:c \to d}{pq:b \to d}$$

~~$0:b \to c$~~ ~~$1:b \to b$~~ $$\frac{p:b \to b}{p^*:b \to b}$$

$c:b \to bc$

typecast or coercion

Typecast operator $c:b \to bc$

```
class Super {}
class Sub extends Super {}
...
void f(Super y) {
     Sub x = null;
     try {
          x = (Sub)y;
     } catch (ClassCastException e) {}
}
...
f(new Sub());
```

Typed KAT and Hoare Logic

$\{b\}p\{c\} \equiv p:b \to c$

$$\frac{\{b \wedge c\}p\{c\}}{\{c\}\text{while } b \text{ do } p\{\neg b \wedge c\}} \quad \Leftrightarrow \quad \frac{p{:}bc \to c}{(bp)^*\bar{b}{:}c \to \bar{b}c}$$

$$\dfrac{\dfrac{\dfrac{b{:}c \to bc \qquad p{:}bc \to c}{bp{:}c \to c}}{(bp)^*{:}c \to c} \qquad \bar{b}{:}c \to \bar{b}c}{(bp)^*\bar{b}{:}c \to \bar{b}c}$$

SKAT = Schematic KAT

```
x := s ; y := t
  ≡ y := t[x/s] ; x := s      (y ∉ Var(s))

x := s ; y := t
  ≡ x := s ; y := t[x/s]      (x ∉ Var(s))

x := s ; x := t  ≡  x := t[x/s]

x := t ; b  ≡  b[x/t] ; x := t

x := x  ≡  1
```

Special Cases

```
x := s ; y := t
  ≡ y := t ; x := s     (x ∉ Var(t), y ∉ Var(s))

x := t ; b  ≡  b ; x := t      (x ∉ Var(b))

x := s  ≡  x := s ; x = s      (x ∉ Var(s))

x = s  ≡  x = s ; x := s
```

Encoding the Hoare Assignment Axiom

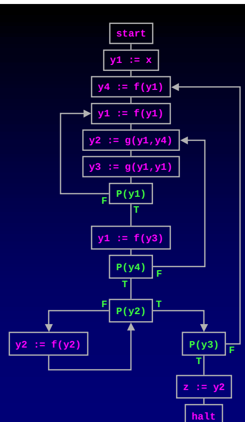
x := t ; b ≡ b[x/t] ; x := t

is equivalent to

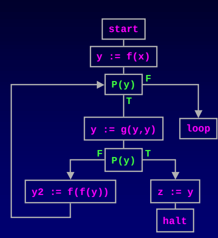
{b[x/t]} x := t {b}   {$\bar{b}$[x/t]} x := t {$\bar{b}$}

$bp = pc \;\leftrightarrow\; \bar{b}p = p\bar{c} \;\leftrightarrow\; bp\bar{c} + \bar{b}pc = 0$

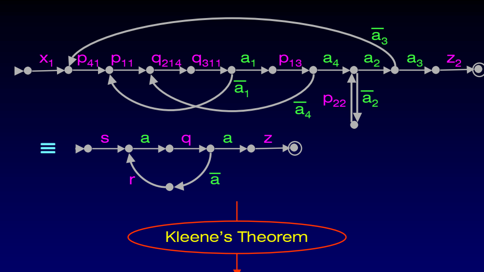
Scheme Equivalence



≡



Example of Paterson from [Manna 74]



$x_1p_{41}p_{11}q_{214}q_{311}(\bar{a}_1p_{11}q_{214}q_{311})^*a_1p_{13}$
$((\bar{a}_4+a_4(\bar{a}_2p_{22})^*a_2\bar{a}_3p_{41}p_{11})\,q_{214}q_{311}(\bar{a}_1p_{11}q_{214}q_{311})^*a_1p_{13})^*$
$a_4(\bar{a}_2p_{22})^*a_2a_3z_2z$

$\equiv saq(\bar{a}raq)^*az$