Kleene Algebra

A *Kleene algebra* is an algebraic structure $(K, +, \cdot, {}^*, 0, 1)$ satisfying (1)–(15) below. We omit the operator $\cdot$ from expressions, writing pq for $p \cdot q$. The precedence of the operators is ${}^* > \cdot > +$; thus $p + qr^*$ should be parsed as $p + (q(r^*))$.

$$\begin{aligned}
p + (q + r) &= (p + q) + r && (1)\\
p + q &= q + p && (2)\\
p + 0 &= p && (3)\\
p + p &= p && (4)\\
p(qr) &= (pq)r && (5)\\
1p &= p && (6)\\
p1 &= p && (7)\\
p(q + r) &= pq + pr && (8)\\
(p + q)r &= pr + qr && (9)\\
0p &= 0 && (10)\\
p0 &= 0 && (11)\\
1 + pp^* &= p^* && (12)\\
1 + p^*p &= p^* && (13)\\
q + pr \le r \quad &\rightarrow \quad p^*q \le r && (14)\\
q + rp \le r \quad &\rightarrow \quad qp^* \le r && (15)
\end{aligned}$$

where $\le$ refers to the natural partial order on K:

$$p \le q \quad \leftrightarrow \quad p + q = q.$$

Instead of (14) and (15), we might take

$$\begin{aligned}
pr \le r \quad &\rightarrow \quad p^*r \le r && (16)\\
rp \le r \quad &\rightarrow \quad rp^* \le r. && (17)
\end{aligned}$$

which are equivalent to (14) and (15) in the presence of the other axioms.

The following are some typical identities that hold in all Kleene algebras:

$$\begin{aligned}
(p^*q)^*p^* &= (p + q)^* && (18)\\
p(qp)^* &= (pq)^*p && (19)\\
(pq)^* &= 1 + p(qp)^*q && (20)\\
p^* &= (pp)^*(1 + p). && (21)
\end{aligned}$$

All the operators are monotone with respect to $\le$. In other words, if $p \le q$, then $pr \le qr$, $rp \le rq$, $p + r \le q + r$, and $p^* \le q^*$ for any r.

Kleene Algebra with Tests

A *Kleene algebras with tests* (KAT) is just a Kleene algebra with an embedded Boolean subalgebra. That is, it is a two-sorted structure $(K, B, +, \cdot, ^*, ^-, 0, 1)$ such that

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

KAT and Hoare Logic

The **while** program constructs are encoded in KAT as follows:

$$
\begin{aligned}
p \,;\, q &\stackrel{\text{def}}{=} pq && (22)\\
\textbf{if } b \textbf{ then } p \textbf{ else } q &\stackrel{\text{def}}{=} bp + \overline{b}q && (23)\\
\textbf{while } b \textbf{ do } p &\stackrel{\text{def}}{=} (bp)^*\overline{b}. && (24)
\end{aligned}
$$

The partial correctness assertion $\{b\}\,p\,\{c\}$ is encoded in KAT by the equation

$$bp\overline{c} \;=\; 0. \tag{25}$$

Intuitively, this says that the program p with preguard b and postguard $\overline{c}$ has no halting execution. An equivalent formulation is

$$bp \;=\; bpc, \tag{26}$$

which says intuitively that testing c after executing bp is always redundant.

The equivalence of (25) and (26) is shown as follows. Assuming (25),

$$
\begin{aligned}
bp &= bp(c + \overline{c}) && \text{by the axiom } a1 = a \text{ and Boolean algebra}\\
&= bpc + bp\overline{c} && \text{by distributivity}\\
&= bpc && \text{by (25) and the axiom } a + 0 = a.
\end{aligned}
$$

Conversely, assuming (26),

$$
\begin{aligned}
bp\overline{c} &= bpc\overline{c} && \text{by (26)}\\
&= bp0 && \text{by associativity and Boolean algebra}\\
&= 0 && \text{by the axiom } a0 = 0.
\end{aligned}
$$

The equation (26) is equivalent to the inequality $bp \leq bpc$, since the reverse inequality is a theorem of KAT; it follows immediately from the axiom $c \leq 1$ of Boolean algebra and monotonicity of multiplication.

The Hoare **while** rule

$$\frac{\{b \wedge c\}\; p\; \{c\}}{\{c\}\; \textbf{while } b \textbf{ do } p\; \{\neg b \wedge c\}} \tag{27}$$

is encoded in KAT as

$$bcp = bcpc \quad \rightarrow \quad c(bp)^*\overline{b} = c(bp)^*\overline{b}\,\overline{b}c \tag{28}$$

To prove (28) in KAT, by trivial simplifications it suffices to show

$$cbp \leq cbpc \quad \rightarrow \quad c(bp)^* \leq c(bp)^*c,$$

or, taking $q = bp$,

$$cq \leq cqc \quad \rightarrow \quad cq^* \leq cq^*c. \tag{29}$$

Assume the left-hand side of (29). By (15), to conclude the right-hand side of (29), we need only show

$$c + cq^*cq \quad \leq \quad cq^*c.$$

But

$$\begin{array}{rcll}
c + cq^*cq & \leq & c + cq^*cqc & \text{by the left-hand side of (29) and monotonicity} \\
& \leq & c1c + cq^*cqc & \text{by Boolean algebra} \\
& \leq & c(1 + q^*cq)c & \text{by distributivity on both sides} \\
& \leq & c(1 + q^*q)c & \text{by monotonicity} \\
& \leq & cq^*c & \text{by (13).}
\end{array}$$