Kleene Algebra

$$(x+y)+z = x+(y+z) \qquad (xy)z = x(yz)$$
$$x+y = y+x \qquad x1 = 1x = x$$
$$x+x = x$$
$$x+0 = 0+x = x$$

$$x(y+z) = xy+xz \qquad x0 = 0x = 0$$
$$(x+y)z = xz+yz$$

$$1+xx^* \le x^* \qquad 1+x^*x \le x^*$$
$$b+ax \le x \to a^*b \le x \qquad b+xa \le x \to ba^* \le x$$

$$x \le y \quad \overset{\text{def}}{\iff} \quad x+y = y$$

Kleene Algebra with Tests

= Kleene algebra with embedded Boolean subalgebra

Some Theorems of Kleene Algebra

$$(x+y)^* = x^*(yx^*)^*$$

$$x(yx)^* = (xy)^*x$$

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

$$yx = 0 \;\rightarrow\; (x+y)^* = x^*y^*$$

A Classical System for Equational Horn Logic

$s, t, \ldots$	terms over signature $\Sigma = \{f, g, \ldots\}$, variables $X = \{x, y, \ldots\}$
$d, e, \ldots$	equations $s = t$
$\varphi, \psi, \ldots$	equational implications (Horn formulas) $e_1 \to \cdots \to e_n \to e$
$e_1, \ldots, e_n \vdash \varphi$	task
σ	substitution $\sigma : X \to \{\text{terms}\}$

E = axioms of equational logic ("system axioms")

$$x = x$$

$$x = y \to y = x$$

$$x = y \to y = z \to x = z$$

$$x_1 = y_1 \to \cdots \to x_n = y_n \to f x_1 \ldots x_n = f y_1 \ldots y_n, \quad f \in \Sigma \ n\text{-ary}$$

Δ = "user axioms"

Rules

$$\vdash \sigma(\varphi), \quad \varphi \in \Delta \cup E \qquad\qquad e \vdash e$$

$$\frac{A \vdash \varphi}{A, e \vdash \varphi} \qquad\qquad \frac{A, e \vdash \varphi}{A \vdash e \to \varphi}$$

$$\frac{A \vdash e \quad A \vdash e \to \varphi}{A \vdash \varphi}$$

permutations of A

Annotated Rules

$$
\begin{aligned}
\mathsf{ref} &: \forall x \;\; x = x \\
\mathsf{sym} &: \forall x \;\; \forall y \;\; x = y \to y = x \\
\mathsf{trans} &: \forall x \;\; \forall y \;\; \forall z \;\; x = y \to y = z \to x = z \\
\mathsf{cong}_f &: \forall \overline{x} \;\; \forall \overline{y} \;\; x_1 = y_1 \to \cdots \to x_n = y_n \to f x_1 \ldots x_n = f y_1 \ldots y_n \\
\mathsf{axiom}_\varphi &: \varphi, \quad \varphi \in \Delta
\end{aligned}
$$

$$\vdash \mathsf{axiom}_\varphi\, \sigma : \sigma(\varphi), \quad \varphi \in \Delta \cup E$$

$$p : e \vdash p : e$$

$$\frac{A \vdash \tau : \varphi}{A, p : e \vdash \tau : \varphi}$$

$$\frac{A, p : e \vdash \tau : \varphi}{A \vdash \lambda p.\tau : e \to \varphi}$$

$$\frac{A \vdash \rho : e \quad A \vdash \tau : e \to \varphi}{A \vdash \tau\rho : \varphi}$$

Example $x = fx \to x = f(fx)$

$$\dfrac{x = fx \vdash x = fx \qquad \dfrac{\vdash x = fx \to fx = f(fx)}{x = fx \vdash x = fx \to fx = f(fx)}}{x = fx \vdash fx = f(fx)}$$

$$\dfrac{x = fx \vdash x = fx \qquad \dfrac{\vdash x = fx \to fx = f(fx) \to x = f(fx)}{x = fx \vdash x = fx \to fx = f(fx) \to x = f(fx)}}{x = fx \vdash fx = f(fx) \to x = f(fx)}$$

$$\dfrac{\dfrac{x = fx \vdash fx = f(fx) \to x = f(fx) \qquad x = fx \vdash fx = f(fx)}{x = fx \vdash x = f(fx)}}{\vdash x = fx \to x = f(fx)}$$

$\lambda p.(\mathsf{trans}\ x\ (fx)\ (f(fx))\ p\ (\mathsf{cong}_f\ x\ (fx)\ p)) : x = fx \to x = f(fx)$

Observation Substitution instances of theorems are theorems

- usually handled by admissible rule

$$\frac{A \vdash \varphi}{A[x/t] \vdash \varphi[x/t]}$$

- alternatively, can introduce $\forall$

Formulas (types)

Individual variables $x, y, \ldots$

Individual terms $s, t, \ldots$ $\quad t ::= x \mid f t_1 \ldots t_n,\ f \in \Sigma\ n$-ary

Equations $d, e, \ldots$ $\quad s = t$

Formulas $\varphi, \psi, \ldots$ $\quad \varphi ::= e \mid e \to \varphi \mid \forall x\ \varphi$

Restriction to universal Horn formulas $\forall x_1\ \ldots\ \forall x_n\ \ e_1 \to \cdots \to e_n \to e$
enforced by type system

Proof terms

Proof variables $p, q, r, \ldots$

Proof terms $\pi, \rho, \tau, \ldots$ $\quad \pi ::= \mathsf{ref} \mid \mathsf{sym} \mid \mathsf{trans} \mid \mathsf{cong}_f,\ f \in \Sigma \mid \mathsf{axiom}_\varphi,\ \ \varphi \in \Delta$
$\quad \mid \pi\ \tau \mid \pi\ t \mid \lambda p.\tau \mid \lambda x.\tau \mid \mathsf{pub}\ \tau$

Universal Horn formulas = no λx occurs in the scope of a λp

enforced by type system

$\forall x\ \ x = x$

$\forall x\, \forall y\ \ x = y \to y = x$

$\forall x\, \forall y\, \forall z\ \ x = y \to y = z \to x = z$

$\forall \overline{x}\, \forall \overline{y}\ \ x_1 = y_1 \to \ldots \to x_n = y_n \to f x_1 \ldots x_n = f y_1 \ldots y_n, \quad f \in \Sigma$

$\varphi, \quad \varphi \in \Delta$

$$\frac{\mathfrak{L}\ ;\ A \vdash \varphi}{\mathfrak{L}\ ;\ A, e \vdash \varphi} \qquad \frac{\mathfrak{L}}{\mathfrak{L}\ ;\ e \vdash e}$$

$$\frac{\mathfrak{L}\ ;\ A \vdash e \to \varphi\ ;\ A \vdash e}{\mathfrak{L}\ ;\ A \vdash \varphi} \qquad \frac{\mathfrak{L}\ ;\ A, e \vdash \varphi}{\mathfrak{L}\ ;\ A \vdash e \to \varphi}$$

$$\frac{\mathfrak{L}\ ;\ \vdash \varphi}{\mathfrak{L}\ ;\ \forall \overline{x}\, \varphi}\ \text{(publish)} \qquad \frac{\mathfrak{L}\ ;\ \forall \overline{x}\, \varphi}{\mathfrak{L}\ ;\ \forall \overline{x}\, \varphi\ ;\ \vdash \varphi[\overline{x}/\overline{t}]}\ \text{(cite)}$$

$$\frac{\mathfrak{L}\ ;\ \varphi}{\mathfrak{L}}\ \text{(forget)}$$

$$
\begin{aligned}
\mathsf{ref} &: \forall x \;\; x = x \\
\mathsf{sym} &: \forall x \;\; \forall y \;\; x = y \to y = x \\
\mathsf{trans} &: \forall x \;\; \forall y \;\; \forall z \;\; x = y \to y = z \to x = z \\
\mathsf{cong}_f &: \forall \overline{x} \;\; \forall \overline{y} \;\; x_1 = y_1 \to \cdots \to x_n = y_n \to f x_1 \ldots x_n = f y_1 \ldots y_n \\
\mathsf{axiom}_\varphi &: \varphi, \quad \varphi \in \Delta
\end{aligned}
$$

$$\frac{\mathfrak{L}\ ;\ A \vdash \tau : \varphi}{\mathfrak{L}\ ;\ A, p : e \vdash \tau : \varphi} \qquad \frac{\mathfrak{L}}{\mathfrak{L}\ ;\ p : e \vdash p : e}$$

$$\frac{\mathfrak{L}\ ;\ A \vdash \rho : e\ ;\ A \vdash \tau : e \to \varphi}{\mathfrak{L}\ ;\ A \vdash \tau\rho : \varphi} \qquad \frac{\mathfrak{L}\ ;\ A, p : e \vdash \tau : \varphi}{\mathfrak{L}\ ;\ A \vdash \lambda p.\tau : e \to \varphi}$$

$$\frac{\mathfrak{L}\ ;\ \vdash \tau : \varphi}{\mathfrak{L}\ ;\ \mathsf{pub}\ \lambda\overline{x}.\tau : \forall\overline{x}\ \varphi}\ \text{(publish)} \qquad \frac{\mathfrak{L}\ ;\ \pi : \forall\overline{x}\ \varphi}{\mathfrak{L}\ ;\ \pi : \forall\overline{x}\ \varphi\ ;\ \vdash \pi\ \overline{t} : \varphi[\overline{x}/\overline{t}]}\ \text{(cite)}$$

$$\frac{\mathfrak{L}\ ;\ \mathsf{pub}\ \pi : \varphi}{\mathfrak{L}[\mathsf{pub}\ \pi/\pi]}\ \text{(forget)}$$

Publication

1. forms the universal closure of $\tau : \varphi$

   - in φ, binds all free individual variables with $\forall x_1 \ldots \forall x_n$ in some order (thus published theorems are always closed universal formulas)

   - in τ, binds with $\lambda x_1 \ldots \lambda x_n$ in the same order

2. wraps $\lambda x_1 \ldots \lambda x_n.\tau$ with pub to get *citation token* $\mathsf{pub}\ \lambda x_1 \ldots \lambda x_n.\tau$

   - polymorphic constant $\mathsf{pub} : \varphi \to \varphi$ inhibits β-reduction without altering type

   - $\mathsf{pub}\ \pi$ is a “short” abbreviation for π—interchangeable in proofs

   - avoids namespace management issues

Citation

- without pub
  - $(\lambda x.\lambda y.\lambda z.\tau)\ s\ t\ u \quad \rightarrow \quad \tau[x/s, y/t, z/u]$
  - $\dfrac{\lambda x.\lambda y.\lambda z.\tau : \forall x\ \forall y\ \forall z\ \ \varphi}{\tau[x/s, y/t, z/u] : \varphi}$
- with pub
  - $\mathsf{pub}\ (\lambda x.\lambda y.\lambda z.\tau)\ s\ t\ u$ is in normal form
  - $\dfrac{\lambda x.\lambda y.\lambda z.\tau : \forall x\ \forall y\ \forall z\ \ \varphi}{\mathsf{pub}\ (\lambda x.\lambda y.\lambda z.\tau)\ s\ t\ u : \varphi}$

Two ways to prove $\forall x \;\; gx = f(gx) \to gx = f(f(gx))$

1. Prove it directly—gives

   $\textsf{pub}\ \lambda x.\lambda p.(\textsf{trans}\ (gx)\ (f(gx))\ (f(f(gx)))\ p\ (\textsf{cong}_f\ (gx)\ (f(gx))\ p))$

2. Prove $\forall y \;\; y = fy \to y = f(fy)$; cite with $[y/gx]$; publish

   - proof of $\forall y \;\; y = fy \to y = f(fy)$ gives

     $\textsf{pub}\ \lambda y.\lambda p.(\textsf{trans}\ y\ (fy)\ (f(fy))\ p\ (\textsf{cong}_f\ y\ (fy)\ p))$

   - citation with $[y/gx]$ gives

     $\textsf{pub}\ \lambda y.\lambda p.(\textsf{trans}\ y\ (fy)\ (f(fy))\ p\ (\textsf{cong}_f\ y\ (fy)\ p))\ (gx)$

   - publication gives

     $\textsf{pub}\ \lambda x.(\textsf{pub}\ \lambda y.\lambda p.(\textsf{trans}\ y\ (fy)\ (f(fy))\ p\ (\textsf{cong}_f\ y\ (fy)\ p))\ (gx))$

Now forgetting $\forall y \;\; y = fy \to y = f(fy)$ after 2 gives the same as 1:

$$\begin{aligned}&\textsf{pub}\ \lambda x.(\lambda y.\lambda p.(\textsf{trans}\ y\ (fy)\ (f(fy))\ p\ (\textsf{cong}_f\ y\ (fy)\ p))\ (gx))\\ \to\quad &\textsf{pub}\ \lambda x.\lambda p.(\textsf{trans}\ (gx)\ (f(gx))\ (f(f(gx)))\ p\ (\textsf{cong}_f\ (gx)\ (f(gx))\ p))\end{aligned}$$

$$\frac{\mathfrak{L}\ ;\ A \vdash \tau : e}{\mathfrak{L}\ ;\ A,\ p : d \vdash \tau : e}$$

$$\frac{\mathfrak{L}}{\mathfrak{L}\ ;\ p : e \vdash p : e}$$

(publish) $$\frac{\mathfrak{L}\ ;\ p_1 : e_1, \ldots, p_n : e_n \vdash \tau : e}{\mathfrak{L}\ ;\ \mathsf{pub}\ \lambda\overline{x}.\lambda p_1 \ldots \lambda p_n.\tau : \forall\overline{x}\ e_1 \to \cdots \to e_n \to e}$$

(cite) $$\frac{\mathfrak{L}\ ;\ \pi : \varphi\ ;\ A \vdash \tau_1 : e_1[\overline{x}/\overline{t}]\ ;\ \ldots\ ;\ A \vdash \tau_n : e_n[\overline{x}/\overline{t}]}{\mathfrak{L}\ ;\ \pi : \varphi\ ;\ A \vdash \pi\ \overline{t}\ \tau_1 \cdots \tau_n : e[\overline{x}/\overline{t}]}$$

(forget) $$\frac{\mathfrak{L}\ ;\ \mathsf{pub}\ \pi : \varphi}{\mathfrak{L}[\mathsf{pub}\ \pi/\pi]}$$

where in (cite), φ is $\forall\overline{x}\ \ e_1 \to \cdots \to e_n \to e$.

Ideas for Things to Do

1. Extend to 1st order, higher order logics

2. Identify generalizations of existing arguments by CSE on proof terms [Mitchell et al. 86, Kolbe and Walther 94, Melis and Schairer 98]