Separation Logic

Heaps, $h : Addr \xrightarrow[fin]{} Val$

(Take $Addr = Val = \mathbb{N}$.)

Assertions, P, Q, R, denote sets of heaps.

$$emp\ h \stackrel{def}{=} h = \emptyset$$

$$(x \mapsto y)\ h \stackrel{def}{=} h = \{x \mapsto y\} \stackrel{def}{=} dom(h) = \{x\} \wedge h(x) = y$$

$$(P * Q)\ h \stackrel{def}{=} \exists h_1 h_2.\ P\ h_1 \wedge Q\ h_2 \wedge h = h_1 \uplus h_2$$

star, separating conjunction

i.e. $h = h_1 \cup h_2$ $\wedge\ dom(h_1) \cap dom(h_2) = \emptyset$

$$(P \mathrel{-\!\!*} Q)\ h \stackrel{def}{=} \forall h'.\ P\ h' \wedge dom(h) \cap dom(h') = \emptyset \Rightarrow Q(h \cup h')$$

magic wand, separating implication, "toilet brush"

$$(P \wedge Q)\ h \stackrel{def}{=} P\ h \wedge Q\ h$$
($\vee$, $\Rightarrow$, ⋮)

$$(\neg P)\ h \stackrel{def}{=} \neg P\ h$$

$$(x = y)\ h \stackrel{def}{=} x = y$$

other logical operators have the standard semantics.

Derived Assertions

- $x \mapsto y, z \stackrel{def}{=} x \mapsto y * x+1 \mapsto z$ (Assuming $Addr = \mathbb{N}$)
- $x \hookrightarrow y \stackrel{def}{=} x \mapsto y * true$
  - $(x \hookrightarrow y)\ h \iff h(x) = y$
- $x \hookrightarrow y, z \stackrel{def}{=} x \mapsto y, z * true$
- $P \mathrel{-\!\circledast} Q \stackrel{def}{=} \neg(P \mathrel{-\!\!*} \neg Q)$
  - $(P \mathrel{-\!\circledast} Q)\ h \iff \exists h_1.\ P\ h_1 \wedge Q(h \uplus h_1)$
  - "septraction"

Properties

- $*$ is commutative & associative: $P * Q \iff Q * P$, $P * (Q * R) \iff (P * Q) * R$
- emp is a unit for $*$: $P * emp \iff P$
- $*$ distributes over $\vee$: $P * (Q \vee R) \iff P * Q \vee P * R$

- $x \mapsto y * z \mapsto w \vdash x \neq y$
- "Modus ponens for $*$" $\quad P * (P -\!\!* Q) \vdash Q$.

<u>Rules for eliminating $-\!\!\circledast$.</u>

- $(x \mapsto y \mathbin{-\!\!\circledast} z \mapsto w) \iff \mathrm{emp} \land x = z \land y = w$
- $(x \mapsto y \mathbin{-\!\!\circledast} P * Q) \iff (x \mapsto y \mathbin{-\!\!\circledast} P) * Q\llcorner_x \lor P\llcorner_x * (x \mapsto y \mathbin{-\!\!\circledast} Q)$
- $(P * Q \mathbin{-\!\!\circledast} R) \iff$
  $P \mathbin{-\!\!\circledast} (Q \mathbin{-\!\!\circledast} R)$

  $Q \land \nexists v.\ x \hookrightarrow v$
- $P \mathbin{-\!\!\circledast} (R \lor Q) \iff (P \mathbin{-\!\!\circledast} R) \lor (P \mathbin{-\!\!\circledast} Q)$.
- $P \mathbin{-\!\!\circledast} \exists x.\, Q \iff \exists x.\ P \mathbin{-\!\!\circledast} Q$
- $P \mathbin{-\!\!\circledast} (P * Q) \not\Leftrightarrow Q$ [does not hold in general!!!]
- Special cases hold, e.g.

  $x \mapsto y \mathbin{-\!\!\circledast} (x \mapsto y * Q) \iff Q\llcorner_x$.

<u>Rules for $\llcorner$</u>

- $x \mapsto y\llcorner_z \iff x \mapsto y \land x \neq z$
- $(P * Q)\llcorner_z \iff P\llcorner_z * Q\llcorner_z$
- $(P \underset{\land}{\lor} Q)\llcorner_z \iff P\llcorner_z \underset{\land}{\lor} Q\llcorner_z$
- $P\llcorner_x\llcorner_y \iff P\llcorner_y\llcorner_x$
- $\mathrm{emp}\llcorner_x \iff \mathrm{emp}$

<u>List segments</u>

$$ls_\alpha(x,y) \overset{\text{def}}{\iff} \begin{array}{l} x = y \land \mathrm{emp} \land \alpha = \varepsilon \\ \lor\ \exists v, z, \beta.\ x \mapsto v, z * ls_\beta(z,y) \land \alpha = v \cdot \beta \end{array}$$

<u>Some properties:</u>

- $ls_\alpha(x,y) * ls_\beta(y,z) \Rightarrow ls_{\alpha\cdot\beta}(x,z)$
- $a \mapsto b \mathbin{-\!\!\circledast} ls_\alpha(x,y) \iff$
  $$\begin{array}{l} \exists \beta, \gamma, z.\quad ls_\beta(x,a)\llcorner_a * a{+}1 \mapsto z * ls_\gamma(z,y)\llcorner_a \land \alpha = \beta\cdot b\cdot\gamma \\ \lor\ \exists \beta, \gamma, v.\quad ls_\beta(x, a{-}1)\llcorner_a * a{-}1 \mapsto v * ls_\gamma(b,y)\llcorner_a \land \alpha = \beta\cdot v\cdot\gamma \end{array}$$