Spec Inference Rules

SL / ISL

Axiom Rule

$$\frac{}{S;\ \Delta}\ \top \qquad \Delta = \emptyset$$

<same>

Elimination Rules

$$\frac{S;\ \Delta}{S;\ \Delta, \{\Sigma_1 \wedge \pi_1 \vdash F_2\}}\ \bot_\pi \qquad \pi_1 \to \text{false}$$

$$\frac{S;\ \Delta}{S;\ \Delta, \{\pi_1 \vdash \pi_2\}}\ \vdash_\pi \qquad \pi_1 \to \pi_2$$

$$\frac{S;\ \Delta}{S;\ \Delta, \{\Sigma_1 * u \xrightarrow{t_1} \{\vec{v}\} * u \xrightarrow{t_2} \{\vec{v}\} \wedge \pi_1 \vdash F_2}\ \bot_\sigma$$

$\dfrac{}{\bot \vdash_{pos}}$

$$\frac{S;\ \Delta}{S;\ \Delta,\ \{\Sigma_1 * u \overset{L_1}{\mapsto} \{\vec{t}\} * u \overset{L_2}{\mapsto} \{\vec{w}\} \wedge \Pi_1 \vdash F_2\}} \quad \text{(same)}$$

$$\bot \vdash_{neg} \quad \frac{S;\ \Delta}{S;\ \Delta,\ \{\Sigma_1 * u \overset{L_1}{\mapsto} \{\vec{t}\} * u \not\mapsto \wedge \Pi_1 \vdash F_2\}} \quad \text{(new)}$$

Skolemisz Rules

$$\exists_L \quad \frac{S;\ \Delta,\ \{F_1[v/x] \vdash F_2\}}{S;\ \Delta,\ \{\exists x.\ F_1 \vdash F_2\}} \qquad v \notin fv(F_1, F_2)$$

$$\exists_R \quad \frac{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}\ F_2[t/u]\}}{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}, u.\ (F_2 \wedge u = t)\}}$$

< same >

Dropping emp

< same >

$$E_L \quad \frac{S;\ \Delta,\ \{F_1 \vdash F_2\}}{S;\ \Delta,\ \{F_1 * emp \vdash F_2\}}$$

$$E_R \quad \frac{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}.\ F_2\}}{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}.\ (F_2 * emp)\}}$$

Equality Rule

$$\frac{S;\ \Delta,\ \{F_1[t/u] \vdash F_2[t/u]\}}{S;\ \Delta,\ \{F_1 \wedge u = t \vdash F_2\}}$$

<Same>

Matching Rules ($\mapsto$) $\mapsto$: singleton cell

$\mapsto$

$$\frac{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}\,(F_2 \wedge u = v \wedge \vec{t} = \vec{r})\}}{S;\ \Delta,\ \{F_1 * u \overset{L}{\mapsto} \{\vec{t}\} \vdash \exists \vec{x}\,(F_2 * v \overset{L}{\mapsto} \{\vec{r}\})\}} \quad fv(v, \vec{r}) \# \vec{x}$$

$\mapsto \longrightarrow$ live (same)

$$\frac{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}\,(F_2 \wedge u = v \wedge \vec{t} = \vec{r})\}}{S;\ \Delta,\ \{F_1 * u \overset{L}{\mapsto} \{\vec{t}\} \vdash \exists \vec{x}\,(F_2 * v \overset{L}{\mapsto} \{\vec{r}\})\}} \quad fv(v, \vec{r}) \# \vec{x}$$

$\mapsto \longrightarrow$ freed (new)

$$\frac{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}\,(F_2 \wedge u = v)\}}{S;\ \Delta,\ \{F_1 * u \mapsto \vdash \exists \vec{x}\,(F_2 * v \mapsto \{\vec{r}\})\}} \quad fv(v) \# \vec{x}$$

Matching Rules ($\not\approx P$) P : inductive predicate

$$\not\approx P\ \frac{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}.(F_2 \wedge \vec{e} = \vec{x})\}}{S;\ \Delta,\ \{F_1 \not\approx P(\vec{e}) \vdash \exists \vec{x}.(F_2 \not\approx P(\vec{r}))\}} \quad fv(\vec{x}) \# \vec{x}$$

<same>

Unknown Rules

$$U_L\ \frac{S \cup \{U(\vec{e}) \stackrel{def}{=} F\};\ \Delta[F/U(\vec{e})],\ \{F_1 \vdash F_2\}}{S;\ \Delta,\ \{F_1 \not\approx U(\vec{e}) \vdash F_2 \not\approx F\}} \quad U \notin F_1, F_2$$

$$U_R\ \frac{S \cup \{U(\vec{e}) \stackrel{def}{=} F\};\ \Delta[F/U(\vec{e})],\ \{F_1 \vdash F_2\}}{S;\ \Delta,\ \{F_1 \not\approx F \vdash F_2 \not\approx U(\vec{e})\}} \quad U \notin F_1, F_2$$

U_L/U_R

- $\mapsto(\Sigma)$ – "all freed-cell heaplets contained in Σ"
- $addr(\Sigma)$ – set of addresses that occur as roots of heaplets in Σ (live or freed)

Using above definitions:

$$fv(F) \subseteq fv(\vec{e})$$
$$\mapsto (F_{1/2} \not\approx F) \cap addr(\vec{e}) \subseteq addr(F)$$

"known side" depending on U_L or U_R

root of the rules <same>

Unfolding Rules

P_L
$$\frac{S;\ \Delta,\ \{F_1 * F_1'^{\,p}(\vec{t}) \vdash F_2,\ \ldots,\ \{F_1 * F_n'^{\,p}(\vec{t}) \vdash F_2\}}{S;\ \Delta,\ \{F_1 * p(\vec{t}) \vdash F_2\}}$$
$$\left(p(\vec{t}) \stackrel{def}{=} F_1'^{\,p}(\vec{t}) \vee \ldots \vee F_m'^{\,p}(\vec{t})\right)$$

P_R
$$\frac{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}\,(F_2 * F_i'^{\,p}(\vec{t}))\}}{S;\ \Delta,\ \{F_1 \vdash \exists \vec{x}.\,(F_2 * p(\vec{t}))\}}$$
$$\left[F_i'^{\,p}(\vec{t}) \stackrel{def}{\Rightarrow} p(\vec{t})\right]$$

(P_L/P_R) • $p(\vec{x}) \stackrel{def}{=} \bigvee_{K \in \mathcal{K}} \exists \vec{y}_K .\ (\Sigma_K * \Pi_K)$ → Every branch 'K' has spatial and pure part.

• freed $(\Sigma_K) \stackrel{def}{=} \Sigma_K * (\mapsto\!\!\!\!\!\!\cdot\ \text{-completion})$

• $\mapsto\!\!\!\!\!\!\cdot$ -completion - adds a negative cell '$a \mapsto$' for every 'a' s.t.

(1.) it appears in argument list $\vec{t}$

(2.) is the root of a live heaplet $a \mapsto \ldots$ in some other branch but not in Σ_K

(If branch stops owning a cell another branch owns, mark it that address as "freed", rather than forgetting it)

↳ Definitions →

PTO for rules

P2

for every branch $\kappa \in K$:

$\Theta_\kappa \stackrel{\text{def}}{=} \text{freed}(\Sigma_\kappa[\vec{E}/\vec{x}])$

↳ instantiate and added ↦ atoms.

→ $\text{addr}(\Theta_\kappa \mapsto) \cap \text{addr}(F_1 * F_2) = \emptyset$

(don't re-allocate freed addresses)

rest of the rule (same)

(→ use Θ instead of $F_1^P(\vec{E}), F_2^P(\vec{E}) \ldots$)

P_k Choose one branch $k \in K$

$\Theta \triangleq \text{fresh}(\Sigma_k[\vec{b}/\vec{x}])$

$\text{addr}(\Theta \mapsto) \cap \text{addr}(F_1 * F_2) = \emptyset$

(use Θ instead of $f_i^p(\vec{E})$)

r.cot of the rule <Same>

Synthesis Rules

$\Gamma; \vec{V}; \{F_1\} \rightsquigarrow \{F_2\}$

- $\vec{V}$: available variables for synthesis
- F_1: pre
- F_2: post
- Γ: list of declared functions

goal: find C that satisfies triple $\{F_1\}\ C\ \{F_2\}$

(SL) $[F_1] \subseteq [F_2]$

(ISL)

Skip $\quad \dfrac{}{\Gamma; V; \{F_1\} \rightsquigarrow \{F_2\} \mid \text{skip}}$

$F_1 \vdash F_2$

?

$\dfrac{}{\Gamma; V; [F_1] \rightsquigarrow [\text{ok}: F_2] \mid \text{skip}}$

(no error path & unchanged heap.)

Return

$$\Gamma; V; [F_1] \rightsquigarrow \{\exists \vec{z}.\ (F_2 \wedge res = e)\} \mid \text{return } e;$$

$F_1 \vdash \exists \vec{z}.\ F_2$, $fv(e) \subseteq V$

$$\Gamma; V; [F_1] \rightsquigarrow [ok: \exists \vec{z}.\ (F_2 \wedge res = e)] \mid \text{return } e;$$

? $F_1 \vdash \exists \vec{z}.\ F_2$, $fv(e) \subseteq V$

Read

$$\Gamma; V \cup \{v\}; \{\Sigma_1 * u \hat{\mapsto} (fld : t) \wedge \pi_1 \wedge v = t\} \rightsquigarrow \{F_2\} \mid C$$

$$\Gamma; V; \{\Sigma_1 * u \hat{\mapsto} (fld : t)\} \wedge \pi_1 \rightsquigarrow \{F_2\} \mid typ\ v = u \to fld = t;$$

$(fld \to field\ data)$

$(typ \to variable\ type)$

$u \in V$, $v \notin V$ →

Read

$$\text{Read}_{\text{ok}}\ \frac{\Gamma; V \cup \{v\}; [\Sigma_1 * u \xrightarrow{1} (\text{fld}:t) \wedge \pi_1 \wedge v = t] \rightsquigarrow [f_2] \mid C}{\Gamma; V; [\Sigma_1 * u \xrightarrow{1} (\text{fld}:t) \wedge \pi_1] \rightsquigarrow [\text{ok}; f_2 * u \xrightarrow{1} (\text{fld}:t)] \mid \text{typ } v = u.\text{fld}; C}$$

$$\text{Read}_{\text{err}}\ \frac{\Gamma; V \cup \{v\}; [\Sigma_1 * u \mapsto \wedge \pi_1 \wedge v = t] \rightsquigarrow [f_2] \mid C}{\Gamma; V; [\Sigma_1 * u \mapsto \wedge \pi_1] \rightsquigarrow [\text{err}; f_2 * u \mapsto] \mid \text{error}; C;}$$

$u \in V$
$v \notin V$

Write

$$\frac{\Gamma; V; \{f_1 * u \xrightarrow{1} (\text{fld}:t)\} \rightsquigarrow \{f_2 * u \xrightarrow{1} (\text{fld}:t)\} \mid C}{\Gamma; V; \{f_1 * u \xrightarrow{1} (\text{fld}:r)\} \rightsquigarrow \{f_2 * u \xrightarrow{1} (\text{fld}:t)\} \mid u.\text{fld} = t; C}$$

for $(v, r) \subseteq V$

$v \neq t$.

<same> except:

(similar to Read ISL rules) ⟷ "error" case for $u \mapsto$ → no writes possible.

Alloc

$$\frac{\Gamma; V \cup \{u\}; \{\Sigma_1 * u \mapsto^{1} \{\vec{v}\} \wedge \pi_1\} \rightsquigarrow \{\Sigma_2 * u \mapsto^{1} \{\vec{t}\} \wedge \pi_2\} \mid C}{\Gamma; V; \{\Sigma_1 \wedge \pi_1\} \rightsquigarrow \{\Sigma_2 * u \mapsto \{\vec{t}\} \wedge \pi_2\} \mid \mathrm{sz}(u) = \mathrm{malloc}(\mathrm{sizeof}(\mathrm{struct}\ c)); C}$$

$u \notin \mathrm{fv}(V, \Sigma_1)$
$\vec{v}$ are fresh
$\vec{t} \subseteq V$

<same for ISL>

Free

$$\frac{\Gamma; V; \{F_1 \wedge \pi_1\} \rightsquigarrow \{\exists \vec{z}.\ (\Sigma_2 \wedge \pi_2)\} \mid C}{\Gamma; V; \{F_1 * u \mapsto \{\vec{t}\} \wedge \pi_1\} \rightsquigarrow \{\exists \vec{z}.\ (\Sigma_2 \wedge \pi_2)\} \mid \mathrm{dec}(u); C}$$

$u \notin \mathrm{fv}(\Sigma_2)$
$u, \vec{t} \subseteq V$

Free$_{OK}$

$$\frac{\Gamma; V; [F_1 \wedge \pi_1] \rightsquigarrow [\exists \vec{z}.\ (\Sigma_2 \wedge \pi_2)] \mid C}{\Gamma; V; [F_1 * u \mapsto \{\vec{t}\} \wedge \pi_1] \rightsquigarrow [\mathrm{OK}: \exists \vec{z}.\ (\Sigma_2 \wedge \pi_2) * u \mapsto] \mid \mathrm{dec}(u); C}$$

Free$_{ER}$ <same as above (with ER) but pre- has $u \mapsto$>

(Keep track of dealloc-ed pointers)

Exists

$$\text{Exists}_L\ \frac{\Gamma; V; \{F_1[t/u]\} \rightsquigarrow \{F_2\} \mid C \qquad \vdash \mathrm{fv}(V, F_1, F_2)}{\Gamma; V; \{\exists u. F_1\} \rightsquigarrow \{F_2\} \mid C}$$

$$\text{Exists}_R\ \frac{\Gamma; V; \{F_1\} \rightsquigarrow \{\exists \vec{z}. F_2[t/u]\} \mid C}{\Gamma; V; \{F_1\} \rightsquigarrow \{\exists \vec{z}, u. (F_2 \wedge u = t)\} \mid C}$$

<Same>

Frame $\mapsto$. $\boxed{\mathrm{fv}(u, \vec{t}) \# \vec{z}}$

$$\frac{\Gamma; V; \{\Sigma_1 \wedge \pi_1\} \rightsquigarrow \{\exists \vec{z}. (\Sigma_2 \wedge \pi_2)\} \mid C}{\Gamma; V; \{\Sigma_1 * u \dot{\mapsto} \{\vec{t}\} \wedge \pi_1\} \rightsquigarrow \{\exists \vec{z}. (\Sigma_2 * u \dot{\mapsto} \{\vec{t}\} \wedge \pi_2)\} \mid C}$$

Frame$_{er}$ $er_1\ u \mapsto$ $er_2\ u$ — $u \mapsto$ "

<OK. Same wlg.>

Frame $\not\downarrow$ $\mathrm{fv}(\vec{t}) \# \vec{z}$

<Same as Frame $\mapsto$, error cases for alloc & dealloced addrs, & de-alloc & alloced addr.>

Unfold Rules

Unfold$_2$

$$\frac{\Gamma; V; \{F_1 * F_p^i(\vec{t})\} \rightsquigarrow \{F_2\} \mid C}{\Gamma; V; \{F_1 * p(\vec{t})\} \rightsquigarrow \{F_2\} \mid C}$$

$$p(\vec{t}) \overset{\text{def}}{=} F_p^1(\vec{t}) \vee \ldots \vee F_p^n(\vec{t})$$

$$1 \le i \le n, \forall j \neq i,\ F_1 * F_p^j(\vec{t}) \equiv \text{false}$$

Unfold$_R$

$$\frac{\Gamma; V; \{F_1\} \rightsquigarrow \{\exists \vec{z}.\ (F_2 * F_p)(\vec{t}))\} \mid C}{\Gamma; V; \{F_1\} \rightsquigarrow \{\exists \vec{z}.\ (F_2 * p(\vec{t}))\} \mid C}$$

$$F_p(\vec{t}) \overset{\text{def}}{\Rightarrow} p(\vec{t})$$

(same treatment as spec-inference unfold rules – migration of freed cells)

Assign.

$$\frac{\Gamma; V \cup \{v\}; \{F_1 \wedge v = e\} \rightsquigarrow \{\exists \vec{z}.\ (F_2 \wedge u = e)\} \mid C}{\Gamma; V \cup \{u\}; \{F_1\} \rightsquigarrow \{\exists \vec{z}.\ (F_2 \wedge u = e)\} \mid v = e; C}$$

(same for ISL)

$$u \notin \vec{z},\ u \notin fv(F_1),\ fv(e) \subseteq V$$

Call

$$\Gamma \cup \{\{q_1\}\ \text{frame}(\vec{u})\{q_2\}\}; V \cup \{v\} \cdot \{F_1 \star q_2\theta[v/res]\} \rightsquigarrow \{F_2\} \mid C$$

$$\Gamma \cup \{\{q_1\}\ \text{frame}(\vec{u})\{q_2\}\}; V; \{F_1 \star F\} \rightsquigarrow \{F_2\} \mid_{typ} V = \text{frame}(\vec{u}\theta); C$$

$$q_1\theta = F_1, \quad fv(\vec{u}\theta) \in V$$

<Same for (SL)>

Examples - (attempts)