Completeness of Incorrectness Separation Logic by Weakest Postcondition

Yeonseok Lee (Nagoya University), Koji Nakazawa (Nagoya University)

Goal

Proving the **relative completeness** of **Incorrectness Separation Logic** [3] with infinitary formulas
− By calculation of weakest postconditions (cf. Reverse Hoare Logic (RHL) [1])

Hoare Logic (HL)

- HL checks "correctness" of programs.
  - Hoare Triples: $\{P\}\ \mathbb{C}\ \{Q\}$
  - For all states s in precondition P if running $\mathbb{C}$ on s terminates in s', then s' is in postcondition Q
- post$(\mathbb{C}, P)$ describes states the set of obtained by executing $\mathbb{C}$ on P
- Q **over-approximates** post$(\mathbb{C}, P)$, i.e., post$(\mathbb{C}, P) \subseteq Q$

Reverse HL & Incorrectness Logic (IL) [2]

- Viewpoint opposite to HL; checks for "incorrectness"
  - Triples: $[P]\ \mathbb{C}\ [Q]$
- For all states s' in Q, s' can be reached by running $\mathbb{C}$ on some s in P
- Q **under-approximates** post$(\mathbb{C}, P)$, i.e., post$(\mathbb{C}, P) \supseteq Q$

	HL	IL
$(\top)\ x := y\ (x = y)$	✔	✔
$(\top)\ x := y\ (\top)$	✔	❌
$(\top)\ x := y\ (x = y \land 0 < x < 10)$	❌	✔

Incorrectness Separation Logic [3]

- Incorrectness Separation Logic = Reverse HL + Separation Logic
  - Moreover, we consider exit statuses (ok = normal end / er = error)
- $x \mapsto y$: Singleton heap
- $x \not\mapsto$: Negative heap (necessary for the "frame rule")
  - x has been deallocated
    - $[x \mapsto - * x \mapsto -]$ free(x) $[\mathsf{emp} * x \mapsto -]$ ❌
    - $[x \mapsto - * x \mapsto -]$ free(x) $[x \not\mapsto - * x \mapsto -]$ ✅
- $P * Q$ (separating conjunction) : P and Q hold for disjoint portions (heaps) $\rightarrow$ modular reasoning
- Heap model
  s : var $\rightarrow$ val (store): representing (dis-) equalities between variables
  h : loc $\rightarrow_{fin}$ val (heap): describing states of heaps

$$s, h \vDash P_1 * P_2 \Leftrightarrow \exists h_1, h_2 . h = h_1 \circ h_2 \land s, h_1 \vDash P_1 \land s, h_2 \vDash P_2$$

$$s, h \vDash x \mapsto y \Leftrightarrow \mathrm{dom}(h) = \{s(x)\} \land h(s(x)) = s(y) \neq \bot$$

$$s, h \vDash x \not\mapsto \Leftrightarrow \mathrm{dom}(h) = \{s(x)\} \land h(s(x)) = \bot$$

$$s, h \vDash x \approx y \Leftrightarrow s(x) = s(y) \land \mathrm{dom}(h) = \varnothing$$

- Inference rules ($\epsilon \in \{\mathsf{ok}, \mathsf{er}\}$ is an exit status)

Cons **Reversed with HL!**

$$\frac{p' \Rightarrow p \qquad \vdash [p']\ \mathbb{C}\ [\epsilon : q'] \qquad q \Rightarrow q'}{\vdash [p]\ \mathbb{C}\ [\epsilon : q]}\ \textsc{Cons}$$

$$\frac{\vdash [p_1]\ \mathbb{C}\ [\epsilon : q_1] \qquad \vdash [p_2]\ \mathbb{C}\ [\epsilon : q_2]}{\vdash [p_1 \lor p_2]\ \mathbb{C}\ [\epsilon : q_1 \lor q_2]}\ \textsc{Disj}$$

$$\textsc{Free}\quad \vdash [x \mapsto e]\ \mathtt{L}\!:\mathtt{free}(x)\ [ok : x \not\mapsto]$$

Formulas of ISL with infinite disjunctions

$$P ::= \bigvee_{i \in I} \exists \vec{x} . \psi_i \mid \psi \qquad (I \text{ may be infinite})$$

$$\psi ::= \psi * \psi \qquad \text{Quantifier-free symbolic heap}$$

$$\mid \mathsf{emp} \mid x \mapsto y \mid x \not\mapsto \qquad \text{Spatial Formulas}$$

$$\mid x \approx y \mid x \not\approx y \qquad \text{Pure Formulas}$$

Relative Completeness of ISL

Theorem: For all $P, \mathbb{C}, \epsilon, Q$, if $[P]\ \mathbb{C}\ [\epsilon : Q]$ is true, then $[P]\ \mathbb{C}\ [\epsilon : Q]$ is provable.

(Outline of the proof)

1. Proving Expressiveness by defining weakest postcondition
   $$\forall \sigma' . \sigma' \in \mathrm{WPO}[\![P, \mathbb{C}, \epsilon]\!] \iff \sigma' \vDash \mathrm{wpo}(P, \mathbb{C}, \epsilon)$$
   - $\mathrm{WPO}[\![P, \mathbb{C}, \epsilon]\!] = \{\sigma' \mid \exists \sigma . \sigma \vDash P \land (\sigma, \sigma') \in [\![\mathbb{C}]\!]_\epsilon\}$
   - A set of states satisfying weakest postconditions for $P, \mathbb{C}$ and ϵ
2. Proving that weakest postcondition is always derivable
   - For all $P, \mathbb{C}, \epsilon$, $\vdash [P]\ \mathbb{C}\ [\epsilon : \mathrm{wpo}(P, \mathbb{C}, \epsilon)]$

Weakest postconditions

- Case analysis for all pairs of variables ($x = y$ or $x \neq y$)
  - Every formula can be tranlstated to the form:
    $$\bigvee_{i \in I} \exists \vec{x} . \psi_i$$
    (ψ_i is a finite symbolic heap for each case, i.e.,
    $\forall i \in I, \forall y, z \in \mathrm{fv}(\psi_i) \cup \mathrm{fv}(\mathbb{C}) . y \approx z \vDash \psi_i$ or $y \not\approx z \vDash \psi_i$)

- Definition of wpo$(P, \mathbb{C}, \epsilon)$
  - $\mathrm{wpo}(P, \mathbb{C}, \epsilon) = \bigvee_{i \in I} \exists \vec{x} . \mathrm{wpo_{sh}}(\psi_i, \mathbb{C}, \epsilon)$

    (P is equivalent to $\bigvee_{i \in I} \exists \vec{x} . \psi_i$)

- Definition of $\mathrm{wpo_{sh}}(\psi, \mathbb{C}, \epsilon)$ for (qf-)symbolic heaps ψ
  - $\mathrm{wpo_{sh}}(\psi' * x \approx y * y \mapsto e, \mathrm{free(x)}, \mathsf{ok}) = \psi' * x \approx y * y \not\mapsto$
  - $\mathrm{wpo_{sh}}(\psi, \mathrm{free(x)}, \mathsf{ok}) = \mathrm{false}$ (otherwise)

    Case 1:
    x is a fresh address

    Case 2: x was once allocated ($x \not\mapsto$)
  - $\mathrm{wpo_{sh}}(\psi, x := \mathrm{alloc}(), \mathsf{ok}) =$
    $\exists x' . (\psi[x := x'] * x \mapsto -) \lor$
    $\bigvee_{j=1}^{n} ((*_{i=1}^{n} y_i \not\mapsto)[y_j \not\mapsto := y_j \mapsto -] * x \approx y_j * \psi'[x := x'])$
    ($\psi = (*_{i=1}^{n} y_i \not\mapsto) * \psi'$ s.t. ψ' does not contain $\not\mapsto$)
  - $\mathrm{wpo_{sh}}(\psi, x := \mathrm{alloc}(), \mathsf{er}) = \mathrm{false}$
  - $\mathrm{wpo_{sh}}(\psi, \mathbb{C}_1; \mathbb{C}_2, \mathsf{ok}) = \mathrm{wpo}(\mathrm{wpo_{sh}}(\psi, \mathbb{C}_1, \mathsf{ok}), \mathbb{C}_2, \mathsf{ok})$
  - $\mathrm{wpo_{sh}}(\psi, \mathbb{C}_1; \mathbb{C}_2, \mathsf{er}) =$
    $\mathrm{wpo_{sh}}(\psi, \mathbb{C}_1, \mathsf{er}) \lor \mathrm{wpo}(\mathrm{wpo_{sh}}(\psi, \mathbb{C}_1, \mathsf{ok}), \mathbb{C}_2, \mathsf{er})$
  - $\mathrm{wpo_{sh}}(\psi, \mathbb{C}^\star, \mathsf{ok}) = \bigvee_{n \in \mathbb{N}} \Upsilon(n)$
    ($\Upsilon(0) = \psi$ and $\Upsilon(n+1) = \mathrm{wpo}(\Upsilon(n), \mathbb{C}, \mathsf{ok})$)

References

[1] De Vries, E., Koutavas, V.: Reverse hoare logic. SEFM 2011, 155–171.
[2] O'Hearn, P.W.: Incorrectness logic. POPL 2019, 1–32.
[3] Raad, A., Berdine, J., Dang, H.H., Dreyer, D., O'Hearn, P., Villard, J.: Local reasoning about the presence of bugs: Incorrectness separation logic. CAV 2020, 225–252.