Program analysis: from proving correctness to proving incorrectness

Roberto Bruni, Roberta Gori
(University of Pisa)
Exam questions

BISS 2024
March 11-15, 2024
Exam 1

Prove that rule \{\text{conj}\} is sound

\[
\frac{\{P_1\} \vdash \{Q_1\} \quad \{P_2\} \vdash \{Q_2\}}{\{P_1 \land P_2\} \vdash \{Q_1 \land Q_2\}} \quad \{\text{conj}\}
\]

Exam 2

Show that the following rule for assignment is not sound

\[
\{P\} \ x := a \ {P[a/x]}
\]
Exam 3

Prove that rule [conj] is unsound

\[
\frac{[P_1] \ r \ [\epsilon : Q_1] \quad [P_2] \ r \ [\epsilon : Q_2]}{[P_1 \land P_2] \ r \ [\epsilon : Q_1 \land Q_2]} \quad \text{[conj]}
\]

Exam 4

Is this “mixed” HL+IL inference rule valid?

\[
\frac{[P \land b] \ c \ [\text{ok} : P]}{\{P\} \ \text{while} \ b \ \text{do} \ c \ \{P \land \neg b\}}
\]
Consider the abstract domain $\text{Sign}'$ in the figure

1. Define the corresponding $\alpha$ and $\gamma$.

2. Does it admit a complete abstract multiplication?

3. If not, can you add some abstract elements to $\text{Sign}'$ so that a complete abstract multiplication can be designed?
Is the bca of $f : \mathbb{Z} \rightarrow \mathbb{Z}$ below complete on the Interval domain?

$$f(x) = \begin{cases} 
  x & \text{if } x \leq 10 \\
  10 & \text{Otherwise}
\end{cases}$$
Let $C \triangleq \wp(\Sigma^*)$ be the domain of sets of strings over a (finite) alphabet $\Sigma$. Let the abstract domain be $A \triangleq \wp(\Sigma)$. Assuming $|\Sigma| \geq 2$:

1. Define suitable $\alpha$ and $\gamma$ and prove that they form a Galois Insertion.

2. Lift the concrete operation $\cdot$ of string concatenation to sets of string.

3. Define its best correct approximation.

4. Prove whether the previously defined abstract operation is complete.
Exam 8

Prove that [conj] is unsound for LCL

\[
\frac{\vdash_{A} [P_1] r [Q_1] \quad \vdash_{A} [P_2] r [Q_2]}{
\vdash_{A} [P_1 \land P_2] r [Q_1 \land Q_2]}
\]

[conj]

Exam 9

Show that the following rule is not sound

\[
\vdash_A [P] x := \text{nondet()} [P[v/x]]
\]
Can you find a derivation for the LCL triple

\[ \vdash_{\text{Sign}^+} \begin{array}{l} \neg (\forall x > 0) \; x := x + 1; x := x - 1 \; \forall x > 0 \end{array} \]

repairing the domain if necessary?
Exam 11

Find a derivation for the SIL triple
\[ \langle \text{true} \rangle \text{ if } x \geq y \text{ then } z := x \text{ else } z := y \langle z = \max(x, y) \rangle \]

Exam 12

Prove or disprove the validity of the following axiom in SIL

\[ \langle P \rangle (b) \Rightarrow \langle P \land b \rangle \]
Consider the imprecise list segment definition below
\[ ils(a_1, a_2) \triangleq (a_1 = a_2 \land \text{emp}) \lor (\exists v . a_1 \mapsto v \ast ls(v, a_2)) \]

Prove that \( ils(a_1, a_2) \not\equiv ls(a_1, a_2) \) by finding a state that distinguishes \( ls(11, 11) \) from \( ils(11, 11) \).
Complete the following derivations, if possible

\[
\{ P \ast x \mapsto _{\_} \} \ [x] := 11 \ \{ P \ast ??? \}
\]
\[
\{ \text{true} \} \ [x] := 11 \ \{ ??? \}
\]

\[
\{ P \ast x \mapsto _{\_} \} \ \text{free}(x) \ \{ ??? \}
\]
\[
\{ \text{true} \} \ \text{free}(x) \ \{ ??? \}
\]
Can we derive the following ISL triple?

\[ x \mapsto 1 \quad \text{free}(x); \quad x := \text{alloc()} \quad \text{ok} : x \mapsto 2 \]
Prove the SepSIL triple $\langle \langle p \leftrightarrow \text{nil} \ast \text{true} \rangle \rangle \ c \ \langle \langle i = 0 \rangle \rangle$ where

$$c \triangleq i := 0 ; q := \ast p ; \text{while} \ (q \neq \text{nil}) \ \text{do} \ \{ \ q := \ast q ; i := i + 1 \ \}$$