Program analysis: from proving correctness to proving incorrectness

Roberto Bruni, Roberta Gori
(University of Pisa)

Exam questions

BISS 2024
March 11-15, 2024

HL

Exam 1

Prove that rule {conj} is sound

$$\frac{\{P_1\}\ r\ \{Q_1\} \quad \{P_2\}\ r\ \{Q_2\}}{\{P_1 \wedge P_2\}\ r\ \{Q_1 \wedge Q_2\}}\ \text{\{conj\}}$$

Exam 2

Show that the following rule for assignment is not sound

$$\frac{}{\{P\}\ x := a\ \{P[a/x]\}}$$

IL

Exam 3

Prove that rule [conj] is unsound

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

Exam 4

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

$$\frac{[P \wedge b]\ c\ [\mathsf{ok} : P]}{\{P\}\ \text{while}\ b\ \text{do}\ c\ \{P \wedge \neg b\}}$$

Exam 5

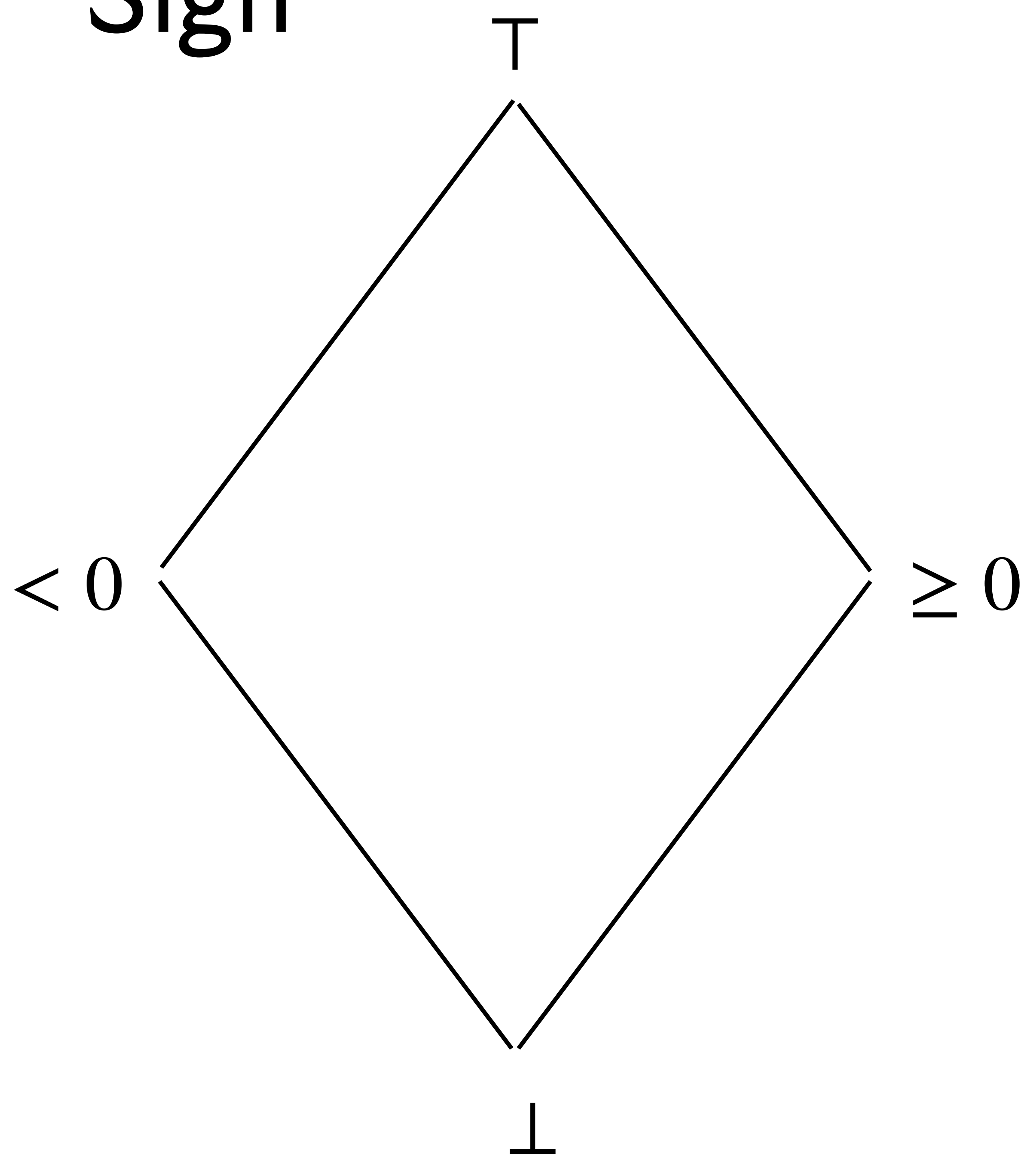
Consider the abstract domain Sign' in the figure

1. Define the corresponding α and γ.

2. Does it admit a complete abstract multiplication?

3. If not, can you add some abstract elements to Sign' so that a complete abstract multiplication can be designed?

Sign'



Abs.Int.

Exam 6

Is the bca of $f : \mathbb{Z} \to \mathbb{Z}$ below complete on the Interval domain?

$$f(x) = \begin{cases} x & \text{if } x \leq 10 \\ 10 & \text{Otherwise} \end{cases}$$

Abs.Int.

Exam 7

Let $C \triangleq \wp(\Sigma^*)$ be the domain of sets of strings over a (finite) alphabet Σ.
Let the abstract domain be $A \triangleq \wp(\Sigma)$. Assuming $|\Sigma| \geq 2$:

1. Define suitable α and γ 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

$$\frac{\vdash_A [P_1]\ r\ [Q_1] \qquad \vdash_A [P_2]\ r\ [Q_2]}{\vdash_A [P_1 \wedge P_2]\ r\ [Q_1 \wedge Q_2]}\ \text{[conj]}$$

Exam 9

Show that the following rule is not sound

$$\frac{}{\vdash_A [P]\ x := \text{nondet}()\ [P[v/x]]}$$

Repair

Exam 10

Can you find a derivation for the LCL triple

$$\vdash_{\mathsf{Sign}^+} [x > 0]\; x := x + 1\,;\; x := x - 1\; [x > 0]$$

repairing the domain if necessary?

SIL

Exam 11

Find a derivation for the SIL triple

$\langle\!\langle \text{true} \rangle\!\rangle$ if $x \geq y$ then $z := x$ else $z := y$ $\langle\!\langle z = \max(x, y) \rangle\!\rangle$

Exam 12

Prove or disprove the validity of the following axiom in SIL

$$\frac{}{\langle\!\langle P \rangle\!\rangle \ \ (b)? \ \ \langle\!\langle P \wedge b \rangle\!\rangle}$$

Exam 13

Consider the imprecise list segment definition below

$\mathsf{ils}(a_1, a_2) \triangleq (a_1 = a_2 \wedge \mathsf{emp}) \vee (\exists v\,.\; a_1 \mapsto v * \mathsf{ls}(v, a_2))$

Prove that $\mathsf{ils}(a_1, a_2) \not\equiv \mathsf{ls}(a_1, a_2)$ by finding a state that distinguishes $\mathsf{ls}(11{,}11)$ from $\mathsf{ils}(11{,}11)$

SL

Exam 14

Complete the following derivations, if possible

$\{P * x \mapsto \_\}\ [x] := 11\ \{P*??\}$

$\{\mathsf{true}\}\ [x] := 11\ \{??\}$

$\{P * x \mapsto \_\}\ \mathsf{free}(x)\ \{??\}$

$\{\mathsf{true}\}\ \mathsf{free}(x)\ \{??\}$

Exam 15

Can we derive the following ISL triple ?

$$[x \mapsto 1]\ \mathsf{free}(x); x := \mathsf{alloc}(\,)\ [\mathsf{ok} : x \mapsto 2]$$

Exam 16

Prove the SepSIL triple $\langle\!\langle p \mapsto \mathsf{nil} * \mathsf{true} \rangle\!\rangle\ c\ \langle\!\langle i = 0 \rangle\!\rangle$ where

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