Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints

Due: October 7

Answer each of the following questions. Label your answer with the specified question tag.

We will discuss up to Section 6 during our meeting on this paper. We will also discuss some of the later examples at a high level.

Cousot 1 In section 3.2 on page 239 a “simple semantics” is given. Bullet 7 defines an environment (a mapping of an identifier to a value) as a function as follows (cond is defined in the bullet just before this).

\[ e[v/x] = \lambda y . \text{cond}(y = x, v, e(y)) \]

– Explain what this representation means.
– Assuming the following value for e (with cond expanded and \( \perp_{\text{Env}} \) as defined at the bottom of the page) give the result of \( e[9/b] \).

\[ e = \lambda y . \text{if} y = a \ \text{then} \ 1 \ \text{else} \ (\lambda y . \text{if} y = b \ \text{then} \ 2 \ \text{else} \ \perp_{\text{Env}})(y) \]

Cousot 2 Explain, in English, what each case of the state transition function \( n\text{-state} \) specifies. This is the function in bullet 8 of section 3.2 on page 239.

Cousot 3 \( n\text{-state} \) was defined as part of the semantic model of programs reflecting dynamic execution. Consider the use of \( n\text{-state} \) in \( n\text{-context} \) (used in the definition the static semantics of a program) on page 240. Explain how the use of \( n\text{-state} \) in \( n\text{-context} \) relates to the axiomatic semantics discussions in Floyd and Hoare and to the dataflow analyses discussed in Kildall.

Cousot 4 The last sentence in Section 4 states that abstract contexts that satisfy \( \alpha \) but that do not necessarily satisfy \( \beta \) approximate concrete context. Why are these only approximations?