1 Pointer Analysis

The states of the concrete semantics used in this section are functions $S = \text{Loc} \to \text{Loc} \cup Z$. The abstract domain in this section is $A = 2^{\text{Var}^* \times \text{Var}^*}$ and the abstraction function (α) is defined by means of an extraction function (β), where $\beta(s) = \{(x, y) \mid s(loc(x)) = loc(y)\}$. The function $loc : \text{Var}^* \to \text{Loc}$ returns the "address" of each variable.

Recall that as usual in cases in which the Galois connection induced by an extraction function, $\alpha(S) = \cup\{\beta(s) \mid s \in S\}$, and $\gamma(a) = \{s \in 2^{\text{Var}^* \times \text{Var}^*} \mid \beta(s) \subseteq a\}$.

1.1 Question 1

The concrete semantics of the statement $x = y$ is

$$[\![x = y]\!](s) = s[loc(x) \mapsto s(loc(y))]$$

. The abstract transformer associated with this statement is

$$[\![x = y]\!]^\sharp(a) = a \backslash \{(x, z) \mid z \in \text{Var}^*\} \cup \{(x, w) \mid (y, w) \in a\}$$

. Show that the abstract transformer is the best, e.g.

$$[\![x = y]\!]^\sharp(a) = \alpha(\{[\![x = y]\!](s) \mid s \in \gamma(a)\})$$

for any $a \in A$.

1.2 Question 2

The abstract transformer of simple assignment

$$[\![x = y]\!]^\sharp(a) = a \backslash \{(x, z) \mid z \in \text{Var}^*\} \cup \{(x, w) \mid (y, w) \in a\}$$

is distributive, i.e.,

$$\forall a_1, a_2 \in A : [\![x = y]\!]^\sharp(a_1) \sqcup [\![x = y]\!]^\sharp(a_2) = [\![x = y]\!]^\sharp(a_1 \sqcup a_2)$$

Proof.

$$\begin{aligned}
&c[\![x = y]\!]^\sharp(a_1) \sqcup [\![x = y]\!]^\sharp(a_2) = \\
&= (a_1 \backslash \{(x, z) \mid z \in \text{Var}^*\} \cup \{(x, w) \mid (y, w) \in a_1\}) \cup (a_2 \backslash \{(x, z) \mid z \in \text{Var}^*\} \cup \{(x, w) \mid (y, w) \in a_2\}) \\
&= ((a_1 \cup a_2) \backslash \{(x, z) \mid z \in \text{Var}^*\}) \cup \{(x, w) \mid (y, w) \in (a_1 \cup a_2)\} \\
&= ((a_1 \sqcup a_2) \backslash \{(x, z) \mid z \in \text{Var}^*\}) \cup \{(x, w) \mid (y, w) \in (a_1 \sqcup a_2)\} \\
&= [\![x = y]\!]^\sharp(a_1 \sqcup a_2)
\end{aligned}$$

□

1.3 Question 3

The abstract transformer of the statement

$$[\![*x = y]\!]^\sharp(a) = a \cup \{(t, z) \mid (x, t) \in a, (y, z) \in a\}$$

is not distributive, i.e. exists $a_1, a_2 \in A$ s.t.

$$[\![*x = y]\!]^\sharp(a_1) \sqcup [\![*x = y]\!]^\sharp(a_2) \neq [\![*x = y]\!]^\sharp(a_1 \sqcup a_2)$$

Proof. We'll show the sets are not equal by showing elements present in $[\![*x = y]\!]^\sharp(a_1 \sqcup a_2)$ but not in $[\![*x = y]\!]^\sharp(a_1) \sqcup [\![*x = y]\!]^\sharp(a_2)$.
Let a_1 s.t.

- $(x, t_1), (y, w_1) \in a_1$
- $(x, t_2), (y, w_2) \notin a_1$

additionally, let a_2 s.t.

- $(x, t_1), (y, w_1) \notin a_2$
- $(x, t_2), (y, w_2) \in a_2$

then, it holds that:

- $(t_1, w_1) \in [\![*x = y]\!]^\sharp(a_1)$
- $(t_2, w_2) \in [\![*x = y]\!]^\sharp(a_2)$
- $(t_2, w_2) \notin [\![*x = y]\!]^\sharp(a_1)$
- $(t_1, w_1) \notin [\![*x = y]\!]^\sharp(a_2)$

therefore also $(t_2, w_2), (t_1, w_1) \notin [\![*x = y]\!]^\sharp(a_1) \sqcup [\![*x = y]\!]^\sharp(a_2)$.
Conversely, $(t_2, w_2), (t_1, w_1) \in [\![*x = y]\!]^\sharp(a_1 \sqcup a_2)$. □

2 Shape Analysis

In the 3-valued logic framework for shape analysis, the user needs to provide the update formulae which describe the effect of every program statement on the core and instrumentation predicates. In the class, we defined at the update formulae for the core predicates for list-manipulating programs. Define the update formulae for the instrumentation predicates capturing the properties: reach-ability from variable x, heap-sharing (is-shared), and cyclicity for list manipulating programs. Assume that the pointer variables of the program are x, y and z.

3 Owiki Gries Logic

Give a (non-trivial) specification for the following program and prove it using Owicki-Griel logic

$$\{X = A \wedge Y = B\}x := X; Y := 1||y := Y; x := X \ldots$$