Program Analysis and Verification
Course 0368-4479
2017/18 - Semester B
Exercise #2

Noam Rinetzky

Due 11/June/2018

1 Galois Connections and Distributive functions

1.1 Question 1

(i) If both (A, α, γ_1, C) and (A, α, γ_2, C) are Galois connections, than $\gamma_1 = \gamma_2$. (ii) If both (A, α_1, γ, C) and (A, α_2, γ, C) are Galois connections, than $\alpha_1 = \alpha_2$.

1.2 Question 2

Let S be a set, L a lattice and $\beta : S \to L$ a total function. Let $\alpha_\beta : 2^S \to L$ be a total function defined as $\alpha_\beta(X) = \sqcup\{\beta(s) \mid s \in X\}$ for any $X \subseteq S$, and $\gamma_\beta(a) : L \to 2^S$, a total function defined as $\gamma_\beta(a) = \{s \in S \mid \beta(s) \sqsubseteq a\}$ for any $a \in L$. Then, $(2^S, \alpha_\beta, \gamma_\beta, L)$ is a Galois connection.

1.3 Question 3

Let S be a set and L a lattice. Let $(2^S, \alpha, \gamma, L)$ be a Galois connection. Then, (A) exists $\beta : S \to L$ s.t. $\alpha(X) = \sqcup\{\beta(s) \mid s \in X\}$ for any $X \subseteq S$, and (B) $\gamma(a) = \{s \in S \mid \beta(s) \sqsubseteq a\}$ for any $a \in A$.

2 Pointer Analysis

The states of the concrete semantics used in this section are functions in $S = \text{Loc} \to \text{Loc} \cup Z$. 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 : Var$*$ $\to$ 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 $\gamma(a) = \{s \in 2^{\text{Var*} \times \text{Var*}} \mid \beta(s) \subseteq a\}$.

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

2.2 Question 2

The abstract transformer of simple assignment ($[\![x = y]\!]^\sharp(a) = a \setminus \{(x, z) \mid z \in \text{Var}*\} \cup \{(x, w) \mid (y, w) \in a\}$) is distributive, i.e.,

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

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

3 Interval Analysis

In this section, $(\mathbf{Interval}, \sqsubseteq)$ is a complete lattice as presented in class.

3.1 Question 1

Define an abstract transformer $[\![x = y + c]\!]^\sharp$ and show that it is the best transformer. (Do *not* use γ to define he transformer.)

3.2 Question 2

Let Var$*$ be a finite set of program variables.

1. Show that $(\text{Var}* \to \mathbf{Interval}, \sqsubseteq')$, where $\forall f_1, f_2 \in \text{Var}^* \to \mathbf{Interval} \colon f_1 \sqsubseteq' f_2 \iff \forall v \in \text{Var}^*, f_1(v) \sqsubseteq f_2(v)$ is a complete lattice.
2. Define a widening operator for the lattice Show that $(\text{Var}* \to \mathbf{Interval}, \sqsubseteq')$ defined above.
3. Define functions α' and γ' such that $(P(\text{Var}* \to \mathbb{Z}), \alpha', \gamma', \text{Var}* \to \mathbf{Interval})$ is a Galois connection. Is the Galois connection a Galois insertion?