Lecturecise 14
Abstract Interpretation - proofs of some lemmas

2013

Problems

A Galois connection is defined by two monotonic functions $\alpha : C \to A$ and $\gamma : A \to C$ between partial orders $\leq$ on C and $\sqsubseteq$ on A, such that

$$\forall a, c. \quad \alpha(c) \sqsubseteq a \iff c \leq \gamma(a) \qquad (*)$$

(intuitively, the condition means that c is approximated by a).

a) Show that the condition $(*)$ is equivalent to the conjunction of these two conditions:

$$\begin{array}{rrcl} \forall c. & c & \leq & \gamma(\alpha(c)) \\ \forall a. & \alpha(\gamma(a)) & \sqsubseteq & a \end{array}$$

b) Let α and γ satisfy the condition of a Galois connection. Show that the following three conditions are equivalent:
   1. $\alpha(\gamma(a)) = a$ for all a
   2. α is a surjective function
   3. γ is an injective function

c) State the condition for $c = \gamma(\alpha(c))$ to hold for all c. When C is the set of sets of concrete states and A is a domain of static analysis, is it more reasonable to expect that $c = \gamma(\alpha(c))$ or $\alpha(\gamma(a)) = a$ to be satisfied, and why?

Proof - part a)

We will show the two directions separately.

- $\Rightarrow$ Suppose $\forall a, c.\ \alpha(c) \sqsubseteq a \iff c \leq \gamma(a)$.
  It trivially holds $\forall c.\ \alpha(c) \sqsubseteq \alpha(c)$, and from the equivalence it then holds $\forall c.\ c \leq \gamma(\alpha(c))$.
  Similarly, it holds $\forall a.\ \gamma(a) \leq \gamma(a)$ and hence $\forall a.\ \alpha(\gamma(a)) \sqsubseteq a$.
- $\Leftarrow$ Suppose $\forall c.\ c \leq \gamma(\alpha(c))$ and $\forall a.\ \alpha(\gamma(a)) \sqsubseteq a$.

$$\begin{aligned}
\forall a, c.\ \alpha(c) \sqsubseteq a &\rightarrow\ \gamma(\alpha(c)) \leq \gamma(a) \\
&\rightarrow\ c \leq \gamma(\alpha(c)) \leq \gamma(a) \\
&\rightarrow\ c \leq \gamma(a)
\end{aligned}$$

$$\begin{aligned}
\forall a, c.\ c \leq \gamma(a) &\rightarrow \alpha(c) \sqsubseteq \alpha(\gamma(a)) \\
&\rightarrow \alpha(c) \sqsubseteq \alpha(\gamma(a)) \sqsubseteq a \\
&\rightarrow\ \alpha(c) \sqsubseteq a
\end{aligned}$$

Proof - part b)

In order to show this equivalence, we will show the following implications hold: $1 \Rightarrow 2$, $2 \Rightarrow 1$, $1 \Rightarrow 3$ and $3 \Rightarrow 1$.

$1 \Rightarrow 2$ Suppose $\forall a.\ \alpha(\gamma(a)) = a$, we want to show that $\forall a.\ \exists c. \alpha(c) = a$. Since $\forall a.\ \alpha(\gamma(a)) = a$, choose $c = \gamma(a)$ and we see that such a c always exists.

$2 \Rightarrow 1$ Pick an arbitrary a, then by surjectivity of α, there exists a c such that $\alpha(c) = a$.

$$\begin{aligned} \alpha(c) &= a \text{ by surjectivity} \\ c &\leq \gamma(a) \text{ by Galois connection} \\ a = \alpha(c) &\sqsubseteq \alpha(\gamma(a)) \text{ by monotonicity} \end{aligned}$$

From the definition of Galois connection, we have $\alpha(\gamma(a)) \sqsubseteq a$, hence we get $\alpha(\gamma(a)) = a$.

$1 \Rightarrow 3$ Suppose $\gamma(a) = \gamma(b)$. Then $\alpha(\gamma(a)) = \alpha(\gamma(b))$. Then since $\alpha(\gamma(a)) = a$ and $\alpha(\gamma(b)) = b$ we get $a = b$.

(Steps 1 and 3 use the two conditions of Galois connection, step 5 the injectivity.)

Proof - part b) continued

$3 \Rightarrow 1$ Suppose γ is injective, i.e. $\forall a, b.\ \gamma(a) = \gamma(b) \Rightarrow a = b$.
Show $\forall a.\ \alpha(\gamma(a)) = a$.

$$\forall a.\ \alpha(\gamma(a)) \sqsubseteq a \tag{1}$$
$$\forall a.\ \gamma(\alpha(\gamma(a))) \leq \gamma(a) \tag{2}$$
$$\forall a.\ \gamma(a) \leq \gamma(\alpha(\gamma(a))) \leq \gamma(a) \tag{3}$$
$$\Rightarrow \gamma(\alpha(\gamma(a))) = \gamma(a) \tag{4}$$
$$\Rightarrow \alpha(\gamma(a)) = a \tag{5}$$

(Steps 1 and 3 use the two conditions of Galois connection, step 5 the injectivity.)

Proof - part c)

For $c = \gamma(\alpha(c))$ to hold, γ should be surjective and α injective. If $c = \gamma(\alpha(c))$, then α is injective, and thus maps one concrete elements to exactly one abstract one. This means that we are exactly encoding the concrete domain, without doing an over-approximation, which was the point of abstract interpretation in the first place. Hence, it is more reasonable to expect $\alpha(\gamma(a)) = a$ to hold. Then we would have that for all elements in the abstract domain we would have a corresponding concrete element and the concretization function would map each abstract element to a unique set of concrete states.