Static Program Analysis

http://proglang.informatik.uni-freiburg.de/teaching/programanalysis/2014ss/

Solution Sheet 5

26.06.2014

Definitions

1. Let $(M, \leq)$ and $(N, \leq)$ be complete lattices, and $f : M \to N$. f is *(Scott) continuous* iff f preserves least upper bounds of chains, i.e. for all chains it holds that
$$f\left(\bigsqcup_{i \in I} x^{(i)}\right) = \bigsqcup_{i \in I} f(x^{(i)})$$
2. Let $(M, \leq)$ be a complete lattice, and $P : M \to \mathbb{B} = \{\texttt{true}, \texttt{false}\}$ a predicate. P is *continuous* iff for every chain $\langle x^{(i)} \rangle_{i \in I}$ in M it holds that $P(x^{(i)}) = \texttt{true}$ for all $i \in I$ implies $P(\bigsqcup_{i \in I} x^{(i)}) = \texttt{true}$.

Exercise 1

Let $(M, \leq)$ be a complete lattice, $f : M \to M$ a continuous function, and $P : M \to \mathbb{B}$ a continuous predicate. Prove that

$$P(\bot) = \texttt{true} \wedge \forall x \in M : (P(x) = \texttt{true} \Rightarrow P(f(x)) = \texttt{true})$$

implies

$$P(\mathit{lfp}(f)) = \texttt{true}$$

where $\mathit{lfp}(f)$ is the smallest fixed point of f.

Solution By induction, $P(f^{(i)}(\bot)) = \texttt{true}$ for all elements in the chain $\langle f^{(i)}(\bot) \rangle_{i \geq 0} = \bot \leq f(\bot) \leq \ldots$: The base case is $P(\bot) = \texttt{true}$, and the induction step is

$$P(f^{(i)}(\bot)) = \texttt{true} \Rightarrow P(f(f^{(i)}(\bot)) = \texttt{true} = P(f^{(i+1)}(\bot)) \tag{1}$$

P is continuous, this means that for every chain $\langle x^{(i)} \rangle_{i \in I}$ in M it holds that $P(x^{(i)}) = \texttt{true}$ for all $i \in I$ implies $P(\bigsqcup_{i \in I} x^{(i)}) = \texttt{true}$. This gives $P(\bigsqcup_{i \geq 0} f^{(i)}(\bot)) = \texttt{true}$.

Now, we show that $\bigsqcup_{i \geq 0} f^{(i)}(\bot) = \mathit{lfp}(f)$. Using that f is continuous for the chain $\langle f^{(i)}(\bot) \rangle_{i \in I}$ means that

$$f\left(\bigsqcup_{i \geq 0} f^{(i)}(\bot)\right) = \bigsqcup_{i \geq 0} f(f^{(i)}(\bot)). \tag{2}$$

Note that

$$\begin{aligned}
& \bigsqcup_{i\geq 0} f^{(i)}(\bot) \\
= \; & \bigsqcup \{f^{(i)}(\bot) \mid i \geq 0\} \\
= \; & \bigsqcup \Big(\{f^{(i+1)}(\bot) \mid i \geq 0\} \cup \{\bot\} \Big) \\
= \; & \bigsqcup \Big(\{f(f^{(i)}(\bot)) \mid i \geq 0\} \cup \{\bot\} \Big) \\
= \; & \bigsqcup \{f(f^{(i)}(\bot)) \mid i \geq 0\} \sqcup \bot \\
= \; & \bigsqcup \{f(f^{(i)}(\bot)) \mid i \geq 0\} \\
= \; & \bigsqcup_{i\geq 0} f(f^{(i)}(\bot))
\end{aligned}$$

which gives us (from equation 2) that $\bigsqcup_{i\geq 0} f^{(i)}(\bot)$ is a fixpoint. Using monotonicity it holds by induction that

$$\forall i \in \mathbb{N} : f^{(i)}(\bot) \sqsubseteq \mathit{lfp}(f)$$

- Case $i = 0 : f^{(0)}(\bot) = \bot \sqsubseteq \mathit{lfp}(f)$
- Inductive case: $f^{(i+1)}(\bot) = f(f^{(i)}(\bot)) \sqsubseteq f(\mathit{lfp}(f)) = \mathit{lfp}(f)$

So $\mathit{lfp}(f)$ is an upper bound of $f^{(i)}(\bot)$. Because $\mathit{lfp}(f)$ is the *least* fixpoint and $\bigsqcup_{i\geq 0} f^{(i)}(\bot)$ is the *least* upper bound, we have that

$$\bigsqcup_{i\geq 0} f^{(i)}(\bot) \sqsubseteq \mathit{lfp}(f) \sqsubseteq \bigsqcup_{i\geq 0} f^{(i)}(\bot).$$

It follows that $\bigsqcup_{i\geq 0} f^{(i)}(\bot) = \mathit{lfp}(f)$.

Exercise 2 (Galois connections)
Let $(A, \leq)$ and $(G, \leq)$ be partial orders, and (α, γ) be a Galois connection between A and G, i.e. for $X \in G$ and $Y \in A$ it holds:

$$X \leq \gamma(Y) \quad \Longleftrightarrow \quad \alpha(X) \leq Y$$

Which of the following statements are true? Give a proof or a counter example.

1. α monotone
2. γ monotone
3. $\alpha = \alpha \circ \gamma \circ \alpha$
4. $\gamma = \gamma \circ \alpha \circ \gamma$

Solution $\alpha(X) \leq \alpha(X)$ implies $X \leq \gamma(\alpha(X))$, and $\gamma(Y) \leq \gamma(Y)$ implies $\alpha(\gamma(Y)) \leq Y$.

1. $X_1 \leq X_2 \quad \Rightarrow \quad X_1 \leq X_2 \leq \gamma(\alpha(X_2)) \quad \Rightarrow \quad \alpha(X_1) \leq \alpha(X_2)$.
2. $Y_1 \leq Y_2 \quad \Rightarrow \quad \alpha(\gamma(Y_1) \leq Y_1 \leq Y_2 \quad \Rightarrow \quad \gamma(Y_1) \leq \gamma(Y_2)$.
3. It holds that $\alpha(\gamma(\alpha(X))) \leq \alpha(X)$ and $X \leq \gamma(\alpha(\gamma(\alpha(X))))$. Therefore, $\alpha(X) \leq \alpha(\gamma(\alpha(X)))$, and we have shown that $\alpha = \alpha \circ \gamma \circ \alpha$.
4. It holds that $\gamma(Y) \leq \gamma(\alpha(\gamma(Y)))$ and $\alpha(\gamma(\alpha(\gamma(Y)))) \leq Y$. Hence, $\gamma(\alpha(\gamma(Y))) \leq \gamma(Y)$. And finally, $\gamma = \gamma \circ \alpha \circ \gamma$.

Exercise 3
Let $(L, \leq)$ be a complete lattice, and $f : L \to L$ a monotone function. If $(L, \leq)$ satisfies the ascending chain condition (ACC), then

$$lfp(f) = \bigsqcup_n f^{(n)}(\bot)$$

Solution $\langle f^{(n)}(\bot)\rangle_{n\in\mathbb{N}}$ is an ascending chain: By definition, $\bot \leq f(\bot)$, and monotonicity of f yields $f^{(i)}(\bot) \leq f^{(i+1)}(\bot)$ for all $i \in \mathbb{N}$. By ACC, there exists $n \in \mathbb{N}$: $f^{(n)}(\bot) = f^{(n+1)}(\bot)$. Hence, $f^{(n)}(\bot) := l_0$ is a fixed point.

Let l be another fixed point, i.e. $l = f(l)$. As $\bot \leq l$ and by monotonicity of f, it holds that

$$f^{(i)}(\bot) \leq f^{(i)}(l) = l \quad \forall i \in \mathbb{N}.$$

Therefore, $l_0 \leq l$, and l_0 is lfp.

Exercise 4 (Comparing different approaches)
Consider the following WHILE program from the slides:

$[y := x]^1$;
$[z := 1]^2$;
`while` $[y > 0]^3$ `do`
    $[z := z * y]^4$;
    $[y := y - 1]^5$;
$[y := 0]^6$

Let $F : (\mathcal{P}(\mathbf{Var} \times \mathbf{Lab}))^{12} \to (\mathcal{P}(\mathbf{Var} \times \mathbf{Lab}))^{12}$ be the function defined by the data flow equations (cf. slides on p. 31 ff.). Further, let (α, γ) be the Galois connection for the Reaching Definitions analysis (cf. slides on p. 69 ff.)

1. Prove that $\vec{\alpha} \circ G \circ \vec{\gamma} \sqsubseteq F$, i.e. show that

   $$\alpha(G_j(\gamma(RD_1), \ldots, \gamma(RD_{12}))) \subseteq F_j(RD_1, \ldots, RD_{12})$$

   holds for all j. Here, $\vec{f}$ denotes the application of function f to all entries of a tuple or vector.

2. Check whether $F = \vec{\alpha} \circ G \circ \vec{\gamma}$.

3. Prove by induction over n that $(\vec{\alpha} \circ G \circ \vec{\gamma})^n(\emptyset) \sqsubseteq F^n(\emptyset)$.

4. Prove that $\vec{\alpha}(G^n(\emptyset)) \sqsubseteq (\vec{\alpha} \circ G \circ \vec{\gamma})^n(\emptyset)$. You may use that $\vec{\alpha}(\emptyset) = \emptyset$ and $G \sqsubseteq G \circ \vec{\gamma} \circ \vec{\alpha}$.

Solution

1. There are three types of equations that correspond to each other:
   a) $RD_{exit}(l) = RD_{entry}(l)$ and $CS_{exit}(l) = CS_{entry}(l)$, $RD_{entry}(l) = RD_{exit}(l-1)$ and $CS_{entry}(l) = CS_{exit}(l-1)$.
   For the tuples we get: $RD_l = RD_{l-1}$ and $CS_l = CS_{l-1}$.
   b) $RD_{exit}(l) = (RD_{entry}(l) \backslash \{(x, l) \mid l \in \mathbf{Lab}\}) \cup \{(x, l)\}$ and
   $CS_{exit}(l) = \{tr : (x, l) \mid tr \in CS_{entry}(l)\}$
   c) $RD_{entry}(l) = RD_{exit}(l-1) \cup RD_{exit}(m)$ and
   $CS_{entry}(l) = CS_{exit}(l-1) \cup CS_{exit}(m)$

a) We show as an example for $l = 3$ with $RD_{exit}(3) = RD_{entry}(3)$ and $CS_{exit}(3) = CS_{entry}(3)$ that the assumption holds. All other cases of the same form are shown analogously.

$$\begin{aligned}
\alpha \circ G_{exit}(3)(\vec{\gamma}(RD)) &= \alpha \circ G_{exit}(3)\big(\times_{i=1}^{12}\{tr \mid \forall x \in \mathbf{DOM}(tr) : \\
&\qquad\qquad (x, \mathbf{SRD}(tr)(x)) \in RD_i\}\big) \\
&= \alpha\big(\{tr \mid \forall x \in \mathbf{DOM}(tr) : (x, \mathbf{SRD}(tr)(x)) \in RD_{entry}(3)\}\big) \\
&= \Big\{(x, SRD(tr)(x)) \mid x \in \mathbf{DOM}(tr) \wedge \\
&\qquad tr \in \{tr \mid \forall x \in \mathbf{DOM}(tr) : (x, \mathbf{SRD}(tr)(x)) \in RD_{entry}(3)\}\Big\} \\
&\subseteq RD_{entry}(3) = F_{exit}(3)(RD)
\end{aligned}$$

b) Cf. book

c) similar as (a)

2. Since γ is strictly monotonic, and α and G are monotonic, $\alpha \circ G \circ \gamma$ is strictly monotonic. Further, F has a fixed point and therefore cannot be strictly monotonic. Hence, it holds that
$$\vec{\alpha} \circ G \circ \vec{\gamma} \sqsubset F$$

3. $n = 0$:
$$(\vec{\alpha} \circ G \circ \vec{\gamma})^0(\vec{\emptyset}) \sqsubseteq F^0(\vec{\emptyset}) = \vec{\emptyset}$$
$n - 1 \to n$:
$$\begin{aligned}
(\vec{\alpha} \circ G \circ \vec{\gamma})^n(\vec{\emptyset}) &= (\vec{\alpha} \circ G \circ \vec{\gamma}) \circ (\vec{\alpha} \circ G \circ \vec{\gamma})^{n-1}(\vec{\emptyset}) \\
&\sqsubseteq^{IH} (\vec{\alpha} \circ G \circ \vec{\gamma}) \circ F^{n-1}(\vec{\emptyset}) \\
&\sqsubseteq^{2.} F \circ F^{n-1}(\vec{\emptyset}) = F^n(\vec{\emptyset})
\end{aligned}$$
since F is monotone.

4. As α is monoton, we can deduce:
$$\begin{aligned}
\vec{\alpha} \circ G^n(\vec{\emptyset}) &\sqsubseteq \vec{\alpha} \circ (G \circ \vec{\gamma} \circ \vec{\alpha})^n(\vec{\emptyset}) \\
&= (\vec{\alpha} \circ G \circ \vec{\gamma})^n \circ \vec{\alpha}(\vec{\emptyset}) \\
&= (\vec{\alpha} \circ G \circ \vec{\gamma})^n(\vec{\emptyset})
\end{aligned}$$