Static Program Analysis

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

Solution Sheet 8

17.07.2014

Exercise 1 (Monotone Frameworks)
Read up Sec. 2.3 in the Nielson&Nielson book and familiarise yourself with the *Monotone Frameworks*.

1. Show that Constant Propagation (as defined in Sec. 2.3.3 of Nielson&Nielson and on the slides) is a Monotone Framework.
2. A *Bit Vector Framework* is a special instance of a Monotone Framework where
   - $L = (\mathcal{P}(D), \sqsubseteq)$ for some finite set D and where $\sqsubseteq$ is either $\subseteq$ or $\supseteq$, and
   - $\mathcal{F} = \{f : \mathcal{P}(D) \to \mathcal{P}(D) \mid \exists Y_f^1, Y_f^2 \subseteq D : \forall Y \subseteq D : f(Y) = (Y \cap Y_f^1) \cup Y_f^2\}$.

   a) Show that the Reaching Definitions Analysis is a Bit Vector Framework.

   b) Show that all Bit Vector Frameworks are indeed Distributive Frameworks.

Solution

1. We have to show that
   - $L = ((\mathbf{Var}_* \to \Sigma^\top)_\perp, \sqsubseteq)$ is a complete lattice which satisfies the Ascending Chain Condition, and
   - $\mathcal{F}_{CP} = \{f \mid f$ is a monotone function on $\widehat{\mathbf{State}_{\mathbf{CP}}}\}$ contains the identity function and is closed under function composition.

   As defined in chap. 2.3.3., L is by construction a complete lattice. It also satisfies ACC because $\mathbf{Var}_*$ is finite for a given program. Further, the identity function is monotone, and compositions of monotone functions are again monotone.

2. a) We have to show that
   - $L = (\mathcal{P}(D), \sqsubseteq)$ for a finite set D, and $\sqsubseteq$ is either $\subseteq$ or $\supseteq$, and
   - $\mathcal{F} = \{f : \mathcal{P}(D) \to \mathcal{P}(D) \mid \exists Y_f^1, Y_f^2 : \forall Y \subseteq D : f(Y) = (Y \cap Y_F^1) \cup Y_F^2\}$.

   For the RD Analysis, we have $L = (\mathcal{P}(\mathbf{Var}_* \times \mathbf{Lab}_*^?), \subseteq)$, and $\mathbf{Var}_* \times \mathbf{Lab}_*^?$ is finite. Further, set $Y_f^1 = D \setminus l_k$ and $Y_f^2 = l_g$. Then,

$$\begin{aligned} f(l) &= (l \cap (D \setminus l_k)) \cup l_g \\ &= ((l \setminus l_k) \cap D) \cup l_g \\ &= (l \setminus l_k) \cup l_g \end{aligned}$$

b) We have to show that $f(l_1 \sqcup l_1) \sqsubseteq f(l_1) \sqcup f(l_2)$.
Case $\sqsubseteq=\subseteq$:
We show that $f(l_1 \cup l_1) \subseteq f(l_1) \cup f(l_2)$:

$$\begin{aligned}
\forall Y_f^1, Y_f^2 : f(l_1 \cup l_2) &= ((l_1 \cup l_2) \cap Y_f^1) \cup Y_f^2 \\
&= ((l_1 \cap Y_f^1) \cup (l_2 \cap Y_f^1)) \cup Y_f^2 \\
&= ((l_1 \cap Y_f^1) \cup (l_2 \cap Y_f^1)) \cup (Y_f^2 \cup Y_f^2) \\
&= (((l_1 \cap Y_f^1) \cup (l_2 \cap Y_f^1)) \cup Y_f^2) \cup Y_f^2 \\
&= ((l_1 \cap Y_f^1) \cup ((l_2 \cap Y_f^1) \cup Y_f^2)) \cup Y_f^2 \\
&= (l_1 \cap Y_f^1) \cup (((l_2 \cap Y_f^1) \cup Y_f^2) \cup Y_f^2) \\
&= (l_1 \cap Y_f^1) \cup (Y_f^2 \cup ((l_2 \cap Y_f^1) \cup Y_f^2)) \\
&= ((l_1 \cap Y_f^1) \cup Y_f^2) \cup ((l_2 \cap Y_f^1) \cup Y_f^2) \\
&= f(l_2) \cup f(l_2)
\end{aligned}$$

Case $\sqsubseteq=\supseteq$:
We need to show that $f(l_1 \cap l_1) \supseteq f(l_1) \cap f(l_2)$.
The proof is the dual of the previous case.

Exercise 2 (Relations)

Consider a context free grammar with start symbol N and productions $N ::= Zero \,|\, Succ(N)$. It can be rephrased as an inductive definition:

$$Zero \in N \qquad \frac{n \in N}{Succ(n) \in N}$$

1. What set N is defined if you interpret the rules inductively? What does a coinductive interpretation yield?

2. Let us now define a relation $\leq$ on N in the following way:

$$Zero \leq n \quad \forall n \in S \qquad \frac{n \leq m}{Succ(n) \leq Succ(m)}$$

   Let $R = \{(x, y) | x, y \in N : x \leq y\} \subseteq N \times N$.

   - Define the generating function $S : \mathcal{P}(N \times N) \to \mathcal{P}(N \times N)$ for this relation. Check that S is a monotone function.
   - Can you find a pair (x, y) such that $(x, y) \in gfp(S)$, but $(x, y) \notin lfp(S)$?
   - Prove that $gfp(S)$ is transitive and reflexive.

Solution

1. The inductive definition yields the natural numbers $\mathbb{N}_0$, the coinductive definition gives $\mathbb{N}_0 \cup \infty$.

2. - We define $S(R) = \{(Zero, n) \,|\, n \in N\} \cup \{(Succ(n), Succ(m)) \,|\, (n, m) \in R\}$.
     Let $P \subseteq R$. Then,

$$\begin{aligned}
S(P) &= \{(Zero, n) \,|\, n \in N\} \cup \{(Succ(n), Succ(m)) \,|\, (n, m) \in P\} \\
&\subseteq \{(Zero, n) \,|\, n \in N\} \cup \{(Succ(n), Succ(m)) \,|\, (n, m) \in R\}
\end{aligned}$$

   - Apparently, $(n, \infty) \notin lfp(S)$, but $(n, \infty) \in gfp(S)$ for all $n \in N$.

- **Transitivity:** Since the $gfp(S)$ is S-consistent, its transitive closure $gfp(S)^+$ is also S-consistent (cf. Lemma in the lecture). Therefore, $gfp(S)^+ \subseteq gfp(S)$.

  By definition of the transitive closure, it holds that $gfp(S) \subseteq gfp(S)^+$. Hence, $gfp(S) = gfp(S)^+$, and the transitive closure is obviously transitive.

  Reflexivity: Let $I = \{(x,x) \mid x \in N\}$ be the identity relation. I is S-consistent:

$$\begin{aligned} I \subseteq S(I) &= \{(Zero, n) \mid n \in N\} \cup \{(Succ(n), Succ(m)) \mid (n,m) \in I\} \\ &= \{(Zero, n) \mid n \in N\} \cup \{(Succ(x), Succ(x)) \mid x \in N\} \end{aligned}$$

  Hence, $I \subseteq gfp(S)$ by the coinduction principle. Therefore, $gfp(S)$ is reflexive.