Lecture: Program analysis
Exercise 2
`http://proglang.informatik.uni-freiburg.de/teaching/programanalysis/2010ss/`

Exercise 1: Complete lattices

1. Let $M = \{a, b, c\}$. Define a relation R such that (M, R) is a complete lattice.
2. For a totally ordered set S, $(\mathcal{P}(S), \subseteq)$ is a complete lattice. Define another relation R such that $(\mathcal{P}(S), R)$ is a complete lattice.
3. Is $(\mathbb{R}, \leq)$ a complete lattice? If not, how can you extend $\mathbb{R}$ such that it becomes a complete lattice?
4. Let $|$ be the relation of divisibility, i.e. $a \mid b$ means a divides b. Is
   - $(\mathbb{N}, |)$
   - $(\mathbb{N}\backslash\{0\}, |)$
   - $(\mathbb{N}\backslash\{0\} \cup \{\infty\}, |)$

   a complete lattice?

Solution

1. Define $a < b$ and $b < c$. Then $(M, \leq)$ is a complete lattice where $\leq$ is the reflexive and transitive hull of $<$.
2. An easy solution is $(\mathcal{P}(S), \supseteq)$. Another relation can be constructed like this: Let $<$ be a total order on S. You can order all elements of a subset of S with $<$. Using this, you can construct a monotonic sequence of the subset (**Careful!** This does not work in general! For this to work, the subset must have a least element). If we take the lexicographical order $<_l$ on these sequences, we get again a complete lattice for $(\mathcal{P}(S), <_l)$.
3. $(\mathbb{R}, \leq)$ is not a complete lattice. For example, $\sqcup\mathbb{N}$ does not exist. The extension $(\mathbb{R} \cup \{\pm\infty\}, \leq)$ with
$$\forall x \in \mathbb{R} : -\infty < x < +\infty \tag{1}$$
   is a complete lattice.
4. $a \mid b$ is defined as $\exists c : a \cdot c = b$.
   - $|$ is reflexive: $\forall a\, \exists c : a \cdot c = a$. Choose $c = 1$.
   - $|$ is transitive: $\forall a, b, c$ with $\exists d : a \cdot d = b$ and $\exists d' : b \cdot d' = c$. Then $\exists e : a \cdot e = c$. Choose $e = d \cdot d'$.
   - $|$ is antisymmetric: $\forall a, b$ with $\exists c : a \cdot c = b$ and $\exists c' : b \cdot c' = a \quad \Rightarrow a \cdot cc' = a \quad \Rightarrow cc' = 1 \quad \Rightarrow c = c' = 1 \quad \Rightarrow a = b$.

   Hence, $(\mathbb{N}, |)$ is a partially ordered set. Let $M \subseteq \mathbb{N}$. We have to distinguish now two cases:

   - $|M| \in \mathbb{N}$ and $0 \notin M$. Then, $\sqcap M = gcd(M)$ (greatest common divisor) and $\sqcup M = lcm(M)$ (least common multiple).
   - $|M| = \infty$ or $0 \in M$. Then, $\sqcap M = gcd(M\backslash\{0\})$ and $\sqcup M = 0$.

   In particular, $\top = 0$ and $\bot = 1$. Hence, $(\mathbb{N}, |)$ is a complete lattice.
   Because $(\mathbb{N}\backslash\{0\}, |)$ has no greatest element, it is not a complete lattice.
   $(\mathbb{N}\backslash\{0\} \cup \{\infty\}, |)$ is again a complete lattice with $\top = \infty$.

Exercise 2: 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 $G \sqsubseteq G \circ \vec{\gamma} \circ \vec{\alpha}$.

Definitions The signatures of the functions are:

$$\begin{aligned} F :&\quad (\mathcal{P}(\mathbf{Var} \times \mathbf{Lab}))^{12} \longrightarrow (\mathcal{P}(\mathbf{Var} \times \mathbf{Lab}))^{12} \\ G :&\quad (\mathcal{P}(\mathbf{Trace}))^{12} \longrightarrow (\mathcal{P}(\mathbf{Trace}))^{12} \\ \alpha :&\quad \mathcal{P}(\mathbf{Trace}) \longrightarrow \mathcal{P}(\mathbf{Var} \times \mathbf{Lab}) \\ \gamma :&\quad \mathcal{P}(\mathbf{Var} \times \mathbf{Lab}) \longrightarrow \mathcal{P}(\mathbf{Trace}) \end{aligned}$$

α and γ are defined as follows:

$$\begin{aligned} \alpha(X) &= \{(x, \mathrm{SRD}(tr)(x) \mid x \in \mathrm{DOM}(tr) \land tr \in X)\} \\ \gamma(Y) &= \{tr \mid \forall x \in \mathrm{DOM}(tr) : (x, \mathrm{SRD}(tr)(x)) \in Y\} \end{aligned}$$

where $\mathrm{SRD}(tr)(x)$ returns the label where the variable x has been set last in trace tr. $\mathrm{DOM}(tr)$ is the set of variables for which SRD is defined.

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.

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

(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. $n = 0$:

$$(\vec{\alpha} \circ G \circ \vec{\gamma})^0(\emptyset) \sqsubseteq F^0(\emptyset) = \emptyset$$

$n - 1 \rightarrow n$:

$$\begin{aligned}
(\vec{\alpha} \circ G \circ \vec{\gamma})^n(\emptyset) &= (\vec{\alpha} \circ G \circ \vec{\gamma})^{n-1}(\vec{\alpha} \circ G \circ \vec{\gamma})(\emptyset) \\
&\leq^{IH} F^{n-1}(\vec{\alpha} \circ G \circ \vec{\gamma}(\emptyset)) \\
&\leq F^{n-1}(F(\emptyset)) = F^n(\emptyset)
\end{aligned}$$

since F is monotone.

4. As α is monoton, we can deduce:

$$\begin{aligned}
\vec{\alpha} \circ G^n(\emptyset) &\sqsubseteq \vec{\alpha} \circ (G \circ \vec{\gamma} \circ \vec{\alpha})^n(\emptyset) \\
&= (\vec{\alpha} \circ G \circ \vec{\gamma})^n \circ \vec{\alpha}(\emptyset) \\
&= (\vec{\alpha} \circ G \circ \vec{\gamma})^n(\emptyset)
\end{aligned}$$