

Exercise Sheet 3

General remarks:

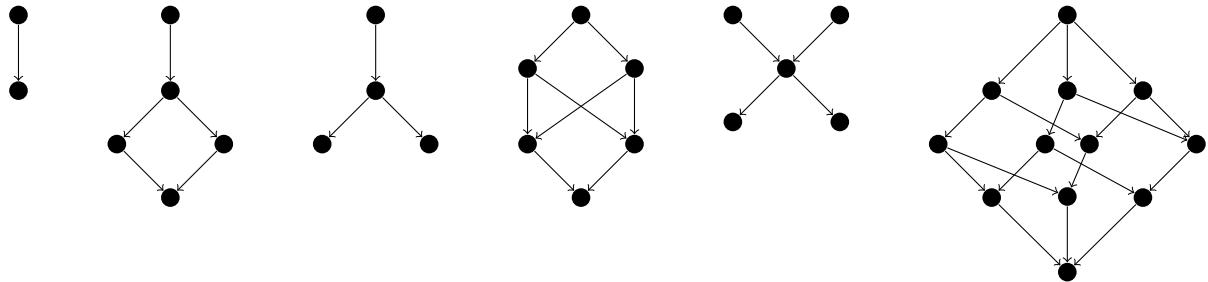
- **Due date:** December 23th.
- Since there is **no exercise class on December 23th**, you may either submit your solution via email to prop1617@i2.informatik.rwth-aachen.de, or put your solutions into the box labeled *Static Program Analysis* at the chair. In the latter case, please make sure to mark them as submissions to Probabilistic Programming.
- Solutions must be written in English.
- If you have any questions regarding the lecture or the exercise, feel free to write us an email or visit us at the chair.

Exercise 1 (Recapitulation of Complete Lattices)

12%

One can depict a finite partial order as a graph, where the elements are represented by the nodes and the order relation is given as (the transitive closure of) directed edges (we omit the trivial self-loops at every node). Here, an edge from node u to node v indicates that $v \sqsubseteq u$ and that there is no element that lies ‘in between’, i.e., there is no $u \neq w \neq v$ such that $v \sqsubseteq w \sqsubseteq u$.

Decide for each of the following graphs whether it represents a complete lattice. Justify your answer.



Solution:

Assume that the graph depicts the PO where greater elements are arranged above elements of lower order.

- Yes. Lattice graphs satisfy all PO-conditions by definition. Furthermore all subsets of nodes have a least upper as well as a greatest lower bound in the PO.
- Yes. Same situation as in the first graph.
- No. This graph/PO has no GLB. Thus does not represent a lattice.
- No. In this graph there exists a subset (two nodes on same height), that have no GLB/LUB. E.g. the LUB of the PO is an upper bound, but not the LUB of nodes four and five.
- No. This graph/PO has neither GLB nor LUB.
- Yes.

Exercise 2 (Computing Weakest Preconditions)
38%

Recall that by the continuity of transformer **wp**, the weakest pre-expectation of a **pGCL** loop can be given by

$$\mathbf{wp}[\mathbf{while}(G) \{body\}](f) = \sup_n F^n(\mathbf{0}) ,$$

where $F(X) = [G] \cdot \mathbf{wp}[body](X) + [\neg G] \cdot f$, $\mathbf{0}$ is the constantly 0 expectation and F^n is the composition of F with itself n times, i.e. $F^0 = id$ and $F^{n+1} = F \circ F^n$. Using this formula,

(a) [15%] Give a closed form of

$$\mathbf{wp}[\mathbf{while}(c = 1) \{c := 0 \ [1/2] \ c := 1\}](f) .$$

Solution: We begin calculating F

$$\begin{aligned} F(X) &= [c = 1] \cdot \mathbf{wp}[c := 0 \ [1/2] \ c := 1](X) + [c \neq 1] \cdot f \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot \mathbf{wp}[c := 0](X) + \frac{1}{2} \cdot \mathbf{wp}[c := 1](X) \right) + [c \neq 1] \cdot f \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot X[0 \leftarrow c] + \frac{1}{2} \cdot X[1 \leftarrow c] \right) + [c \neq 1] \cdot f \end{aligned}$$

and then continue with the “powers” of F

$$\begin{aligned} F^0(\mathbf{0}) &= id(\mathbf{0}) = \mathbf{0} \\ F^1(\mathbf{0}) &= F(\mathbf{0}) = [c \neq 1] \cdot f \\ F^2(\mathbf{0}) &= F([c \neq 1] \cdot f) \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot \underbrace{([c \neq 1] \cdot f)[0 \leftarrow c]}_{= f[0 \leftarrow c]} + \frac{1}{2} \cdot \underbrace{([c \neq 1] \cdot f)[1 \leftarrow c]}_{= \mathbf{0}} \right) + [c \neq 1] \cdot f \\ &= \frac{1}{2} \cdot [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f \\ F^3(\mathbf{0}) &= F\left(\frac{1}{2} \cdot [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f\right) \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot \underbrace{\left(\frac{1}{2} \cdot [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f \right)[0 \leftarrow c]}_{= f[0 \leftarrow c]} + \right. \\ &\quad \left. \frac{1}{2} \cdot \underbrace{\left(\frac{1}{2} \cdot [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f \right)[1 \leftarrow c]}_{= 1/2 \cdot f[0 \leftarrow c]} \right) + [c \neq 1] \cdot f \\ &= \frac{3}{4} \cdot [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f \\ F^4(\mathbf{0}) &= \frac{7}{8} \cdot [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f \end{aligned}$$

In general we have that for $n \geq 0$,

$$F^{n+1}(\mathbf{0}) = \left(\frac{2^n - 1}{2^n} \right) \cdot [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f ,$$

for which

$$\mathbf{wp}[\mathbf{while}(c = 1) \{c := 0 \ [1/2] \ c := 1\}](f) = [c = 1] \cdot f[0 \leftarrow c] + [c \neq 1] \cdot f .$$

(b) [15%] Given loop

$$\text{wp}[\text{while } (c = 1) \{c := 0 \text{ [1/2]} \ x := x + 1\}](x) ,$$

you are asked to: First, compute $F^0(\mathbf{0})$, $F^1(\mathbf{0})$, $F^2(\mathbf{0})$ and $F^3(\mathbf{0})$. Second, use these first terms of the sequence to infer the general form of $F^n(\mathbf{0})$.

Solution: We begin calculating F

$$\begin{aligned} F(X) &= [c = 1] \cdot \text{wp}[c := 0 \text{ [1/2]} \ x := x + 1](X) + [c \neq 1] \cdot x \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot \text{wp}[c := 0](X) + \frac{1}{2} \cdot \text{wp}[x := x + 1](X) \right) + [c \neq 1] \cdot x \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot X[0 \leftarrow c] + \frac{1}{2} \cdot X[x + 1 \leftarrow x] \right) + [c \neq 1] \cdot x \end{aligned}$$

and then continue with the “powers” of F

$$\begin{aligned} F^0(\mathbf{0}) &= id(\mathbf{0}) = \mathbf{0} \\ F^1(\mathbf{0}) &= F(\mathbf{0}) = [c \neq 1] \cdot x \\ F^2(\mathbf{0}) &= F([c \neq 1] \cdot x) \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot \underbrace{([c \neq 1] \cdot x)[0 \leftarrow c]}_{= x} + \frac{1}{2} \cdot \underbrace{([c \neq 1] \cdot x)[x + 1 \leftarrow x]}_{= [c \neq 1] \cdot (x+1)} \right) + [c \neq 1] \cdot x \\ &= [c = 1] \cdot \frac{1}{2} \cdot x + [c \neq 1] \cdot x \\ F^3(\mathbf{0}) &= F\left(\frac{1}{2} \cdot [c = 1] \cdot x + [c \neq 1] \cdot x\right) \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot \underbrace{([c = 1] \cdot \frac{1}{2} \cdot x + [c \neq 1] \cdot x)[0 \leftarrow c]}_{= x} + \right. \\ &\quad \left. \frac{1}{2} \cdot \underbrace{([c = 1] \cdot \frac{1}{2} \cdot x + [c \neq 1] \cdot x)[x + 1 \leftarrow x]}_{= [c=1] \cdot \frac{1}{2} \cdot (x+1) + [c \neq 1] \cdot (x+1)} \right) + [c \neq 1] \cdot x \\ &= [c = 1] \cdot \left(\frac{1}{2} \cdot x + \frac{1}{4} \cdot (x + 1) \right) + [c \neq 1] \cdot x \end{aligned}$$

In general we will have that for $n \geq 1$,

$$F^n(\mathbf{0}) = [c = 1] \cdot \sum_{1 \leq i < n} \left(\frac{1}{2}\right)^i \cdot (x + i - 1) + [c \neq 1] \cdot x ,$$

for which

$$\text{wp}[\text{while } (c = 1) \{c := 0 \text{ [1/2]} \ x := x + 1\}](x) = [c = 1] \cdot \sum_{i=1}^{\infty} \left(\frac{1}{2}\right)^i \cdot (x + i - 1) + [c \neq 1] \cdot x .$$

(c) [8%] Use the result above to compute the expected value of variable x after running program

$$x := 0; \text{ while } (c = 1) \{c := 0 \text{ [1/2]} \ x := x + 1\} .$$

Solution: Call the above loop *loop*. Then the expected value of x after running the program is

$$\begin{aligned}\text{wp}[x := 0; \text{loop}](x) &= \text{wp}[x := 0](\text{wp}[\text{loop}](x)) \\ &= \text{wp}[x := 0]\left([c = 1] \cdot \sum_{i=1}^{\infty} (1/2)^i \cdot (x + i - 1) + [c \neq 1] \cdot x\right) \\ &= [c = 1] \cdot \sum_{i=1}^{\infty} (1/2)^i \cdot (i - 1)\end{aligned}$$

Using the fact that $\sum_{i=1}^{\infty} p^i (i - 1) = \frac{p^2}{(1-p)^2}$ for $|p| < 1$, we conclude that

$$= [c = 1] \cdot 1 ,$$

Or colloquially, that the expected value of x is 1 when the program is started in a state with $c = 1$ and 0 otherwise.

Exercise 3 (On Greatest Fixpoints)

15%

Let $(D, \sqsubseteq)$ be a complete lattice and $f : D \rightarrow D$ be a monotonic function. Show that for every $d \in D$, $d \sqsubseteq f(d)$ implies $d \sqsubseteq \nu f$, where νf denotes the *greatest* fixpoint of f .

Hint. Under the above hypotheses, the greatest fixed point νf can be obtained as $\nu f = \inf_n f^n(\top)$ where $\top$ is the top or greatest element of the lattice.

Solution: Let $d \sqsubseteq f(d)$. Using the above hint, statement $d \sqsubseteq \nu f = \inf_n f^n(\top)$ then follows from

$$\forall n. d \sqsubseteq f^n(\top) ,$$

which we prove by induction on n . The base case is immediate since it reduces to $d \sqsubseteq f^0(\top) = \top$. For the inductive case we reason as follows

$$\begin{aligned}d \sqsubseteq f^{n+1}(\top) & \\ \Leftarrow & \langle d \sqsubseteq f(d), \text{transit. of } \sqsubseteq \rangle \\ f(d) \sqsubseteq f^{n+1}(\top) & \\ \Leftrightarrow & \langle \text{def. } f^{n+1} \rangle \\ f(d) \sqsubseteq f(f^n(\top)) & \\ \Leftarrow & \langle f \text{ monotonic} \rangle \\ d \sqsubseteq f^n(\top) & \\ \Leftarrow & \langle \text{I.H.} \rangle \\ \text{true} & \end{aligned}$$

Exercise 4 (Liberal Probabilistic Invariants)

20%

In addition to the weakest precondition semantics from the lecture, we can also define a weakest *liberal* precondition (wlp) semantics. The corresponding transformer **wlp** is

defined just like **wp** except that $\text{wp}[\text{abort}](f) = \mathbf{1}$ and we take the *greatest* fixpoint for loops instead of the least fixpoint. More formally, we have

$$\text{wp}[\text{while } (G) \{C\}](f) = \nu X. ([\neg G] \cdot f + [G] \cdot \text{wp}[C](X)).$$

Show that probabilistic loop invariants of **wp** imply (in the sense of $\leq$) the **wp** of the whole loop w.r.t. postexpectation $[\neg G] \cdot I$. Formally, show that

$$[G] \cdot I \leq \text{wp}[C](I) \text{ implies } I \leq \text{wp}[\text{while } (G) \{C\}]([\neg G] \cdot I).$$

Solution: Assume that $[G] \cdot I \leq \text{wp}[C](I)$. We first show that I as specified above is a fixed point of the functional F given by

$$X \mapsto [\neg G] \cdot [\neg G] \cdot I + [G] \cdot \text{wp}[C](X)$$

.

$$\begin{aligned} F(I) &= [\neg G] \cdot [\neg G] \cdot I + [G] \cdot \text{wp}[C](I) \\ &\geq [\neg G] \cdot [\neg G] \cdot I + [G] \cdot [G] \cdot I && \text{(assumption)} \\ &= ([\neg G] + [G]) \cdot I = I. \end{aligned}$$

Thus, we have $F(I) \geq I$. By task 3, this means that $I \leq \nu X. F(X)$ and thus

$$I \leq \nu X. F(X) = \text{wp}[\text{while } (G) \{C\}]([\neg G] \cdot I).$$

Exercise 5 (Probabilistic Invariants)

15%

Let $I \leq \mathbf{1}$ be an expectation. Recall that I is a probabilistic invariant of program $P = \text{while } (G) \{C\}$ whenever $[G] \cdot I \leq \text{wp}[C](I)$.

Show that the probabilistic invariants provided in the lecture are sound for almost surely terminating programs. More formally, show that

$$I \leq \text{wp}[P]([\neg G] \cdot I) = \mu X ([\neg G] \cdot I + [G] \cdot \text{wp}[C](X)).$$

whenever I is a probabilistic invariant as above and $\text{wp}[P](\mathbf{1}) = \mathbf{1}$.

Hint: You may assume that we already know for all expectations $f, g \leq \mathbf{1}$ and programs C that

$$\max\{\text{wp}[C](f) + \text{wp}[C](g) - 1, 0\} \leq \text{wp}[C](\max\{f + g - 1, 0\}).$$

Solution:

$$\begin{aligned} & \text{wp}[P](\neg G \cdot I) \\ = & \text{wp}[P](\neg G \cdot I + \mathbf{1} - \mathbf{1}) \\ = & \text{wp}[P](\neg G \cdot I + \text{wp}[P](\mathbf{1}) - \mathbf{1}) & (\text{wp}[P](\mathbf{1}) = \mathbf{1}) \\ \geq & \text{wlp}[P](\neg G \cdot I) + \text{wp}[P](\text{wp}[P](\mathbf{1})) - \text{wp}[P](\mathbf{1}) & (\text{using hint}) \\ = & \text{wlp}[P](\neg G \cdot I) + \mathbf{1} - \mathbf{1} \\ = & \text{wlp}[P](\neg G \cdot I) \\ \geq & I & (\text{using Ex. 4}) \end{aligned}$$