Technische Universität Wien
Compilers and Languages
Prof. J. Knoop

A-1040 Wien
Argentinierstr. 8
Tel.: 01-58801-18510

" Analysis and Verification (185.276, VU 2.0, ECTS 3.0) " SS 2019

Assignment 4

10 April 2019

Exercise 1 : (4+4 Points)

Give a While program π, for which the Hoare assertion

$$\{true\} \quad \pi \ \{false\}$$

is partially correct, and prove your claim in two ways, by providing

1. a tree-like proof
2. a linear proof sketch

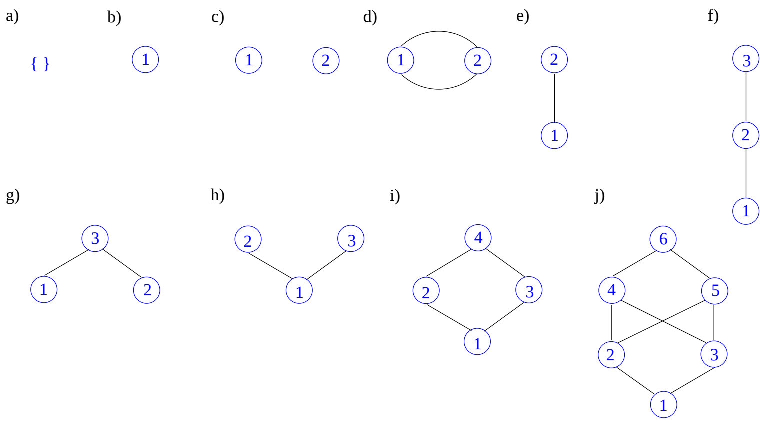
Exercise 2 : (8 Points)

Prove that the While program computing the product of two numbers of Assignment 3 is also totally correct wrt the precondition $x = n \ \wedge y = m \ \wedge \ n > 1$ and the postcondition $y = n * m$, i.e., prove the validity of the Hoare assertion:

$$[x = n \ \wedge y = m \ \wedge \ n > 1] \ \ \textbf{while} \ x \neq 1 \ \mathrm{y} := y + m; \ x := x - 1 \ \textbf{od} \ \ [y = n * m]$$

Exercise 3 : (10 Points)

Consider the below (pre-) orders given by their Hasse diagrams (resp. Hasse-like diagrams):



Which of these orders are (i) partial orders (dtsch. partielle Ordnungen), which ones are (ii) chain-complete partial orders CCPOs (dtsch. (ketten-) vollständige partielle Ordnungen (KV-POs)), (ii) lattices (dtsch. Verbände), which ones are (iii) complete lattices (dtsch. vollständige Verbändec)? Explain your reasoning (proof or counterexample).

Note: Partial orders and Hasse diagrams are introduced in Appendices A.2.1 and A.2.2, respectively, lattices and complete lattices in Appendix A.4.

Exercise 4 : (4 Points)

Which of the following pairs are i) partial orders, (ii) (chain) complete partial orders, (iii) lattices, (iv) complete lattices? Explain your reasoning (proof or counterexample).

1. $(ST, \sqsubseteq)$ with
   - $ST =_{\text{df}} [\Sigma \to \Sigma]$ the set of state transformations.
   - $\sqsubseteq \subseteq ST \times ST$ defined by:

     $\forall\, g_1, g_2 \in ST.\ g_1 \sqsubseteq g_2 \iff_{df}$

     $\forall\, \sigma \in \Sigma.\ g_1(\sigma)\ \mathit{defined} = \sigma' \Rightarrow g_2(\sigma)\ \mathit{defined} = \sigma'$
2. $(\mathcal{P}(S), \subseteq)$ with S finite set, $\subseteq$ subset relation, and $\mathcal{P}$ powerset operator, i.e., $\mathcal{P}(S) =_{\text{df}} \{S' \mid S' \subseteq S\}$.
3. $(\mathcal{P}(S), \subseteq)$ with S nonfinite set, $\subseteq$ subset relation and $\mathcal{P}$ powerset operator.
4. $(\mathcal{P}_{fin}(S), \subseteq)$ with S nonfinite set, $\subseteq$ subset relation and $\mathcal{P}_{fin}$ 'finite' powerset operator, i.e., $\mathcal{P}_{fin}(S) =_{\text{df}} \{S' \mid S' \subseteq S,\ S'\ \mathit{finite}\}$.

Exercise 5 : (4 Points)

Prove or refute (proof or counterexample):

1. Every CCPO $(S, \sqsubseteq)$ is a lattice: $(S, \sqsubseteq)\ \mathit{CCPO} \Rightarrow (S, \sqsubseteq)\ \mathit{lattice}$.
2. Every CCPO $(S, \sqsubseteq)$ is a complete lattice: $(S, \sqsubseteq)\ \mathit{CCPO} \Rightarrow (S, \sqsubseteq)\ \mathit{complete\ lattice}$.
3. Every lattice $(S, \sqsubseteq)$ is a CCPO: $(S, \sqsubseteq)\ \mathit{lattice} \Rightarrow (S, \sqsubseteq)\ \mathit{CCPO}$.
4. Every complete lattice $(S, \sqsubseteq)$ is a CCPO: $(S, \sqsubseteq)\ \mathit{complete\ lattice} \Rightarrow (S, \sqsubseteq)\ \mathit{CCPO}$.

Exercise 6: (Without Submission)

Install the KeY-Hoare system (cf. Chapter 4.9 for the system's URL) and conduct correctness proofs for the following three Hoare assertions:

- $\models_{pk}\ \{\mathit{true}\}\ \textbf{while}\ \mathit{true}\ \textbf{do}\ \mathit{skip}\ \textbf{od}\ \{\mathit{false}\}$
- $\models_{pk}\ \{x = n\ \wedge y = m\}\ \textbf{while}\ x \neq 1\ \textbf{do}\ y := y + m;\ x := x - 1\ \textbf{od}\ \{y = n * m\}$
- $\models_{tk}\ [x = n\ \wedge y = m\ \wedge\ n > 1]\ \textbf{while}\ x \neq 1\ \textbf{do}\ y := y + m;\ x := x - 1\ \textbf{od}\ [y = n * m]$

The proofs shall be (voluntarily) presented "live" on May 15, 2019.

Submission: Wednesday, 15 May 2019, before the lecture.