University of Tartu *Fall 2014*
Department of Computer Science *Vesal Vojdani*

Formal Methods in Software Engineering

`Exercise sheet 3`

Exercise 1: *Implication Ordering* *2 Points*

For a program point $p \in N$ and lattice element $d \in \mathbb{D}$, we define $p \vDash d$ to mean that whenever program execution reaches p, the condition imposed by d holds. This condition will be defined in different ways below, but in each case, the ordering of the lattice elements $d_1, d_2 \in \mathbb{D}$ should be such that for $d_1 \sqsubseteq d_2$, we have $(p \vDash d_1) \implies (p \vDash d_2)$. That is, whenever the claim represented by d_1 holds, also that of d_2 is true.

For the following lattices and definitions of $p \vDash d$, indicate how the lattice needs to be ordered so that $d_1 \sqsubseteq d_2$ respects the above implication ordering.

a) Let $\mathbb{D} = 2^V$, where V is the set of variables in the program. For any $X \subseteq V$, let $p \vDash X$ be the claim "every $v \in X$ is initialized along all paths to p."
b) Again, let $\mathbb{D} = 2^V$, but now $p \vDash X$ means "if a variable v is read at some program point reachable from p, then $v \in X$." (In other words, only variables in X are possibly read.)
c) Now let $\mathbb{D}$ be the set of logical formulas, and $p \vDash \phi$ holds if $S_p \vDash \phi$, where S_p is the set of program states reaching program point p.
d) Let $\mathbb{D}$ again be logical formulas, but now we fix a post-condition ψ that should hold at the exit node r of the program, and $p \vDash \phi$ if ϕ is a pre-condition for ψ; that is, $p \vDash \phi$ is the claim "if $S_p \vDash \phi$, then $S_r \vDash \psi$".

Exercise 2: *Kleene iteration* *4 Points*

Solve the following constraint system over the domain $\mathbb{D} = 2^{\mathbb{Z}\times\mathbb{Z}}$ using Kleene iteration:

$$
\begin{aligned}
S_1 &\supseteq \{\langle 1, 5\rangle\} \\
S_2 &\supseteq S_1 \cup \{\langle a-1, b+1\rangle \mid \langle a, b\rangle \in S_3\} \\
S_3 &\supseteq \{\langle a, b\rangle \in S_2 \mid a \neq 0\} \\
S_4 &\supseteq \{\langle a, b\rangle \in S_2 \mid a = 0\}
\end{aligned}
$$

Exercise 3: *Complete Lattice* *4 Points*

Recall that we defined a complete lattice $\mathbb{D}$ as a partially ordered set where every subset $S \subseteq D$ has a least upper bound $\bigsqcup S$.

Show that if a partially ordered set P has a greatest element $\top \in P$ and every non-empty subset $\emptyset \neq S \subseteq P$ has a greatest lower bound $\bigsqcap S \in P$, then P is a complete lattice.