Exercise 1 (30 points). Let $P$ and $Q$ be finite sets of predicates such that $P \supseteq Q$. Define functions $\alpha : \text{Cubes}(P) \to \text{Cubes}(Q)$ and $\gamma : \text{Cubes}(Q) \to \text{Cubes}(P)$ that are monotonic with respect to $|=|$ and form a Galois insertion $\text{Cubes}(P) \xrightarrow{\gamma} \text{Cubes}(Q)$ for lattices $(\text{Cubes}(P),|=|)$ and $(\text{Cubes}(Q),|=|)$ (where in each of them the logically equivalent formulas are considered identical, in order to ensure antisymmetry of $|=|$). Prove that the defined functions $\alpha$ and $\gamma$ have the required properties.

Exercise 2 (40 points). Consider a program $c$ and a safety property defined by giving a program location $c_{\text{bad}}$. Consider the abstract semantics of $c$ with respect to a finite set of predicates $P$. Let $(c, \text{true}) \Rightarrow (c_1, q_1) \Rightarrow \ldots \Rightarrow (c_k, q_k)$ be a spurious abstract counterexample and let $r_1, \ldots, r_k$ be the corresponding sequence of commands. Let the formulas $b_0, b_1, \ldots, b_k$ be defined by

- $b_0 := \text{true}$,
- $b_i := \text{sp}(b_{i-1}, r_i)$ for $1 \leq i \leq k$.

and the formulas $p_0, p_1, \ldots, p_k$ be defined by

- $p_k := \text{false}$,
- $p_i := \text{wp}(r_{i+1}, p_{i+1})$ for $0 \leq i < k$.

Prove that $b_i |= p_i$ for each $i = 0, \ldots, k$. 

1
Exercise 3 (30 points). Consider the following program $c$ and the safety property that states that block 5 is not reachable.

$$
[x:=y]^1;
\text{if } [y>0]^2 \text{ then } \{ \\
[x:=x-1]^3; \\
\text{if } [x<0]^4 \text{ then } \{ \\
[\text{skip}]^5 \\
\} \\
\text{else } \{ \\
[\text{skip}]^6 \\
\} \\
\} \\
\text{else } \{ \\
[\text{skip}]^7 \\
\}
$$

Consider the abstraction of $c$ w.r.t. the set of predicates $P = \{x<0, y>0\}$.

a) Give an abstract counterexample.

b) Give the strongest postconditions for this abstract counterexample.

Determine whether the abstract counterexample is spurious.

c) Use this abstract counterexample to refine the abstraction.

Does the safety property hold in the refined abstraction?