Homework 4 - Abstract interpretation

Problem 1

Let $C[0,1]$ be the set of continuous functions from $[0,1]$ to the reals. Define $\leq$ on $C[0,1]$ by $f \leq g$ if and only if $f(a) \leq g(a)$ for all $a \in [0,1]$. Show that $\leq$ is a partial order and that $C[0,1]$ with this order forms a lattice.

Problem 2

Recall that Tarski's fixed-point theorem says, that if we have a complete lattice and a monotonic function on this lattice, then the least fixed point always exists. Note that the theorem is not constructive, i.e. it does not provide an algorithm for computing this fixed point. In this exercise you'll see what happens in the case of discontinuous functions.

Let $A = [0,1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ be the interval of real numbers. Recall that, by definition of real numbers and complete lattice, $(A, \leq)$ is a complete lattice with least lattice element 0 and greatest lattice element 1. Here $\sqcup$ is the least upper bound operator on sets of real numbers, also called *supremum* and denoted *sup* in real analysis.
Let function $f : A \to A$ be given by

$$f(x) = \begin{cases} \frac{1}{2} + \frac{1}{4}x, & \text{if } x \in [0, \frac{2}{3}) \\ \frac{3}{5} + \frac{1}{5}x, & \text{if } x \in [\frac{2}{3}, 1] \end{cases}$$

(It may help you to try to draw f.)

a) Show that f is monotonic and injective (so it is strictly monotonic).

b) Compute the set of fixpoints of f.

c) Define $\mathit{iter}(x) = \sqcup\{f^n(x) \mid n \in \{0, 1, 2, \ldots\}\}$. (This is in fact equal to $\lim_{n\to\infty} f^n(x)$ when f is a monotonic bounded function.)

   Compute $\mathit{iter}(0)$ (show that the computed value is correct by definition of *iter*, that is, that the value is indeed $\sqcup$ of the set of values). Is $\mathit{iter}(0)$ a fixpoint of f? Is $\mathit{iter}(\mathit{iter}(0))$ a fixpoint of f?

Problem 3

A Galois connection is defined by two monotonic functions $\alpha : C \to A$ and $\gamma : A \to C$ between partial orders $\leq$ on C and $\sqsubseteq$ on A, such that

$$\alpha(c) \sqsubseteq a \iff c \leq \gamma(a) \qquad (*)$$

for all c and a (intuitively, the condition means that c is approximated by a).

a) Show that the condition $(*)$ is equivalent to the conjunction of these two conditions:

$$\begin{array}{lrcl} \forall c. & c & \leq & \gamma(\alpha(c)) \\ \forall a. & \alpha(\gamma(a)) & \sqsubseteq & a \end{array}$$

b) Let α and γ satisfy the condition of a Galois connection. Show that the following three conditions are equivalent:

1. $\alpha(\gamma(a)) = a$ for all a
2. α is a surjective function
3. γ is an injective function

c) State the condition for $c = \gamma(\alpha(c))$ to hold for all c. When C is the set of sets of concrete states and A is a domain of static analysis, is it more reasonable to expect that $c = \gamma(\alpha(c))$ or $\alpha(\gamma(a)) = a$ to be satisfied, and why?

Problem 4

Suppose you are given a set of predicates $\cap P = \{P_0, P_1, \ldots, P_n\}$ in a decidable theory of first-order logic (for example, quantifier-free formulas in the combination of uninterpreted function symbols with integer linear arithmetic) where P_0 is the predicate 'false'.

a) Consider conjunctions of predicates as an abstract interpretation domain. Give an example showing that it need not be the case that

$$a_1 \leq a_2 \leftrightarrow \gamma(a_1) \subseteq \gamma(a_2)$$

b) Describe how to construct from A a new, smaller, lattice B, where the above equivalence holds. Is there an algorithm to compute B and the partial order on B using a decision procedure for the logic of predicates?

c) Suppose that, for the same set of predicates, we use lattice A and lattice B to compute the fixpoints g_A and g_B of the function $F^{\#}$ from the Abstract Interpretation Recipe (see course wiki). What can you say about

i) the comparison of numbers of iterations needed to compute the fixpoint g_A and g_B (is one always less than the other, can they be equal, does it depend on set $\mathcal{P}$ of predicates)

ii) the precision of computed information, that is, comparison of sets $\gamma(g_A(p))$ and $\gamma(g_B(p))$ for an arbitrary program point $p \in V$.