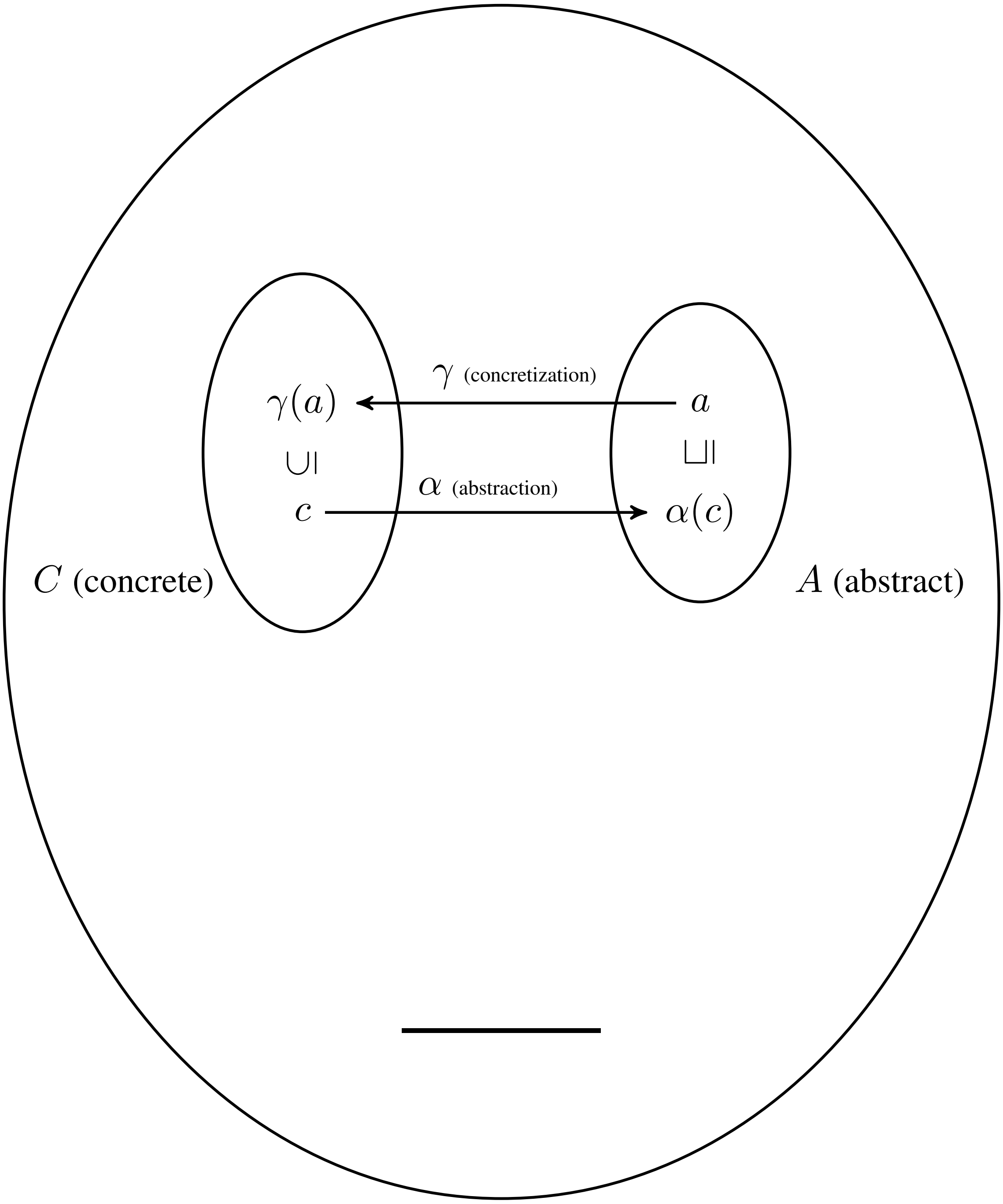
Quiz Solutions Outline

Synthesis, Analysis, and Verification 2013

for the quiz given on Friday, May 3rd, 2013



Problem 1: Relations ([10 points])

Task a) (*3 points*)
Not true. Consider $r = \{(a,b),(b,c)\}$ and $s = \{(c,d)\}$. Then clearly $(a,d) \in (r \cup s)^*$. On the other hand, we can compute each elements of the right-hand side. We have

$$r^* = \{(a,a),(b,b),(c,c),(a,b),(b,c),(a,c),(b,c),(c,a)\}$$

and

$$s^* = \{(a,a),(b,b),(c,c),(d,d),(c,d),(d,c)\}$$

Then we have $(r \circ s) = \{(c,d)\}$, and $(s \circ r) = \emptyset$. None of them contains (a,d).

Task b) (*3 points*)

Task c) (*2 points*)
True. We have that $r \cap s \subseteq r$, which implies that $(r \cap s)^* \subseteq r^*$. Similarly we get $(r \cap s)^* \subseteq s^*$, and we conclude that $(r \cap s)^* \subseteq r^* \cap s^*$.

Task d) (*2 points*)
Not true. Consider $r = \{(a,b),(b,c)\}, s = \{(a,c)\}$. We can compute $r^* = \{(a,b),(b,c),(a,c)\}$ and $s^* = \{(a,c)\}$. Finally the left-hand side is equals to $\{(a,c)\}$. But $r \cap s = \emptyset$.

Problem 2: Loop Semantics with Relations ([20 points])

Task a) (*3 points*)

$$r \doteq x < n \implies (x' = x + 1 \land y' = y \cdot m)$$

Task b) (*3 points*)

- (7, 2, 2, 49)
- (5, -2, 0, 1)
- (2, 3, 3, 64)

Task c) (*6 points*)

$$m' = m \wedge n' = n \wedge (x < n \implies x' = n) \wedge (x \geq n \implies x' = x) \wedge y' = m \cdot x'$$

Task d) (*8 points*)
The precondition sets the initial values of the computation variables x and y as well as the precondition on the exponent n:

$$x = 0 \wedge y = 1 \wedge n > 0$$

The postcondition that follows:

$$y = m^n$$

A sufficient loop invariant is:

$$x \geq 0 \wedge x \leq n \wedge y = m^x$$

It is initially true since $x = 0 < n$ and $m^0 = 1 = y$. For each iteration, x increases so is still greater than 0, it only increased by one if it is stricly smaller than n so will remain smaller than n. Also we have $y' = y \cdot m = m^x \cdot m = m^{x+1} = m^{x'}$. The invariant is sufficient because on exit we can additionally assume $x \geq n$, which combined with $x \leq n$ implies that $x = n$ and finally $y = m^x = m^n$, the postcondition.

Problem 3: Hoare Triples and Loop Invariants ([20 points])

Task a) (*5 points*)

$$\{length > 0\}\ r = \mathsf{max}(m, \mathsf{length})\ \{\forall i.(0 \leq i < \mathsf{length}) \implies r \geq \mathrm{m}(i) \wedge \exists i.(0 \leq i < \mathsf{length}) \implies r = \mathrm{m}(i)\}$$

Task b) (*15 points*)
The loop invariant is:

$$i \geq 0 \wedge i \leq \mathsf{length} \wedge \forall k.(0 \leq k < i) \implies r \geq m(k) \wedge \exists k.(0 \leq k \leq i) \wedge r = m(k)$$

The invariant holds initially because $i = 0$, $\mathsf{length} > 0$, and $r = map(0)$. The forall holds vacuously and the existential is true for $k = 0$.
The invariant is enough to prove the postcondition. At the end of the loop, we can further assume $i \geq \mathsf{length}$, and combined with $i \leq \mathsf{length}$ we get $i = \mathsf{length}$. Instantiating the quantifier with the value of i gives us the postcondition.
Finally we need to prove the inductive step. Suppose the invariant is true when entering the body of the loop, we know that $i < \mathsf{lenght}$ so $i' = i + i \leq \mathsf{length}$ and $i' > 0$. We need to prove that

$$(\forall k.(0 \leq k < i) \implies r \geq m(k)) \implies (\forall k.(0 \leq k < i + 1) \implies r \geq m(k))$$

which can be reduced to proving that $r \geq m(i+1)$ at the end of the body. That fact is obvious from the `if` expression. The last part of the proof is to show

$$(\exists k.(0 \leq k < i) \wedge r = m(k)) \implies (\exists k.(0 \leq k < i+1) \wedge r = m(k))$$

Which follows trivially from the assumption (there already exists such a k).

Problem 4: Lattices ([15 points])

Task a) (*5 points*)
First we prove that the new ordering is a partial order:

Reflexivity We have $\forall i \in I.\ f(i) \sqsubseteq f(i)$, thus $f \preceq f$.

Antisymmetry Take $i \in I$, then if by antisymmetry of $(L, \sqsubseteq)$ we have that $f(i) \sqsubseteq g(i) \wedge g(i) \sqsubseteq f(i) \implies f(i) = g(i)$, and thus $f \preceq g \wedge g \preceq f \implies f = g$.

Transitivity If $f \preceq g \wedge g \preceq h$, we have for any $i \in I$ that $f(i) \sqsubseteq g(i) \wedge g(i) \sqsubseteq h(i)$ and by transitivity of the underlying order we get $f(i) \sqsubseteq h(i)$ for any i, which is the definition of $f \preceq h$.

We can define the least upper bound as $f \sqcup g = h$, where $h(i) = f(i) \sqcup g(i)$. Similarly $f \sqcap g = h$, with $h(i) = f(i) \sqcap g(i)$.
We prove that the definition of $\sqcup$ is correct, proving for $\sqcap$ follows the exact same technique. First we need to show that $f \sqcup g$ is an upper bound of $\{f, g\}$. We have for any i that $f(i) \sqsubseteq f(i) \sqcup g(i)$. Same goes for $g(i)$. So h is an upper bound to f and g.
Let us we prove that it is the least upper bound. Suppose an arbitrary upper bound h' such that $f \preceq h'$ and $g \preceq h'$. So for any i, $f(i) \sqsubseteq h'(i) \wedge g(i) \sqsubseteq h'(i)$, and so $h'(i)$ is an upper bound of $f(i)$ and $g(i)$. Since $f(i) \sqcup g(i)$ is the least upper bound, it follows that $f(i) \sqcup g(i) \sqsubseteq h'(i)$, and, by definition, $f \sqcup g \preceq h'$, showing that $f \sqcup g$ is the least upper bound.

Task b) (*2 points*)
The size of this lattice is the number of functions from I to L, which can be computed by $|L|^{|I|}$.

Task c) (*8 points*)
Suppose $h((L, \sqsubseteq)) = N$. Given f and g, we have $f \prec g$ only if $f \preceq g$ and $\exists i \in I.\ f(i) \sqsubset g(i)$. Notice that we only need to have one value in the range of g being greater than f. Given a chain of L with $x_1 \sqsubset x_2 \sqsubset \ldots \sqsubset x_N$, we can build a chain of functions where each function is only "bumped" by one element from the chain of x_is. Formally, given f_k, we defined f_{k+1} by selecting an element i such that $f_k(i) = x_j \sqsubset x_N$ and replace it by $f_k(i) = x_{j+1}$. We define f_1 with $f_1(i) = x_1$, for all i. The length of such a chain is the number of time we can bump a value, which is clearly $N \cdot |I|$.

Problem 5: Predicate Abstraction ([15 points])

a) $\mathsf{sp}^{\#}(\{0 \leq x, 0 \leq y, x \leq y\}, x = x+1) = \{0 \leq y\}$

b) $\mathsf{sp}^{\#}(\{0 \leq x, 0 \leq y, x \leq 10, x \leq y\}, (x = x+1; x = x+1)) = \{0 \leq x, 0 \leq y\}$

c) $\mathsf{sp}^{\#}(\mathsf{sp}^{\#}(\{0 \leq x, 0 \leq y, x \leq 10\}, x = x+1), x = x+1) = \{0 \leq y\}$

d) $\mathsf{sp}^{\#}(\{0 \leq x, 0 \leq y, x \leq y\}, (x = x+1; y = y+1)) = \{\}$.
We are also losing $x \leq y$ since y could overflow while x does not.