Quiz Solutions Outline

Synthesis, Analysis, and Verification 2015

for the quiz given on Wednesday, April 22nd, 2015

PLEASE SIGN AND PRINT YOUR NAME ABOVE

This exam has 5 questions.
When handing in, please hand in the sheets with questions as well as any additional sheets with solutions.

Problem 1: Relations ([14 points])

Task a) (*4 points*)
Not true. Consider $A = \{a, b, c, d\}$, $r = \{(a, b), (b, c)\}$, 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

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

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 nor their transitive closure contains (a, d).

Task b) (*4 points*)
We prove both directions.

$(r \cup s)^* \subseteq (r^* \circ s^*)^*$ We show that $(r \cup s) \subseteq (r^* \circ s^*)$ and the result follows by monotonicity of the $*$ operator. We have that $r \subseteq r^* = r^* \circ \Delta \subseteq r^* \circ s^*$. We can prove that $s \subseteq r^* \circ s^*$ in a similar way.

$(r^* \circ s^*)^* \subseteq (r \cup s)^*$ We show that $(r^* \circ s^*) \subseteq (r \cup s)^*$. Then we get the result by taking transitive closures of both side and using $((r \cup s)^*)^* = (r \cup s)^*$. We have $r^* \circ s^* \subseteq (r \cup s)^* \circ (s \cup r)^* = (r \cup s)^*$.

Task c) (*3 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) (*3 points*)
Not true. Consider $r = \{(a, b), (b, c)\}, s = \{(a, c)\}$. We can compute $r^* \supseteq \{(a, b), (b, c), (a, c)\}$ and $s^* \supseteq \{(a, c)\}$, so that the left-hand side contains $\{(a, c)\}$. But $r \cap s = \emptyset$.

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

Task a) (*4 points*)
We define the precondition to execute the body C_F as $x < n$. The formula B_F represents the body and can be defined as

$$x' = x + 1 \land y' = y \cdot m \land m' = m \land n' = n$$

Note that we need to specify that variables m' and n' do not change.
Task b) (*9 points*)
Task b.1) (*3 points*)

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

Repetitive applications of F lead to $x \geq n$ and then the premise of the implication becomes false and the transitive closure can build the set of all transitions such that $x \geq n$, which is much bigger $\Delta_C \circ B$.

Task b.2) (*3 points*)

$$x < n \wedge (x' = x + 1 \wedge y' = y \cdot m \wedge m' = m \wedge n' = n)$$

Transitive closure of F corresponds to $\Delta_C \circ B$.

Task b.3) (*3 points*)

$$x < n \implies (x' = x + 1 \wedge y' = y \cdot m \wedge m' = m \wedge n' = n)$$

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

Transitive closure of F corresponds to $\Delta_C \circ B$.

Task c) (*3 points*)

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

Task d) (*6 points*)

$$m' = m \wedge n' = n \wedge x' = \max(x, n) \wedge y' = y \cdot m^{\max(n-x,0)}$$

Task e) (*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*)

$$\{length > 0\}\ r = \mathsf{max}(m, \mathsf{length})\ \{\forall i.(0 \le i < \mathsf{length}) \implies r \ge \mathrm{m}(i) \land \exists i.(0 \le i < \mathsf{length}) \land r = \mathrm{m}(i)\}$$

The poscondition states that r is at greater or equals to all the elements, and at least equals to one of them. The existential clause is needed to make sure the output is actually an element of the array and not just some random high enough number.

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

$$i \ge 0 \land i \le \mathsf{length} \land \forall k.(0 \le k < i) \implies r \ge m(k) \land \exists k.(0 \le k \le i) \land r = m(k)$$

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 $i \ge \mathsf{length}$, and combined with $i \le \mathsf{length}$ 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 $i' = i + i \le \mathsf{length}$ and $i' > 0$. We need to prove that

$$(\forall k.(0 \le k < i) \implies r \ge m(k)) \implies (\forall k.(0 \le k < i + 1) \implies r \ge m(k))$$

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

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

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

Problem 4: Lattices ([21 points])

Task a) (*9 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 $f(i) \sqsubseteq g(i) \land g(i) \sqsubseteq f(i) \implies f(i) = g(i)$, and thus $f \preceq g \land g \preceq f \implies f = g$.

Transitivity If $f \preceq g \land g \preceq h$, we have for any $i \in I$ that $f(i) \sqsubseteq g(i) \land g(i) \sqsubseteq h(i)$ 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) (*10 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 one index i such that $g(i)$ is greater than $f(i)$ in order to have a greater function g. Given a chain of L with $x_0 \sqsubset x_1 \sqsubset \ldots \sqsubset x_N$, 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 define f_{k+1} by selecting an element i such that $f_k(i) = x_j \sqsubset x_N$ and replace it by $f_{k+1}(i) = x_{j+1}$. We define f_0 with $f_0(i) = x_0$, for all i. The length of such a chain is the number of time we can bump a value, which is clearly $M = N \cdot |I|$.
We now prove this is the longest chain. Suppose there exists a longer chain $g_0 \sqsubset g_1 \sqsubset \ldots \sqsubset g_M \sqsubset g_{M+1}$ of length $M + 1$. By definition, $g_k \sqsubset g_{k+1}$ if and only if $\exists i \in I.\ g_k(i) \sqsubset g_{k+1}(i)$. So we can clearly build a chain of size at least $N + 1$ along one of the $|I|$ indices. This would be a contradiction to the height of the lattice $(L, \sqsubseteq)$.

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.