Final Exam
CS477: Spring’11

Due: Wednesday, May 11, 4:30pm. Submit either by email to both the instructor and TA, or submit a physical copy at the office of Elaine Wilson, 3229 SC (slide it under the door if the door is closed). Check the newsgroup regularly for typos, clarifications, etc.

You must work alone; no groups. You can consult any book or the internet; but you must write the answers in your own words and cite any source that you used explicitly, if it is beyond the resources we have used for this class.

This paper contains seven questions (I, II, III, IV, V, VI, VII). Make sure you see all questions. The points for each questions are also given. Note that the distribution of points is quite uneven across questions. Prioritize your work accordingly.

The exam was designed to take about 3 hours.

I. Logic [Points: 3+3+4+5]

Remember that universes of models are always non-empty.

1. Is the formula $(\forall x (f(x) = g(x))) \Rightarrow (\forall x.(f(g(x)) = g(f(x))))$ valid? If yes, argue why it is valid. If not, give a model in which the formula does not hold.

2. Express the following as a first-order formula over natural numbers with the signature $\{0, 1, 2, +, =, prime, <\}$, where prime is a unary predicate characterizing prime numbers:

\[ \text{There are infinitely many twin primes.} \]

where a twin prime is a pair of numbers $(x, x+2)$ where both $x$ and $x+2$ are prime.

3. Is the formula $(\forall x (f(f(x)) = f(x))) \wedge (\exists x, y. (\neg (x = y) \wedge f(x) = y))$ satisfiable? If yes, give a model for it. If not, argue why it is not satisfiable.

4. Is the formula $(\forall x.f(f(x)) = f(x)) \wedge (\forall x(\neg(x = f(x))))$ satisfiable? If yes, give a model for it. If not, argue why it is not satisfiable.
II. Weakest-pre; strongest-post  [Points: 4+2+4]

1. Let $\varphi : x \geq 0 \land x \leq y$. Write down the strongest-post condition of $\varphi$ with respect to the statement $x := y$, without using quantifiers.

2. Let $\varphi : x \leq y$. Write down the weakest pre-condition of $\varphi$ with respect to the statement $x := y$.

3. What is the weakest pre-condition of the formula $\varphi : x = y$ with respect to the following program, expressed over integers, where the signature also includes an operator $|$ that stands for "divides". $x|y$ means that $x$ divides $y$. (E.g. 3|45.).

```java
while (x < y) {
    x:=x+1;
    y:=y-1;
}
```

Note: You can’t compute this using the usual computation of weakest pre-conditions; but you can still express the weakest-pre-condition in FOL. Also, assume integers above are non-negative.
III. Verifying programs  [Points: 20+20]

Consider the following program:

while(b != 0) {
    if (a>b)
        a:= a-b;
    else
        b:= b-a;
}

Notation: For two natural numbers s and t, we write s|t we mean that the number s divides the number t. I.e. there is an integer z such that t = zs. For example, 5|35.

Show the following:

(a) Let d > 0. Assume the precondition a > 0 ∧ b > 0 ∧ d|a ∧ d|b holds, and prove that the post-condition d|a holds.

(b) Assume the same pre-condition as above, and prove that the program always terminates.

For each of the above, you must perform the following tasks:

1. Write the loop invariant for the loop in the program. The loop invariant should be sufficient to prove the post-condition/termination.
2. For (b) above, you must also give the ranking function. Give a ranking function that takes states to non-negative natural numbers.
3. Write down each basic path in the program, with the appropriate pre-conditions and post-conditions.
4. Write down, for each basic path, the weakest pre-condition of the post-condition with respect to the basic path, and the associated verification condition.
5. Argue why the verification conditions are valid.

IV. Code Contracts  [Points: 5]

Design the weakest pre-condition for the following method foo() in a class that has a variable x, and that has the class invariant: ∃u. (u + u + u + u = x).

    void foo(int z) {
        this.x = this.x + 2*z;
    }
V. Symbolic test-input generation [Points: 10]

Consider the following program:

1. \( x := x+1; \)
2. \( y := x+y; \)
3. if (\( x > y \)) then
   4. \( z := 1; \)
   5. else
   6. \( z := 0; \)
7. if (\( x+y+z>c \)) then
   8. \( z := 1; \)
   9. else
   10. \( z := 0; \)

A tester wants a test-input for the above program that will take the then-branch of the first if-statement, and the else-branch of the second if-statement (i.e. the path 1.2.3.4.7.9.10). Design a quantifier free first-order formula over integers, \( \varphi \), such that \( \varphi \) is satisfiable iff this path is feasible.

*Do not reason with the program yourself; rather, derive the formula syntactically from the program.*

VI. Monotonic functions and fixed-points [Points: 5+5]

(a) Let \( S \) be a set with \( s, s_0 \in S \) with \( s \neq s_0 \). Let \( f : 2^S \to 2^S \) be such that

\[
\begin{align*}
f(X) &= X \cup \{s\} \text{ if } s_0 \in X \\
&= X \setminus \{s\} \text{ otherwise}
\end{align*}
\]

Is \( f \) monotonic (wrt \( \subseteq \))? If yes, argue why. If not, argue why.

(b) Consider the function \( f : 2^\mathbb{N} \to 2^\mathbb{N} \), where for any \( X \),

\[
f(X) = \{2n \mid n \in X\} \cup \{3\}
\]

Exhibit a fixed-point of \( f \) that is not the empty set. Is there a fixed-point of \( f \) that is a finite set? If yes, give one; else argue why there cannot be one.
VII. Abstractions [Points: 2+4+4]

Let $C = 2^\mathbb{N}$ be subsets of concrete-states (say that associate the set of non-negative values an integer variable can take).

We want to build an abstraction to track whether the variable is a perfect square (e.g. 0, 1, 4, 9, etc.) So let’s define the abstract state-space $A = \{\bot, \text{PerfectSquare}, \top\}$.

The concretization function is given by:

$$
\begin{align*}
\gamma(\bot) &= \emptyset \\
\gamma(\text{PerfectSquare}) &= \{n^2 \mid n \in \mathbb{N}\} \\
\gamma(\top) &= \mathbb{N}
\end{align*}
$$

Let $\alpha$ be the natural analogous abstraction function, such that $\langle \alpha, \gamma \rangle$ is a Galois connection.

- What is $\alpha(\{1, 4, 9\})$? What is $\alpha(\{1, 2, 3\})$?
- Design the best abstract transformer for the statement $x := x^2 + 2x + 1$.
- Design the best abstract transformer for the statement $x := 15$. 