Problem Set 1 - Solutions and Comments

1. The statement suggests "no amount of testing can certify software will always behave correctly". Is this claim valid or invalid? Support your answer with a short justification.

   (This problem was discussed in Class 5.) One could support the claim being invalid by interpreting it as a statement about all software:

   $$\forall s \in software.\neg(\exists t \in Tests(s).t \implies Correct(s))$$

   Then, it would be sufficient to show it is invalid to identify one counter-example: an example of some software that can be shown to be correct by testing. It is possible to test some software exhaustively, if the set of possible inputs is finite (and small enough to be feasible to test in practice). Some programs do indeed have some input spaces small enough to test exhaustively; the non-trivial example of this from class was a Tic-Tac-Toe game, where the number of possible board positions is small enough to test it exhaustively. Most interesting software, though, has far too many possible inputs to test exhaustively. In a theoretical sense, the number of inputs is infinite since we think about most datatypes in programs as being unbounded, even though they are effectively bounded by the amount of memory available (which is always finite, even with seemingly unlimited cloud storage).

2. The statement suggests "proofs can certify that software will always behave correctly". Argue that this is not a correct statement.

   Proofs can certify properties of software, but can only certify properties of actual behavior of computing systems with lots of assumptions about how they work in reality. For example, when we prove properties about programs (or reason informally), we nearly always assume that code like,

   ```
   a = 3
   print(a)
   ```

   will print 3 since the value of ‘a‘ after the assignment will be the same the next time that location is read. In the real world, though, memory is stored in a physical way, and physical memories are imperfect (e.g., bits can be flipped if a cosmic ray hits that location of memory at the wrong time, or if someone is executing a row-hammer attack).

   Although proofs can provide a lot of confidence that code is correct, they cannot provide assurances that an actual computing system that executes that code will behave as the programming language model used to general the proof expects. You can think of this like a set of axioms; in this case, the axioms are assumptions about how the program will execute, but they are not necessarily true in a physical computer executing a real program.

   Grader's Note: For questions 1 and 2, answers received full credit if they were thoughtful and sensible, regardless of the position you argued. Since we hadn't yet talked about this in class, but wanted to use these questions to get you thinking about things and set up the class discussion, we didn't expect great answers to these questions.

Inference Rules

For each candidate rule below, state whether or not the rule is sound. Support your answer with a convincing proof.

3. $$\frac{P \implies Q, Q \implies R}{R}$$

   Not sound. When P, Q, and R are all false, both $P \implies Q$ and $Q \implies R$ are true, but R is false. Since the rule would allow a false conclusion, it is not sound.

4. $$\frac{(NOT(NOT(P)))}{P}$$

   Sound. By using proof by cases:

   1. When P is true, both $NOT(NOT(P))$ and P are true.
   2. When P is false, both $NOT(NOT(P))$ and P are false.

   Another way to show this is to use $P \equiv NOT(NOT(P))$.

5. $$\frac{P \implies Q}{Q \implies P}$$

   Not sound. When P is false and Q is true, $P \implies Q$ is true, but $Q \implies P$ is false. Since the rule can lead to a false conclusion, it is not sound.

6. $$\frac{P}{NOT(Q) \implies P}$$

   Sound. The antecedent is only true when P is true. Hence, $NOT(Q) \implies P$ is always true (a valid conclusion), regardless of the value of NOT(Q). This is a rather useless and misleading, rule, of course. It does not allow us to conclude $NOT(Q) \implies P$ in any context except when we already know P is true, so tells us nothing new about P or Q.

Grader's Note: (for questions 3-6)

For not sound cases, the easiest proof is a counter example. It could be an example (such as when P, Q, and R are all false) or using truth table. Just showing a truth table is not enough, you need to have some prose to explain how the truth table shows the contradiction.

The main problems with these question were misunderstanding the difference between proving and inference rule is sound and proving equivalence. For an inference rule to be sound, we need to show that whenever the conclusion is false the antecedent must be false (or, equivalently, whenever the antecedent is true, the conclusion must be true).

Proofs

7. Prove rigorously that if $x + y$ is even and x is odd, y must be odd. (For this proof, you should be more rigorous than will be expected on most proofs in cs2102, showing all of the steps and justifying each step, similar to the level of rigor from the proof in Class 2.)

   We assume $x \in \mathbb{N}$ and $y \in \mathbb{N}$ (which should have been stated in the question, and was well raised by several students). I use the quantifier notation introduced after PS1 in my proof, but you should be familiar with it now.

   Since $x + y$ is even and x is odd, we can write $\exists a \in \mathbb{N}.\, x + y = 2a$ and $\exists b \in \mathbb{N}.\, x = 2b + 1$ by the definitions of even and odd.

   Then,
   $$y = (x + y) - x = 2a - (2b + 1) = 2(a - b) + 1.$$

   Since a and b are integers, and the integers are closed under subtraction (meaning the difference between any two integers is also an integer), we know $\exists c \in \mathbb{Z}.\, c = a - b$ (note that we don't need to establish that $c \in \mathbb{N}$ since it is not required that c is non-negative).

   Thus $\exists c \in \mathbb{Z}.\, y = 2c + 1$, and y is odd by the definition of odd.

8. The proof that $\sqrt{2}$ is irrational (Theorem 1.8.1) in the book includes relies on this implication: d^2 is a multiple of two implies d is a multiple of 2. Prove that this is a valid implication to a skeptical reader.

   By using indirect proof, if we can prove that $d \nmid 2 \implies d^2 \nmid 2$ (that is, if d is not a multiple of two then d^2 must not be a multiple of two), that proves that $d^2 \mid 2 \implies d \mid 2$ (d^2 is a multiple of two implies d is a multiple of two).

   Since $d \nmid 2$, we can express d as $d = 2a + 1$ for some $a \in Z$, and then $d^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$.

   Thus $d^2 \nmid 2$, proving that if d^2 is a multiple of 2 then d is a multiple of 2.

   Grader's Note: Most students did the contra-positive proof. Some used direct proofs using the proof from Question 7. Both are good approaches for this problem.

9. Problem 1.4 (parts a, b, and c) from the MCS book.

   a. The error occurs where $3(\log 1/2) > 2(\log 1/2)$, since $\log 1/2 = -0.301$. Thus, it should be fixed to $3(\log 1/2) < 2(\log 1/2)$.

   Grader's Note: Most students got this right. However, some students simply said that you can not take out logs from both sides or $[a \times (logx) \neq log(x)^a]$. This is not true - it is legitimate to take the log of both sides of an equality. The problem is that logs can be negative, and multiplying by a negative number changes the direction of the inequality.

   b. The error occurs when $\$0.01 = (\$0.1)^2$, since $\$^2$ and \$ are different units.

   c. The error occurs when $(a - b)$ is divided on both sides, since $a = b$ this means $a - b = 0$ and division is not defined when the divisor is 0.

10. Prove that for any non-negative real numbers, x and y, if $xy = n$ then the minimum of x and y is not greater than $\sqrt{n}$. (Hint: prove by contradiction.)

To prove by contradiction, we start by assuming the opposite and showing it leads to a contradiction.

Suppose $\min(\{x, y\}) > \sqrt{n}$. Assume without loss of generality that $x = \min(x, y)$. (This doesn't lose generality, since we could always rename x and y, nothing in the statement depends on which is first.)

Then, $x = \sqrt{n} + a$ for some positive a ($a \in \mathbb{R}_+$, the set of positive real numbers).

Since x is the minimum of $\{x, y\}$, we know y is not smaller than x:

$$y = \sqrt{n} + a + b = x + b \text{ for some } b \in \mathbb{R}, b \geq 0.$$

Multiplying x and y gives:

$$xy = (\sqrt{n} + a) * (\sqrt{n} + (a + b)) = n + 2a * \sqrt{n} + a^2 + b * \sqrt{n} + ab.$$

Now we have two cases. The first is where $\sqrt{n} > 0$. Then, since $a > 0$, $b \geq 0$ and $\sqrt{n} > 0$, we know the $2a * \sqrt{n}$ term is positive, and the other terms added to n are all non-negative, so $xy > n$. Thus, $xy \neq n$ which contradicts our assumption that $xy = n$ and $\min(\{x, y\}) > \sqrt(n)$.

The second case is where $\sqrt{n} = 0$. In that case, we can't assume $2a * \sqrt{n}$ is positive (it would be 0), so our reasoning above doesn't quite work. But, we know the only way for $\sqrt{n} = 0$ is if $xy = 0$, which means $x = 0$ and $y = 0$, neither of which is greater than $\sqrt{0} = 0$.

Grader's Note: Most students did well on this question (and it was not necessary to consider the 0 case to be considered a full credit answer). Some clever answers go to the contradiction $xy > xy$, which is a clearer contradiction.