

CSci 360, Fall 2004, Assignment 3

This assignment is worth 25 points. Your solutions to this assignment (which may be typed or handwritten) are due at the beginning of class Friday, September 17. Note that your solution will be considered late if you bring it with you to class and arrive late.

Recall the proof system we examined in class.

$$\text{Rule of Sequence: } \frac{\{P\}S\{Q\} \quad \{Q\}T\{R\}}{\{P\}S T\{R\}}$$

$$\text{Rule of Consequence: } \frac{P \text{ implies } Q}{\{P\}\{Q\}}$$

$$\text{Rule of Assignment: } \frac{}{\{P_{x \rightarrow E}\}x := E; \{P\}}$$

$$\text{Rule of Condition: } \frac{\{P \wedge B\}S\{Q\} \quad \{P \wedge \neg B\}T\{Q\}}{\{P\}\text{if } B \text{ then } S \text{ else } T \text{ end if}; \{Q\}}$$

$$\text{Rule of Iteration: } \frac{\{I \wedge B\}S\{I\}}{\{I\}\text{while } B \text{ loop } S \text{ end loop}; \{I \wedge \neg B\}}$$

Using this proof system, provide a step-by-step partial correctness proof for the following hypothesis. Justify each step with one of the axioms, or “mathematical fact” if the step involves no assertions and is algebraically true.

```
{x = m ∧ y = n}
z := 1;
while y /= 0 loop
  if y mod 2 = 0 then
    x := x * x;
    y := y / 2;
  else
    z := z * x;
    x := x * x;
    y := (y - 1) / 2;
  end if;
end loop;
{z = mn}
```

Since the proof involves writing similar things many times, you may, if you wish, use letters to represent blocks of code or logical statements, as long as those definitions are clearly defined in a separate section. Do not use arrows in lieu of copying text. Be neat: Part of the grade will be based on how easily I can figure out what you’re writing.

Hint: A good invariant to choose is $z \cdot x^y = m^n$.