

CMSC 631, Fall 2007

Homework 5

Due Monday, October 29, in class

This homework is concerned with the practice of program verification according to Hoare logic. Please refer to the Huth & Ryan chapter for background and terminology. As a primer, try the practice exercises at <http://www.cs.bham.ac.uk/research/projects/lics/tutor/chap4/questions.html> (solutions provided on the web site).

1. (H & R, 1st ed., Ex. 4.3.1.) Use the proof rule for assignment and logical implication as appropriate to show the following partial correctness proofs:

- (a) $\vdash_{\text{par}} (x > 0) y = x + 1 (y > 1)$
- (b) $\vdash_{\text{par}} (\top) y = x; y = x + x + y (y = 3 \cdot x)$
- (c) $\vdash_{\text{par}} (x > 1) a = 1; y = x; y = y - a (y > 0 \wedge x > y)$

2. (H & R, 1st ed., Ex. 4.3.2.) Write down a program P such that

- (a) $(\top) P (y = x + 2)$
- (b) $(\top) P (z > x + y + y)$

and prove it.

3. (H & R, 1st ed., Ex. 4.5.2(b).) Write code for P for the following specification and prove the correctness of the input/output behavior:

$$(\top) P (z = \max(w, x, y))$$

where $\max(w, x, y)$ denotes the largest of w , x , and y . Show your program and the proof that it satisfies the given post condition using a proof tableaux.

4. (H & R, 1st ed., Ex. 4.6.1.) Show that $\vdash_{\text{par}} (x \geq 0) \text{Copy1} (x = y)$ where `Copy1` is the following code:

```
a = x;
y = 0;
while (a != 0) {
  y = y + 1;
  a = a - 1;
}
```