

Hoare Logic and Model Checking

Supervision 2

Easter 2018

Supervisor: Joe Isaacs (josi2).

All work should be submitted in **PDF** form 36 hours before the supervision to the email josi2@cam.ac.uk, ideally written in \LaTeX , with page numbers (e.g. 1/9). If you have any questions on the course please include these at the top of the supervision work and we can talk about them in the supervision. Since there are many proofs, it would be best for these to be done by hand and included using `\includegraphics`.

1 Separation Logic

1. <http://www.cl.cam.ac.uk/teaching/1718/HLog+ModC/part1-exercises-updated.pdf> (Exercise 5, 6 and 7)
2. <https://www.cl.cam.ac.uk/teaching/exams/pastpapers/y2017p7q8.pdf>
3. Slide 23 of lecture 5 says that the assertion

$$X \mapsto E_1 \wedge Y \mapsto E_2$$

force $E_1 = E_2$ why?

4. What values can h take in

$$\forall s. h \in \llbracket X \mapsto 3, Y \wedge Y \mapsto 3, X \rrbracket(s)$$

5. Show, carefully that

$$\vdash (X \mapsto v_1 \wedge A = v_1) * Y \mapsto v_2 \Rightarrow X \mapsto v_1 * Y \mapsto v_2 \wedge A = v_1$$

2 Model Checking

1. <http://www.cl.cam.ac.uk/teaching/1718/HLog+ModC/MJCG-MC-Solutions.pdf> Questions [1,2,3].
2. <http://www.cl.cam.ac.uk/teaching/exams/pastpapers/y2012p7q13.pdf> (Part a)