COMSM0067: Advanced Topics in Programming Languages
Problem Sheet: Separation Logic

The frame rule, small axioms and list segments

---

1. (*) The following program stores the sum of two heap cells in a fresh cell, and then clears the first cell:

$$\begin{array}{rl} d \triangleq & u := [x]; \\ & v := [y]; \\ & z := \mathsf{new}(u + v); \\ & [x] := 0. \end{array}$$

   Prove

$$\{(x \mapsto a) * (y \mapsto b)\} \;\; d \;\; \{(x \mapsto 0) * (y \mapsto b) * (z \mapsto a + b)\}.$$

   Give the assertion holding after each of the four commands. At each step, state which small axiom you apply and which part of the assertion you isolate using the frame rule.

2. The following program removes the first node of a list segment:

$$\begin{array}{rl} d \triangleq & y := [x.\mathsf{next}]; \\ & \mathsf{dispose}(x); \\ & x := y. \end{array}$$

   Prove

$$\{x \neq z \wedge \mathsf{lseg}(x, z)\} \;\; d \;\; \{\mathsf{lseg}(x, z)\}.$$

   Give the assertion holding after each of the three commands. At each step, state which rule or small axiom you apply and which part of the assertion you isolate using the frame rule. State where you unfold the definition of lseg, and why the precondition needs $x \neq z$.