Exercise Sheet 10

Due date: July 12th. Please hand in your solutions at the start of the exercise class.

Task 1: Distributivity of $\wedge$ over $*$ (30)

Recall from Theorem 18.1.5 that for all $A, B, C \in \mathsf{SLA}$, we have

$$\models (A \wedge B) * C \Rightarrow (A * C) \wedge (B * C) \ . \tag{1}$$

(a) Prove that the converse direction does *not* hold by providing suitable $A, B, C \in \mathsf{SLA}$.

(b) We call an assertion $C \in \mathsf{SLA}$ *domain exact* iff

$$\forall (s,h),(s,h') \in \Sigma\colon\ (s,h) \models C \text{ and } (s,h') \models C \quad \text{implies} \quad \mathsf{dom}\,(h) = \mathsf{dom}\,(h') \ .$$

Prove that the converse direction of (1) holds if C is domain exact.

Task 2: Altering Lists (40)

Let c be the following program:

$$\begin{aligned} & i := [x]\,; \\ & j := [i]\,; \\ & \mathsf{free}\,(x)\,; \\ & \mathsf{free}\,(i)\,; \\ & x := \mathsf{alloc}\,(j) \end{aligned}$$

Prove in SL:

$$\vdash \{x \mapsto a * a \mapsto b * \mathsf{sll}\,(b, 0)\} c \{\mathsf{sll}\,(x, 0)\}$$

Task 3: Partial Correctness Properties in Separation Logic (30)

(a) Disprove: For all programs c, we have

$$\models \{\mathsf{true}\} c \{\mathsf{true}\} \ .$$

(b) Provide the *maximal* set of programs $\mathfrak{A}$ such that for all $c \in \mathfrak{A}$ it holds that

$$\models \{\mathsf{true}\} c \{\mathsf{true}\} \ .$$