CS256-Assignment#4

3 Problems. 55 points.

Read Chapter 1 (you may skip Section 1.5). Start reading Chapter 2 (not covered in this homework). Do the following exercises.

[10 points] Textbook, Problem 1.4, parts (a) and (b). Simplify your answers. In particular, your answers should contain no primes.

[15 points] Textbook, Problem 1.5.

[30 points] Consider program MUX-BAK-A from Fig 1.33 (page 159 in the text). To characterize the behavior of the program, fill in the boxes below. Each box should contain an assertion over only the program variables y_1 and y_2. Furthermore, each invariant (i.e., each φ_i and each ψ_i) should be inductive with respect to previously proved invariants. (A "previously proved invariant" is a formula with a lower index; for example, in the proof of ψ_3 you are only allowed to use φ_0, φ_1, ψ_1, φ_2, and ψ_2.)

$$\varphi_0 : \;\; y_1 \geq 0 \land y_2 \geq 0$$

$$\begin{array}{llll}
\varphi_1 : & at\_\ell_{0..2} \leftrightarrow \boxed{\qquad\qquad} & \psi_1 : & at\_m_{0..2} \leftrightarrow \boxed{\qquad\qquad} \\
\varphi_2 : & at\_\ell_{3..5} \leftrightarrow \boxed{\qquad\qquad} & \psi_2 : & at\_m_{3..5} \leftrightarrow \boxed{\qquad\qquad} \\
\varphi_3 : & at\_\ell_4 \rightarrow \boxed{\qquad\qquad\qquad\qquad} & \psi_3 :: & at\_m_4 \rightarrow \boxed{\qquad\qquad\qquad\qquad}
\end{array}$$

$$\varphi_4 : \;\; \neg(at\_\ell_4 \land at\_m_4 \;)$$

(Note that the φ_i and ψ_i involve more than just what is necessary to show mutual exclusion.)

To prove an invariant φ_i, one could use B-INV and thus prove $\{\varphi_i\}\tau\{\varphi_i\}$ for all $\tau \in \mathcal{T}$. In general, for some τ's the verification condition (VC) will be state valid, while for other τ's you will need to appeal to previously proved invariants (as in slide 6-31). For φ_i ranging over

$$\varphi_1,\ \varphi_2,\ \varphi_3,\ \varphi_4,$$

say for which τ's the VC $\{\varphi_i\}\tau\{\varphi_i\}$ is **not** state valid. For each of these, say which previous invariants you need to conjoin to the antecedent of the VC to be able to prove it. Each φ_i should be proved by using B-INV (perhaps also appealing to previously proved invariants). Don't consider other rules like CON-I or MON-I.

NOTE: You do not need to actually write out the details of the proofs; just answer the questions above.