4.3 SaDS

If statement (11.1.2)

~~$\Gamma \vdash C \Rightarrow [t]F$~~

$$\frac{\Gamma \vdash C \Rightarrow [t]F \quad \Gamma \vdash \neg C \Rightarrow [t']F}{\Gamma \vdash [\text{if}(C)\{t\}\text{else}\{t'\}]F}$$

Assuming C is true, the result will be [t]F. We know that this means, F holds true in all possible states that can be reached by evaluating t.

Assuming ¬C instead, the result will be [t']F, F holds true in all possible states that can be reached by evaluating t'.

This shows that ~~the~~ if followed by F always evaluates to true.

Hence, Sound

While statement (11.1.3)

$$\frac{\Gamma \vdash I \quad \Gamma^* \vdash (I \wedge C) \Rightarrow [t]I \quad \Gamma^* \vdash (I \wedge \neg C) \Rightarrow F}{\Gamma \vdash [\text{while } C\{t\}]F}$$

A loop invariant is always preserved as true by execution of the loop. From section 9.4.1, we know I always holds true in every possible successor state that can be reached by evaluating t.

Assuming C is true, result will bee [t]I. Using section 9.4.1, we know that I always holds true ~~——~~ evaluating t.

Assuming ¬C instead, result will be F. F is a declaration that will hold true.

This shows that while followed by F always evaluates to true.

Hence, Sound