Let \( S \) be a specification. Let \( A \) be an assertion and let \( A' \) be the same as \( A \) but with primes on all the variables. How does the exact precondition for \( A' \) to be refined by \( S \) differ from \((S, A)\) ? Hint: consider prestates in which \( S \) is unsatisfiable, then deterministic, then nondeterministic.

After trying the question, scroll down to the solution.
§ (the exact precondition for $A'$ to be refined by $S$)

\[ \forall \sigma' \cdot A' \Leftarrow S \]

definition of sequential composition

\[ S, A \]

rename $\sigma''$ to $\sigma'$

\[ \exists \sigma'' \cdot (\sigma'' \cdot S) \land (\sigma \cdot A) \sigma'' \]

\[ \exists \sigma' \cdot S \land A' \]

We are being asked about the difference between $\forall \sigma' \cdot A' \Leftarrow S$ and $\exists \sigma' \cdot S \land A'$. In a prestate for which $S$ is both satisfiable and deterministic, there is no difference. In a prestate for which $S$ is unsatisfiable, $\forall \sigma' \cdot A' \Leftarrow S$ is $\top$ and $\exists \sigma' \cdot S \land A'$ is $\bot$. In a prestate for which $S$ is nondeterministic, $\forall \sigma' \cdot A' \Leftarrow S$ is as strong as or stronger than $\exists \sigma' \cdot S \land A'$; if $A'$ is $\top$ for all corresponding poststates, they are equal; if $A'$ is $\bot$ for all corresponding poststates, they are equal; but if $A'$ is $\top$ for some and $\bot$ for other corresponding poststates, then $\forall \sigma' \cdot A' \Leftarrow S$ is $\bot$ and $\exists \sigma' \cdot S \land A'$ is $\top$. Here is an example to illustrate the difference. Let $n$ be a natural variable, let $S = n' < n$, and let $A' = n' = 0$. If $n = 0$, $S$ is unsatisfiable, and

\[ n=0 \Rightarrow (\forall \sigma' \cdot A' \Leftarrow S) \land \neg (\exists \sigma' \cdot S \land A') \]

If $n = 1$, $S$ is satisfiable and deterministic, and

\[ n=1 \Rightarrow (\forall \sigma' \cdot A' \Leftarrow S) \land (\exists \sigma' \cdot S \land A') \]

If $n = 2$, $S$ is nondeterministic, and

\[ n=2 \Rightarrow \neg (\forall \sigma' \cdot A' \Leftarrow S) \land (\exists \sigma' \cdot S \land A') \]