Let \( S \) be a specification. Let \( C \) and \( C' \) be corresponding pre- and postconditions. How does the exact precondition for \( C' \) to be refined by \( S \) differ from \((S, C)\)? Hint: consider prestates in which \( S \) is unsatisfiable, then deterministic, then nondeterministic.

§

(the exact precondition for \( C' \) to be refined by \( S \))

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

\[
S, C
\]

\[
\exists \sigma'' \cdot (\sigma' \Rightarrow S) \sigma'' \land (\sigma \Rightarrow C) \sigma''
\]

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

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

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

If \( n = 1 \), \( S \) is satisfiable and deterministic, and

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

If \( n = 2 \), \( S \) is nondeterministic, and

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