Proof of Theorem: $TCSpec \Rightarrow \Box TCTypeOK$

We **prove by induction** that the Transaction Commit specification $TCSpec$ holds the invariant $TCTypeOK$, i.e.,

$$TCSpec = TCInit \wedge \Box[TCNext] \Rightarrow \Box TCTypeOK$$

1. Base case

Definition of $TCInit$:

$$\forall rm \in RM : rmState[rm] = working$$

Definition of $TCTypeOK$:

$$\forall rm \in RM : rmState[rm] \in \{working, prepared, committed, aborted\}$$

Clearly, $TCInit \Rightarrow TCTypeOK$.

2. Inductive case

$$TCTypeOK \wedge TCNext \Rightarrow TCTypeOK'$$

is also clear from definitions:

$$\begin{aligned}
&\forall rm \in RM : rmState[rm] \in \{working, prepared, committed, aborted\} \\
&\qquad \wedge \\
&\exists r1 \in RM : ((rmState'[r1] = prepared \wedge ...) \vee \\
&\qquad\qquad (rmState'[r1] = committed \wedge ...) \vee \\
&\qquad\qquad (rmState'[r1] = aborted \wedge ...)) \wedge \\
&\qquad\qquad (\forall r2 \in RM \setminus \{r1\} : rmState'[r2] = rmState[r2]) \\
&\qquad \Rightarrow \\
&\forall rm \in RM : rmState'[rm] \in \{working, prepared, committed, aborted\}
\end{aligned}$$