

CONSTANTS *Server, Client*

VARIABLE *locked, held*

$$\begin{aligned} Init &\triangleq \\ &\wedge \textit{locked} = [i \in \textit{Server} \mapsto \text{TRUE}] \\ &\wedge \textit{held} = [i \in \textit{Client} \mapsto \{\}] \end{aligned}$$

$$\begin{aligned} \textit{Connect}(\textit{client}, \textit{server}) &\triangleq \\ &\wedge \textit{locked}[\textit{server}] = \text{TRUE} \\ &\wedge \textit{held}' = [\textit{held} \text{ EXCEPT } ![\textit{client}] = \textit{held}[\textit{client}] \cup \{\textit{server}\}] \\ &\wedge \textit{locked}' = [\textit{locked} \text{ EXCEPT } ![\textit{server}] = \text{FALSE}] \end{aligned}$$

$$\begin{aligned} \textit{Disconnect}(\textit{client}, \textit{server}) &\triangleq \\ &\wedge \textit{server} \in \textit{held}[\textit{client}] \\ &\wedge \textit{held}' = [\textit{held} \text{ EXCEPT } ![\textit{client}] = \textit{held}[\textit{client}] \setminus \{\textit{server}\}] \\ &\wedge \textit{locked}' = [\textit{locked} \text{ EXCEPT } ![\textit{server}] = \text{TRUE}] \end{aligned}$$

$$\begin{aligned} \textit{Next} &\triangleq \\ &\vee \exists \textit{client} \in \textit{Client}, \textit{server} \in \textit{Server} : \textit{Connect}(\textit{client}, \textit{server}) \\ &\vee \exists \textit{client} \in \textit{Client}, \textit{server} \in \textit{Server} : \textit{Disconnect}(\textit{client}, \textit{server}) \end{aligned}$$

$$\textit{Spec} \triangleq \textit{Init} \wedge \Box[\textit{Next}]_{\langle \textit{locked}, \textit{held} \rangle}$$

$$\begin{aligned} \textit{Safe} &\triangleq \\ &\forall \textit{client}_i, \textit{client}_j \in \textit{Client} : \\ &(\textit{held}[\textit{client}_i] \cap \textit{held}[\textit{client}_j] = \{\}) \vee (\textit{client}_i = \textit{client}_j) \end{aligned}$$