

CONSTANT *CLIENTS*

VARIABLE *storage, clState*

$WVTypeOk \triangleq \wedge storage \in [CLIENTS \rightarrow \{\text{"none"}, \text{"empty"}, \text{"written"}\}]$
 $\wedge clState \in [CLIENTS \rightarrow \{\text{"begin"}, \text{"precheck-done"}, \text{"blank-written"},$
 $\text{"write-check-done"}, \text{"committed"}, \text{"aborted"}\}]$

$WVInit \triangleq \wedge storage = [cli \in CLIENTS \mapsto \text{"none"}]$
 $\wedge clState = [cli \in CLIENTS \mapsto \text{"begin"}]$

Only one execution can be committed.

Once committed, the file has been written.

$WVConsistency \triangleq \wedge \forall i, j \in CLIENTS :$
 $\quad \text{If } i \neq j, clState[i] \text{ and } clState[j] \text{ cannot be both committed.}$
 $\quad i \neq j \wedge clState[i] = \text{"committed"} \Rightarrow \neg clState[j] = \text{"committed"}$
 $\wedge \forall i, j \in CLIENTS :$
 $\quad i \neq j \wedge storage[i] = \text{"written"} \Rightarrow \neg storage[j] = \text{"written"}$
 $\wedge \forall i \in CLIENTS : clState[i] = \text{"committed"} \equiv storage[i] = \text{"written"}$

“Verify” condition: storage only contains our file or nothing.

$Check(c) \triangleq \wedge \forall f \in CLIENTS : f = c \vee storage[f] = \text{"none"}$

$Precheck(c) \triangleq \wedge clState[c] = \text{"begin"}$
 $\wedge \text{IF } Check(c)$
 $\quad \text{THEN } clState' = [clState \text{ EXCEPT } ![c] = \text{"precheck-done"}]$
 $\quad \text{ELSE } clState' = [clState \text{ EXCEPT } ![c] = \text{"aborted"}]$
 $\wedge \text{UNCHANGED } \langle storage \rangle$

$WriteBlank(c) \triangleq \wedge clState[c] = \text{"precheck-done"}$
 $\wedge storage' = [storage \text{ EXCEPT } ![c] = \text{"empty"}]$
 $\wedge clState' = [clState \text{ EXCEPT } ![c] = \text{"blank-written"}]$

$ConflictCheck(c) \triangleq \wedge clState[c] = \text{"blank-written"}$
 $\wedge \text{IF } Check(c)$
 $\quad \text{THEN } clState' = [clState \text{ EXCEPT } ![c] = \text{"write-check-done"}]$
 $\quad \text{ELSE } clState' = [clState \text{ EXCEPT } ![c] = \text{"aborted"}]$
 $\wedge \text{UNCHANGED } \langle storage \rangle$

Delete the file when aborted.

$RollBack(c) \triangleq \wedge clState[c] = \text{"aborted"}$
 $\wedge storage[c] \neq \text{"none"}$
 $\wedge storage' = [storage \text{ EXCEPT } ![c] = \text{"none"}]$
 $\wedge clState' = [clState \text{ EXCEPT } ![c] = \text{"begin"}]$

$Commit(c) \triangleq \wedge clState[c] = \text{"write-check-done"}$

$$\begin{aligned} \wedge clState' &= [clState \text{ EXCEPT } ![c] = \text{"committed"}] \\ \wedge storage' &= [storage \text{ EXCEPT } ![c] = \text{"written"}] \end{aligned}$$

$$\begin{aligned} WVNext \triangleq \exists c \in CLIENTS : & \vee Precheck(c) \\ & \vee WriteBlank(c) \\ & \vee ConflictCheck(c) \\ & \vee RollBack(c) \\ & \vee Commit(c) \end{aligned}$$

$$WVSpec \triangleq WVInit \wedge \Box [WVNext]_{(storage, clState)}$$

$$\text{THEOREM } WVSpec \Rightarrow \Box (WVConsistency \wedge WVTypeOk)$$

\ * Modification History
 \ * Last modified Sat Jun 29 14:21:06 CST 2024 by Hillium
 \ * Created Sat Jun 29 10:41:34 CST 2024 by Hillium