MODULE *RWSet*

CONSTANTS Key, $Version$, $Value$, $NULL$

$State \triangleq [Key \to (Value \cup NULL)]$

CONSTANTS $Operation$

CONSTANTS $Apply(\_, \_, \_)$

ASSUME $\forall\, s0 \in State,\, s1 \in State,\, f \in Operation : Apply(s0,\, f,\, s1) \in \text{BOOLEAN}$

$Deterministic(f) \triangleq$
$\forall\, s0,\, s1,\, s2 \in State : Apply(s0,\, f,\, s1) \land Apply(s0,\, f,\, s2) \Rightarrow s1 = s2$

CONSTANT $WriteSet$, $ComputeWS(\_, \_)$, $Commit(\_, \_)$
ASSUME $\forall\, s1,\, s2 \in State : ComputeWS(s1,\, s2) \in WriteSet$
ASSUME $\forall\, s \in State,\, ws \in WriteSet : Commit(s,\, ws) \in State$
ASSUME $\forall\, s1,\, s2 \in State : Commit(s1,\, ComputeWS(s1,\, s2)) = s2$

CONSTANTS $Simulate(\_, \_, \_)$

ASSUME $\forall\, s0,\, f,\, rw : Simulate(s0,\, f,\, rw) \in \text{BOOLEAN}$

$SefetyOfWriteSet \triangleq$ TRUE
$SefetyOfReadSet \triangleq$ TRUE
$SafetyOfSimulation \triangleq SefetyOfWriteSet \land SefetyOfReadSet$

$ReadSetOK(s,\ rwset) \triangleq$ TRUE s satisfies $rwset$ condition (= $MVCC$ condition)
$ApplyTx(s1,\ f,\ s2) \triangleq$ TRUE $f(s1) = s2$
$ApplyWriteSet(s1,\ rwset,\ s2) \triangleq$ TRUE committing $WriteSet$ $rwset$ at state $s1$ results in state $s2$

$SafetyOfCommit \triangleq \forall\, ss0,\ ss1,\ s,\ s1,\ s2 \in State,\ f,\ rwset \in RWSet :$
$Simulate(ss0,\ f,\ ss1,\ rwset) \land ReadSetOK(s,\ rwset) \land ApplyTx(s,\ f,\ s1) \land ApplyWriteSet(s,\ rwset,\ s2) \Rightarrow s1 =$