

B Method

We consider the B Abstract State Machine given below, which implements a system for processing administrative files. Each file is first received and can then either be validated or discarded.

MACHINE	File_Processing
SETS	FILES
VARIABLES	received, valid
INVARIANT	$\text{received} \subseteq \text{FILES} \wedge \text{valid} \subseteq \text{received}$
INITIALISATION	$\text{received} := \emptyset; \text{valid} := \emptyset$
OPERATIONS	$\text{receive}(f) =$ PRE $f \in \text{FILES}$ THEN $\text{received} := \text{received} \cup \{f\}$ END ; $\text{validate}(f) =$ PRE $f \in \text{received}$ THEN $\text{valid} := \text{valid} \cup \{f\}$ END ; $\text{discard}(f) =$ PRE $f \in \text{received}$ THEN $\text{received} := \text{received} \setminus \{f\}$ END ;

1. Write the proof obligation which should guarantee that the invariant is true after initialization. Is it correct? If not, how can the machine be corrected? Please justify your answer.
2. Write the proof obligation which should guarantee that the operation receive preserves the invariant. Is it correct? If not, how can the machine be corrected? Please justify your answer.
3. Write the proof obligation which should guarantee that the operation discard preserves the invariant. Is it correct? If not, how can the machine be corrected? Please justify your answer.