MACHINE

VARIABLES

p1_in, p1_out

INVARIANTS

inv10: ⟨theorem⟩ $(phase = checking \land p1\_in = p1\_out) \Rightarrow R\_est \leq R\_real$

inv12: $phase = est \Rightarrow (p1\_in(int) \in \{0,1\} \Rightarrow p1\_in(len) = 0)$

inv13: $phase = est \Rightarrow (p1\_in(int) = 2 \Rightarrow p1\_in(len) \geq 3)$

inv14: $phase = est \Rightarrow (p1\_in(front) \geq R\_est \land p1\_in(front) \in T \land p1\_in(front) - p1\_in(len) \in T \land p1\_in(int) \in \{0,1,2\})$

EVENTS

Event Report ⟨ordinary⟩ ≙

refines Report

where

grd2: $fr \in T \land le \in T \land i \in \{0,1,2\}$

grd4: $fr \geq F\_real \land fr \leq F\_real + 2$

grd5: $i = 2 \Rightarrow (fr - R\_real \leq le)$

grd6: $i \in \{0,1\} \Rightarrow le = 0$

then

act2: $p1\_out := \{front \mapsto fr, int \mapsto i, len \mapsto le\}$

end

Event Res ⟨ordinary⟩ ≙

refines Res

where

grd4: $bool(p1\_in(int) \in \{0,1\} \Rightarrow p1\_in(len) = 0) = valid1$

grd5: $bool(p1\_in(int) = 2 \Rightarrow p1\_in(len) \geq 3) = valid2$

grd6: $bool(p1\_in(front) \geq R\_est \land p1\_in(front) \in T \land p1\_in(front) - p1\_in(len) \in T \land p1\_in(int) \in \{0,1,2\}) = valid3$

grd7: $validity = TRUE \Leftrightarrow (valid1 = TRUE \land valid2 = TRUE \land valid3 = TRUE)$

then

act1: $phase :| (validity = TRUE \Rightarrow phase' = est) \land (validity = FALSE \Rightarrow phase' = detection)$

end

Event Est ⟨ordinary⟩ ≙

refines Est

where

grd5: $f\_est = p1\_in(front)$

grd9: $p1\_in(int) = 2 \Rightarrow r\_est = f\_est - p1\_in(len)$

grd8: $p1\_in(int) \in \{0,1\} \Rightarrow r\_est = R\_est$

then

act1: $phase := checking$

act2: $R\_est := r\_est$

act3: $F\_est := f\_est$

end

END