```
───────────────────── MODULE Elevator ─────────────────────
EXTENDS Naturals

CONSTANTS MaxFloors,     Total number of floors in building
          Ascending,     Upward movement state
          Descending     Downward movement state

ASSUME MaxFloors ∈ Nat   Must be a natural number

VARIABLES position,      Current position (odd = at floor, even = between floors)
          movement       Current movement state (Ascending or Descending)

 Helper function to determine if elevator is stopped at a specific floor
AtFloor(floor) ≜ position = 2 ∗ floor − 1

 Helper function to determine if elevator is between floors
InTransit ≜ position%2 = 0

 Initial state - start at ground floor
Init ≜ ∧ position   = 1
       ∧ movement ∈ {Ascending, Descending}

 Start ascending from a floor
StartAscending ≜
    ∧ ∃ f ∈ 1 . . MaxFloors  − 1 : AtFloor(f)   At any floor except top
    ∧ position′   = position + 1   Move to in-between state
    ∧ movement′ = Ascending

 Continue ascending between floors
ContinueAscending ≜
    ∧ InTransit   Must be between floors
    ∧ movement = Ascending
    ∧ position′ = position + 1
    ∧ UNCHANGED movement

 Start descending from a floor
StartDescending ≜
    ∧ ∃ f ∈ 2 . . MaxFloors : AtFloor(f)   At any floor except bottom
    ∧ position′   = position − 1
    ∧ movement′ = Descending

 Continue descending between floors
ContinueDescending ≜
    ∧ InTransit
    ∧ movement = Descending
    ∧ position′ = position − 1
    ∧ UNCHANGED movement
```

All possible next states

$$\mathit{Next} \triangleq \begin{array}{l} \lor\ \mathit{StartAscending} \\ \lor\ \mathit{ContinueAscending} \\ \lor\ \mathit{StartDescending} \\ \lor\ \mathit{ContinueDescending} \end{array}$$

Variables for fairness conditions

$$\mathit{vars} \triangleq \langle \mathit{position},\ \mathit{movement} \rangle$$

Fairness conditions to ensure progress

$$\begin{array}{l} \mathit{Fairness} \triangleq \\ \quad \land\ \mathrm{WF}_{\mathit{vars}}(\mathit{ContinueAscending}) \quad \text{Must complete in-progress movements} \\ \quad \land\ \mathrm{WF}_{\mathit{vars}}(\mathit{ContinueDescending}) \\ \quad \land\ \mathrm{WF}_{\mathit{vars}}(\mathit{StartAscending} \land \mathit{AtFloor}(1)) \quad \text{Must move from terminal floors} \\ \quad \land\ \mathrm{WF}_{\mathit{vars}}(\mathit{StartDescending} \land \mathit{AtFloor}(\mathit{MaxFloors})) \\ \quad \land\ \forall f \in 2 \mathrel{..} \mathit{MaxFloors} - 1 : \quad \text{Must eventually move from middle floors} \\ \qquad \land\ \mathrm{SF}_{\mathit{vars}}(\mathit{StartAscending} \land \mathit{AtFloor}(f)) \\ \qquad \land\ \mathrm{SF}_{\mathit{vars}}(\mathit{StartDescending} \land \mathit{AtFloor}(f)) \end{array}$$

Complete system specification

$$\mathit{Spec} \triangleq \mathit{Init} \land \Box[\mathit{Next}]_{\mathit{vars}} \land \mathit{Fairness}$$