

Elevator Control System: Formal Specification and Implementation

CS254 Final Project

March 24, 2025

1 Problem Description

We present a formal specification and implementation of a simple elevator control system. The system models an elevator that can move between floors while maintaining essential safety and liveness properties.

2 State Space

The elevator's state is represented by two key variables:

- **position:** Represents both floor locations and between-floor positions
 - Odd numbers ($2f - 1$) indicate the elevator is at floor f
 - Even numbers indicate the elevator is between floors
- **movement:** Direction of travel (Ascending or Descending)

3 System Diagram

```
Floor 5 -----|   |----- pos = 9
                |   |         pos = 8
Floor 4 -----|   |----- pos = 7
                |   |         pos = 6
Floor 3 -----|   |----- pos = 5
                |   |         pos = 4
Floor 2 -----| [E] |----- pos = 3
                |   |         pos = 2
Floor 1 -----|   |----- pos = 1
```

E = Elevator position

Odd numbers (1,3,5,7,9): At floor

Even numbers (2,4,6,8): Between floors

4 Actions

The system supports four basic actions:

1. **StartAscending:** Begin moving up from a floor
2. **ContinueAscending:** Continue moving up between floors
3. **StartDescending:** Begin moving down from a floor
4. **ContinueDescending:** Continue moving down between floors

5 Properties

The system maintains three critical properties:

5.1 Safety Property

ValidBounds: The elevator must stay within valid position bounds

$$position \in [1..2N - 1]$$

where N is the number of floors.

5.2 Liveness Properties

1. **ReachesAllFloors:** The elevator can eventually reach any floor

$$\forall f \in 1..N : \Box \Diamond AtFloor(f)$$

2. **NoStuck:** The elevator cannot get permanently stuck between floors

$$\neg \Diamond \Box InTransit$$

6 Fairness Conditions

To ensure progress, the system implements both weak and strong fairness:

- **Weak Fairness** for:
 - Completing in-progress movements (ContinueAscending, ContinueDescending)
 - Moving from terminal floors
- **Strong Fairness** for:
 - Moving from intermediate floors in either direction