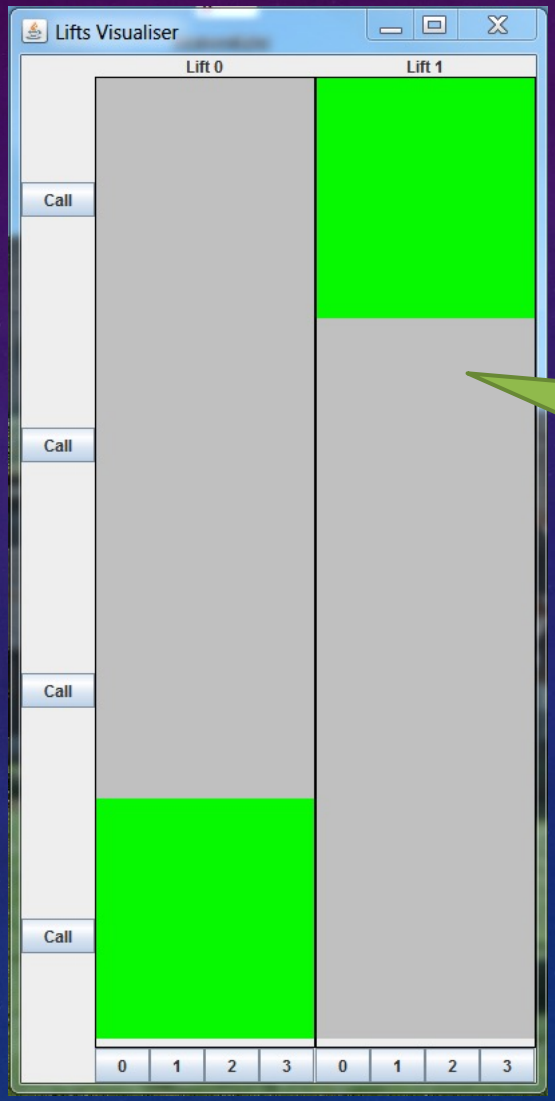
VERIFICATION TECHNIQUES THE ELEVATOR SYSTEM

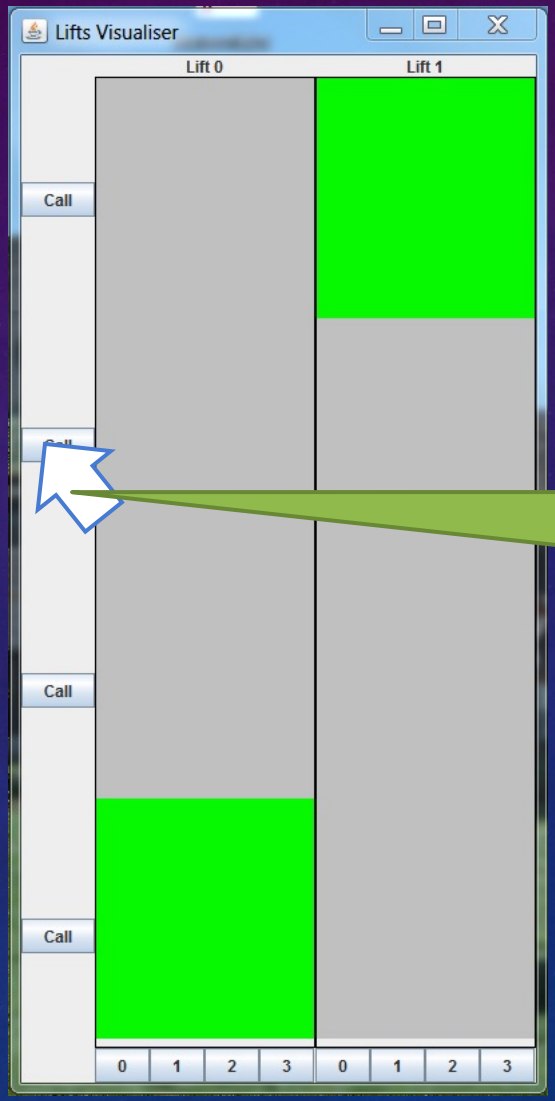
GORDON J. PACE AND CHRISTIAN COLOMBO

UNIVERSITY OF MALTA

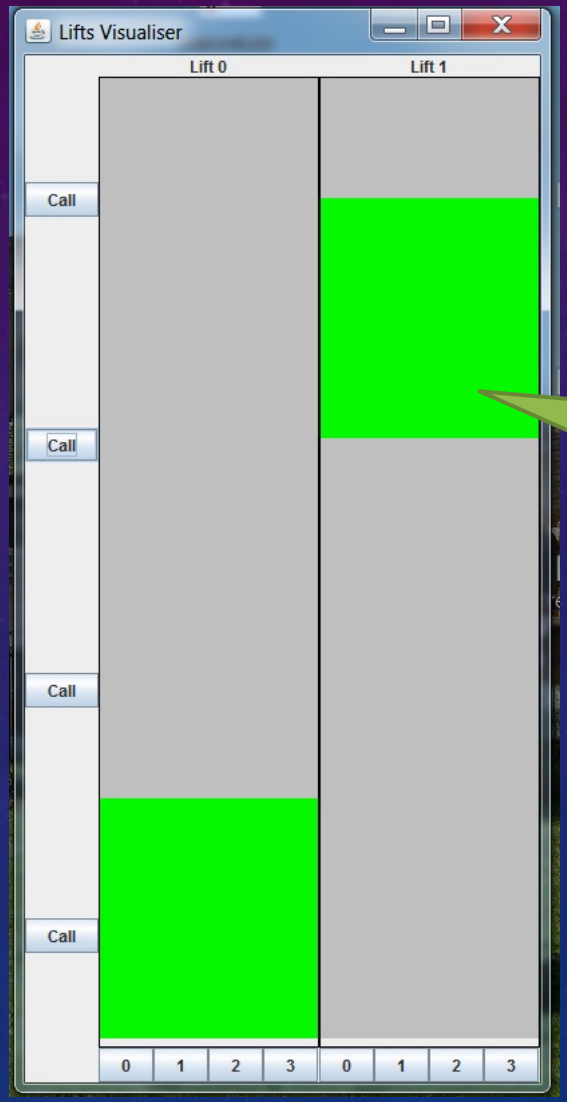
OCTOBER 2020



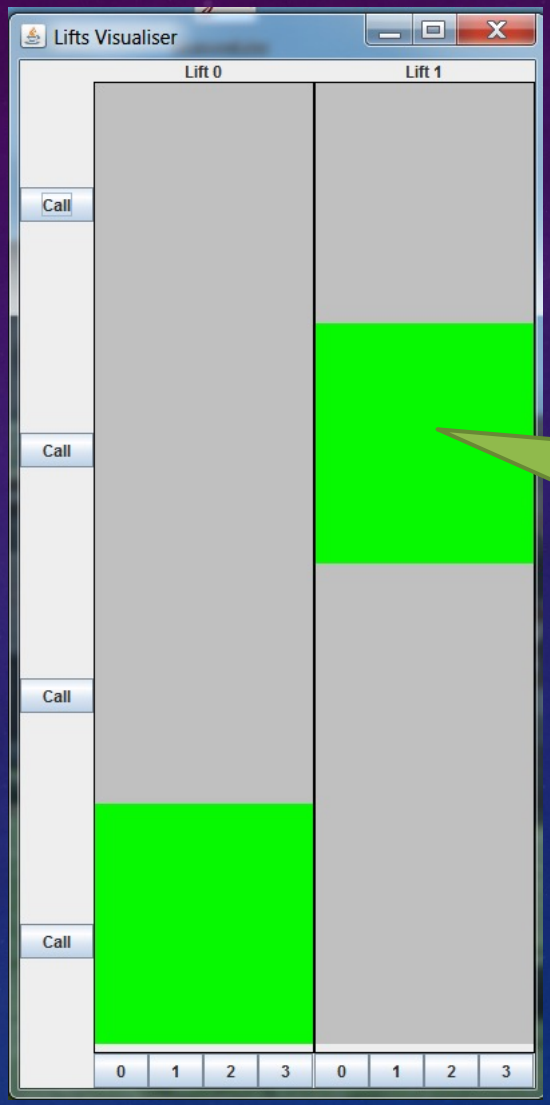
Elevator initial state



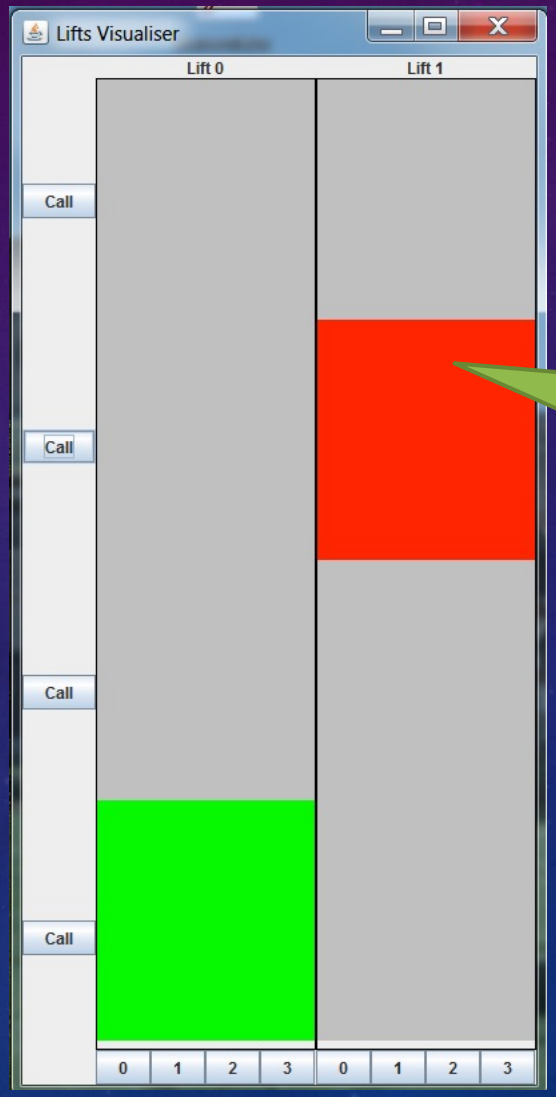
Summon elevator



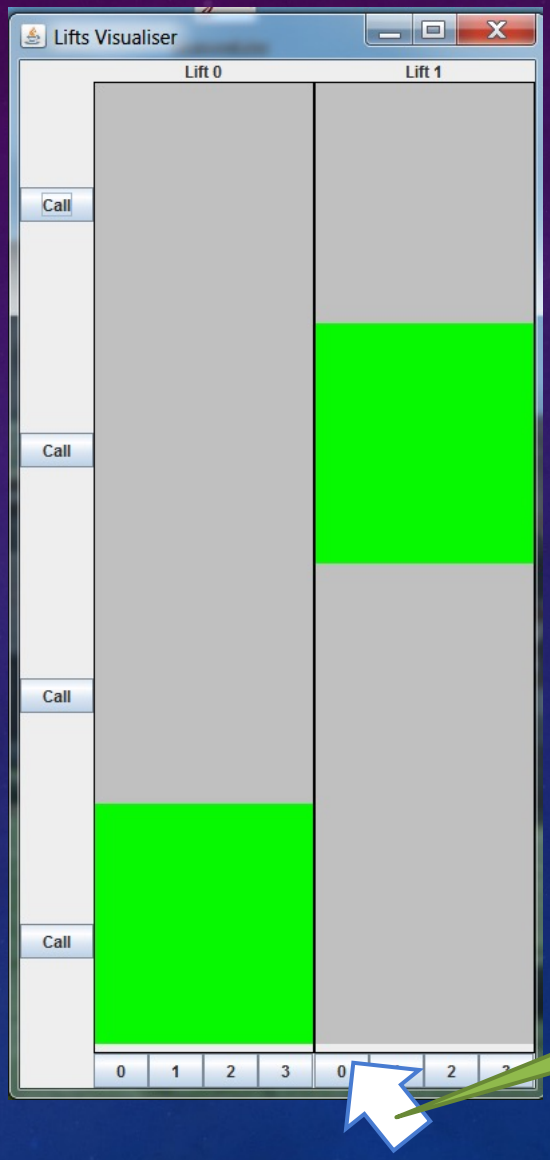
Lift 1 starts moving



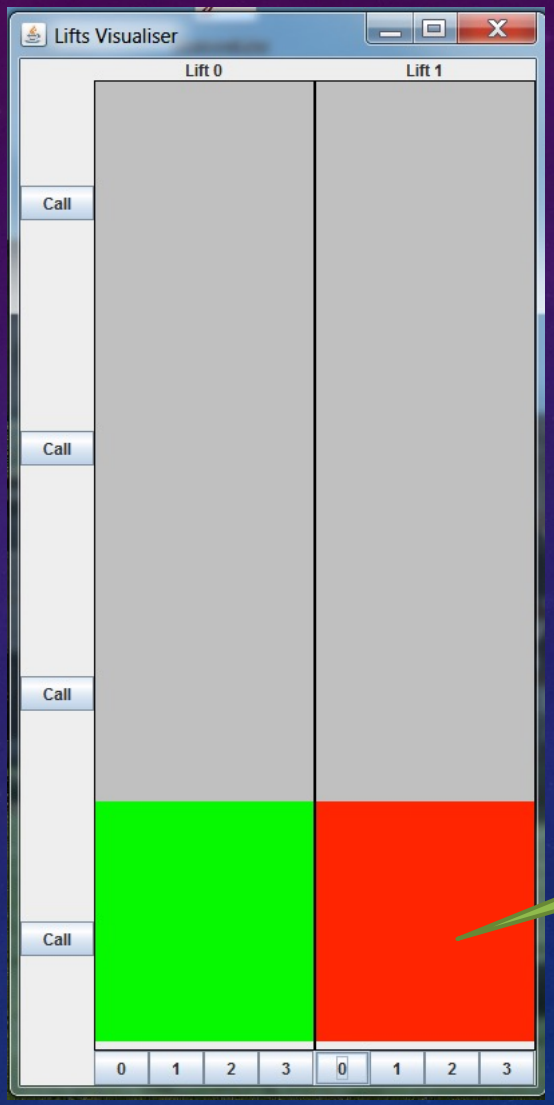
Lift 1 arrives and stops



Lift 1 opens door



User requests floor 0



Elevator moves to floor 0, stops and opens door

EXERCISE

- Can you mention some properties?

UNDERSTANDING THE SYSTEM

- The elevator system has the following **buttons**:
- elevator summoning (1 at each floor)
- elevator floor request (1 per floor in each elevator)

UNDERSTANDING THE SYSTEM

The elevator system has the following **sensors**:

- door is open/close
- elevator is stationary/moving
- elevator is at a particular floor
- elevator is in between floors

UNDERSTANDING THE SYSTEM

The elevator system has the following **control signals**:

- open/close door
- go up/down
- stop

INVARIANTS

- elevator never moves up/down when the door is not closed
- elevator never attempts to go above the topmost floor/below the lowermost floor
- elevator never moves unless a button press occurs which has not yet been serviced
- elevator never stops in between floors
- elevator doors are only opened once the elevator reaches a floor

TEMPORAL PROPERTIES (1)

- when a button (summon or floor request) is pressed, the elevator eventually services the request (Model checking only)
- multiple presses of the same button in between servicing are considered as a single request
- if an elevator is moving through a floor for which a summons button has been pressed, the elevator should service that floor. Otherwise, the elevator closest to the requested floor should service it.

TEMPORAL PROPERTIES (2)

- door opening/closing signals always alternate each other; there should never be two consecutive door opening/two consecutive door closing.
- if the summon button is pressed for a floor where the door is closing, the door should open again
- if the summon button is held down on a floor where the door is not closed, then the door should open and remain open (while the button is held down)

REAL-TIME PROPERTIES

- upon a request, after the door closes, the elevator starts moving in less than 3 seconds
- after the door has been open for 3 seconds, it closes automatically