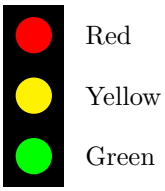
Single Traffic Light System: TLA+ Specification and Analysis

CS254 Final Project

March 24, 2025

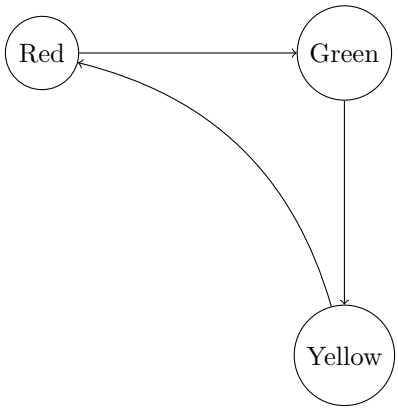
1 System Overview

A simple traffic light system that cycles through three colors: red, green, and yellow.



2 State Transitions

The system follows a strict cyclic pattern:



3 TLA+ Specification

3.1 Variables and Types

```
VARIABLE light
Colors == {"red", "yellow", "green"}

TypeOK == light \in Colors
```

3.2 Initial State

```
Init == light = "red"
```

3.3 State Transitions

```
Next ==
    \/ /\ light = "red"
       /\ light' = "green"
    \/ /\ light = "green"
       /\ light' = "yellow"
    \/ /\ light = "yellow"
       /\ light' = "red"
```

3.4 Safety Properties

The system maintains two types of safety properties:

1. State Safety (Invariant):

```
SafetyInvariant ==
    light \in Colors  \* Only valid colors are allowed
```

2. Transition Safety:

```
Safety ==
    [][
        /\ (light = "red" => light' \in {"red", "green"})
        /\ (light = "green" => light' \in {"green", "yellow"})
        /\ (light = "yellow" => light' \in {"yellow", "red"})
    ]_vars
```

3.5 Liveness Properties

The system ensures that each color eventually appears:

```
Liveness ==
    /\ []<>(light = "red")
    /\ []<>(light = "yellow")
    /\ []<>(light = "green")
```

4 Complete Specification

```
Spec == Init /\ [][Next]_vars /\ Liveness
```

5 Theorems

The specification guarantees:

```
THEOREM Spec => []TypeOK
THEOREM Spec => Safety
```