System Modelling and Design

Traffic Lights

Revision: 2, March 23, 2010

Ken Robinson

School of Computer Science & Engineering
The University of New South Wales, Sydney Australia

August 17, 2011

©Ken Robinson 2005-2010

mailto:k.robinson@unsw.edu.au
Outline I

Objectives of this lecture

A simple 2-way intersection

The Context Machine

The Invariant
  A Safe state
  Strengthening the Invariant
  Other Invariants
  Some Theorems

The ChangeLight Event
  Sequencing
Part I

A simple 2-way intersection
Objectives of this lecture

- To explore the use of a state invariant to ensure safety.
- To explore the specification of some simple traffic light controllers for a simple traffic light controlled intersection.
- To expand safety to a general intersection.
- To model a traffic light controller for a general intersection.
Objectives of this lecture

- To explore the use of a state invariant to ensure safety.
- To explore the specification of some simple traffic light controllers for a simple traffic light controlled intersection.
- To expand safety to a general intersection.
- To model a traffic light controller for a general intersection.
Objectives of this lecture

- To explore the use of a state invariant to ensure safety.
- To explore the specification of some simple traffic light controllers for a simple traffic light controlled intersection.
- To expand safety to a general intersection.
- To model a traffic light controller for a general intersection.
Objectives of this lecture

• To explore the use of a state invariant to ensure safety.
• To explore the specification of some simple traffic light controllers for a simple traffic light controlled intersection.
• To expand safety to a general intersection.
• To model a traffic light controller for a general intersection.
A simple 2-way intersection

Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at *North*, *East*, *South* and *West* positions. The *North* and *South* lights are always identical, as are the *East* and *West* lights.

There are no *right-turn* lights.

Lights should change in the sequence:

Red $\rightarrow$ Green $\rightarrow$ Amber $\rightarrow$ Red $\rightarrow$ ...

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at *North*, *East*, *South* and *West* positions.

The *North* and *South* lights are always identical, as are the *East* and *West* lights.

There are no *right-turn* lights.

Lights should change in the sequence: Red $\rightarrow$ Green $\rightarrow$ Amber $\rightarrow$ Red $\rightarrow$ …

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
A simple 2-way intersection

Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at *North*, *East*, *South* and *West* positions.

The North and South lights are always identical, as are the East and West lights.

There are no right-turn lights.

Lights should change in the sequence:

Red $\rightarrow$ Green $\rightarrow$ Amber $\rightarrow$ Red $\rightarrow$ …

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at *North*, *East*, *South* and *West* positions. The *North* and *South* lights are always identical, as are the *East* and *West* lights.

There are no *right-turn* lights.

Lights should change in the sequence:

Red $\rightarrow$ Green $\rightarrow$ Amber $\rightarrow$ Red $\rightarrow$ ...  

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
A simple 2-way intersection

Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at North, East, South and West positions.

The North and South lights are always identical, as are the East and West lights.

There are no right-turn lights.

Lights should change in the sequence:

Red → Green → Amber → Red → . . .

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
A simple 2-way intersection

Consider traffic lights at the intersection of two roads, one running **North-South** and the other **East-West**.

There are four sets of lights, each capable of showing **Red**, **Green** and **Amber**, placed at **North**, **East**, **South** and **West** positions.

The **North** and **South** lights are always identical, as are the **East** and **West** lights.

There are no **right-turn** lights.

Lights should change in the sequence:

Red → Green → Amber → Red → …

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing *Red*, *Green* and *Amber*, placed at *North*, *East*, *South* and *West* positions.

The *North* and *South* lights are always identical, as are the *East* and *West* lights.

There are no *right-turn* lights.

Lights should change in the sequence:

Red $\rightarrow$ Green $\rightarrow$ Amber $\rightarrow$ Red $\rightarrow$ ...

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
A simple 2-way intersection

Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at *North*, *East*, *South* and *West* positions.

The *North* and *South* lights are always identical, as are the *East* and *West* lights.

There are no *right-turn* lights.

Lights should change in the sequence:

Red → Green → Amber → Red → ...

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
A simple 2-way intersection

Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at *North*, *East*, *South* and *West* positions.

The *North* and *South* lights are always identical, as are the *East* and *West* lights.

There are no *right-turn* lights.

Lights should change in the sequence:

Red $\rightarrow$ Green $\rightarrow$ Amber $\rightarrow$ Red $\rightarrow$ ... 

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
A simple 2-way intersection

Consider traffic lights at the intersection of two roads, one running *North-South* and the other *East-West*.

There are four sets of lights, each capable of showing Red, Green and Amber, placed at *North, East, South* and *West* positions.

The *North* and *South* lights are always identical, as are the *East* and *West* lights.

There are no *right-turn* lights.

Lights should change in the sequence:

Red $\rightarrow$ Green $\rightarrow$ Amber $\rightarrow$ Red $\rightarrow$ …

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
Consider traffic lights at the intersection of two roads, one running \textit{North-South} and the other \textit{East-West}.

There are four sets of lights, each capable of showing \textcolor{Red}{Red}, \textcolor{Green}{Green} and \textcolor{Amber}{Amber}, placed at \textit{North}, \textit{East}, \textit{South} and \textit{West} positions.

The \textit{North} and \textit{South} lights are always identical, as are the \textit{East} and \textit{West} lights.

There are no \textit{right-turn} lights.

Lights should change in the sequence:

\textcolor{Red}{Red} \rightarrow \textcolor{Green}{Green} \rightarrow \textcolor{Amber}{Amber} \rightarrow \textcolor{Red}{Red} \rightarrow \ldots

We wish to specify a traffic light controller that ensures safety and the correct sequencing.
The Context Machine

We will introduce a context machine containing the enumerated sets \textit{DIRECTION} and \textit{LIGHT}.

We will also specify a constant (function) \textit{OTHERDIR} that maps each direction to the other direction.

Context machines must be used in Event B to define sets and constants.
The Context Machine

We will introduce a context machine containing the enumerated sets \( DIRECTION \) and \( LIGHT \).

We will also specify a constant (function) \( OTHERDIR \) that maps each direction to the other direction.

Context machines must be used in Event B to define sets and constants.
We will introduce a context machine containing the enumerated sets $DIRECTION$ and $LIGHT$.

We will also specify a constant (function) $OTHERDIR$ that maps each direction to the other direction.

**Context machines must be used in Event B to define sets and constants.**
TwoWay_ctx.mch

CONTEXT TrafficLights_ctx

SETS

LIGHTS
DIRECTION

CONSTANTS

Red
Green
Amber
NorthSouth
EastWest
OTHERDIR
AXIOMS

axm1: \( \text{LIGHTS} = \{ \text{Red}, \text{Green}, \text{Amber} \} \)

axm2: \( \text{Red} \neq \text{Green} \)

axm3: \( \text{Red} \neq \text{Amber} \)

axm4: \( \text{Green} \neq \text{Amber} \)

axm5: \( \text{DIRECTION} = \{ \text{NorthSouth}, \text{EastWest} \} \)

axm6: \( \text{NorthSouth} \neq \text{EastWest} \)

axm7: \( \text{OTHERDIR} \in \text{DIRECTION} \rightarrow \text{DIRECTION} \)

axm8: \( \text{OTHERDIR}(\text{NorthSouth}) = \text{EastWest} \)

axm9: \( \text{OTHERDIR}(\text{EastWest}) = \text{NorthSouth} \)
THEOREMS

\[ thm1: \forall d \cdot d \in DIRECTION \Rightarrow \text{OTHERDIR}(\text{OTHERDIR}(d)) = d \]

END
The above can be expressed more simply as

**AXIOMS**

\[
\text{axiom: } \text{partition}(\text{LIGHTS}, \{\text{Red}\}, \{\text{Green}\}, \{\text{Amber}\})
\]

\[
\text{axiom: } \text{partition}(\text{DIRECTION}, \{\text{NorthSouth}\}, \{\text{EastWest}\})
\]
The Simple TwoWay Machine

The **TwoWay** machine

1. sees the context machine and has a state of one variable, *lights*, which is a total function from *DIRECTION* to *LIGHT*;
2. has a single event ChangeLight to change the lights;
3. ensures that lights change in the sequence Red, Green, Amber, ...
4. maintains a safe intersection;
The Simple TwoWay Machine

The TwoWay machine

1. sees the context machine and has a state of one variable, lights, which is a total function from DIRECTION to LIGHT;
2. has a single event ChangeLight to change the lights;
3. ensures that lights change in the sequence Red, Green, Amber, ...
4. maintains a safe intersection;
The Simple TwoWay Machine

The TwoWay machine

1. sees the context machine and has a state of one variable, \textit{lights}, which is a total function from \textit{DIRECTION} to \textit{LIGHT};
2. has a single event ChangeLight to change the lights;
3. ensures that lights change in the sequence Red, Green, Amber, …;
4. maintains a safe intersection;
The **TwoWay** machine

1. sees the context machine and has a state of one variable, *lights*, which is a total function from *DIRECTION* to *LIGHT*;
2. has a single event ChangeLight to change the lights;
3. ensures that lights change in the sequence Red, Green, Amber, …;
4. maintains a safe intersection;
The Invariant

1. We wish to formulate an invariant that will ensure safety.
2. Whenever the state is unsafe, the invariant must be false.

\[ \neg (\text{safe}) \implies \neg (\text{invariant}) \]  \hspace{1cm} (1)

3. Conversely, whenever the invariant is true, the state should be safe.

\[ \text{invariant} \implies \text{safe} \]  \hspace{1cm} (2)

4. Of course, 1 and 2 are equivalent; one is the contrapositive of the other: \[ P \implies Q \equiv \neg Q \implies \neg P \]

5. If we have the weakest invariant, then whenever the state is safe, the invariant will be true.

6. We need to find adequately strong guards.
The Invariant

1. We wish to formulate an invariant that will ensure safety.
2. Whenever the state is unsafe, the invariant must be \textit{false}.
   \[ \neg (\text{safe}) \implies \neg (\text{invariant}) \] (1)
3. Conversely, whenever the invariant is \textit{true}, the state should be safe.
   \[ \text{invariant} \implies \text{safe} \] (2)
4. Of course, 1 and 2 are equivalent; one is the \textit{contrapositive} of the other: \[ P \implies Q \equiv \neg Q \implies \neg P \]
5. If we have the \textit{weakest} invariant, then whenever the state is safe, the invariant will be \textit{true}.
6. We need to find adequately strong guards.
### The Invariant

1. We wish to formulate an invariant that will ensure safety.

2. Whenever the state is unsafe, the invariant must be *false*.

\[
\neg (\text{safe}) \implies \neg (\text{invariant}) \tag{1}
\]

3. Conversely, whenever the invariant is *true*, the state should be safe.

\[
\text{invariant} \implies \text{safe} \tag{2}
\]

4. Of course, 1 and 2 are equivalent; one is the *contrapositive* of the other: 
   \[ P \implies Q \equiv \neg Q \implies \neg P \]

5. If we have the *weakest* invariant, then whenever the state is safe, the invariant will be *true*.

6. We need to find adequately strong guards.
The Invariant

1. We wish to formulate an invariant that will ensure safety.
2. Whenever the state is unsafe, the invariant must be false.
   \[ \neg(safe) \implies \neg(invariant) \] (1)
3. Conversely, whenever the invariant is true, the state should be safe.
   \[ invariant \implies safe \] (2)
4. Of course, 1 and 2 are equivalent; one is the contrapositive of the other: \[ P \implies Q \equiv \neg Q \implies \neg P \]
5. If we have the weakest invariant, then whenever the state is safe, the invariant will be true.
6. We need to find adequately strong guards.
1. We wish to formulate an invariant that will ensure safety.

2. Whenever the state is unsafe, the invariant must be \textit{false}.

\[ \neg (\text{safe}) \implies \neg (\text{invariant}) \]  

(1)

3. Conversely, whenever the invariant is \textit{true}, the state should be safe.

\[ \text{invariant} \implies \text{safe} \]  

(2)

4. Of course, 1 and 2 are equivalent; one is the \textit{contrapositive} of the other: \( P \implies Q \equiv \neg Q \implies \neg P \)

5. If we have the \textit{weakest} invariant, then whenever the state is safe, the invariant will be \textit{true}.

6. We need to find adequately strong guards.
The Invariant

1. We wish to formulate an invariant that will ensure safety.
2. Whenever the state is unsafe, the invariant must be false.
   
   \[ \neg (\text{safe}) \implies \neg (\text{invariant}) \]  
   
   (1)
3. Conversely, whenever the invariant is true, the state should be safe.
   
   \[ \text{invariant} \implies \text{safe} \]  
   
   (2)
4. Of course, 1 and 2 are equivalent; one is the contrapositive of the other:
   
   \[ P \implies Q \equiv \neg Q \implies \neg P \]
5. If we have the weakest invariant, then whenever the state is safe, 
   the invariant will be true.
6. We need to find adequately strong guards.
The Invariant

1. We wish to formulate an invariant that will ensure safety.

2. Whenever the state is unsafe, the invariant must be false.

\[ \neg(safe) \implies \neg(invariant) \]  \hspace{1cm} (1)

3. Conversely, whenever the invariant is true, the state should be safe.

\[ invariant \implies safe \]  \hspace{1cm} (2)

4. Of course, 1 and 2 are equivalent; one is the contrapositive of the other: \( P \implies Q \equiv \neg Q \implies \neg P \)

5. If we have the weakest invariant, then whenever the state is safe, the invariant will be true.

6. We need to find adequately strong guards.
A Safe state

The state invariant should be:

1. false for all unsafe states, true for all safe states
2. An initial attempt at an invariant might be

   \( \neg (\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green}) \)

   which, using the predicate identities

   \( \neg (P \land Q) = \neg P \lor \neg Q = P \implies \neg Q \),

   may be written

   \( \text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg (\text{lights}(\text{EastWest}) = \text{Green}) \)

If used as a term in a larger predicate, the above implication may need to be parenthesised.
A Safe state

The state invariant should be:

1. *false* for all unsafe states    *true* for all safe states
2. An initial attempt at an invariant might be

\[-(\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green})\]

which, using the predicate identities

\[-(P \land Q) = \neg P \lor \neg Q = P \implies \neg Q\]

may be written

\[\text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg(\text{lights}(\text{EastWest}) = \text{Green})\]

If used as a term in a larger predicate, the above implication may need to be parenthesised.
A Safe state

The state invariant should be:

1. *false* for all unsafe states    *true* for all safe states
2. An initial attempt at an invariant might be

\[ \neg (\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green}) \]

which, using the predicate identities

\[ \neg (P \land Q) = \neg P \lor \neg Q = P \implies \neg Q \]

may be written

\[ \text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg (\text{lights}(\text{EastWest}) = \text{Green}) \]

If used as a term in a larger predicate, the above implication may need to be parenthesised.
A Safe state

The state invariant should be:

1. \textit{false} for all unsafe states \textit{true} for all safe states
2. An initial attempt at an invariant might be

\[ \neg (\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green}) \]

which, using the predicate identities

\[ \neg (P \land Q) = \neg P \lor \neg Q = P \implies \neg Q \]

may be written

\[ \text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg (\text{lights}(\text{EastWest}) = \text{Green}) \]

If used as a term in a larger predicate, the above implication may need to be parenthesised.
A Safe state

The state invariant should be:

1. *false* for all unsafe states  
   *true* for all safe states

2. An initial attempt at an invariant might be

   \[ \neg (\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green}) \]

which, using the predicate identities

\[ \neg (P \land Q) \equiv \neg P \lor \neg Q \equiv P \implies \neg Q \]

may be written

\[ \text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg (\text{lights}(\text{EastWest}) = \text{Green}) \]

If used as a term in a larger predicate, the above implication may need to be parenthesised.
A Safe state

The state invariant should be:

1. $false$ for all unsafe states $true$ for all safe states
2. An initial attempt at an invariant might be

$$\neg (\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green})$$

which, using the predicate identities

$$\neg (P \land Q) \equiv \neg P \lor \neg Q \equiv P \implies \neg Q,$$

may be written

$$\text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg (\text{lights}(\text{EastWest}) = \text{Green})$$

If used as a term in a larger predicate, the above implication may need to be parenthesised.
A Safe state

The state invariant should be:

1. *false* for all unsafe states  *true* for all safe states
2. An initial attempt at an invariant might be

\[ \neg (\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green}) \]

which, using the predicate identities

\[ \neg (P \land Q) \equiv \neg P \lor \neg Q \equiv P \implies \neg Q \]

may be written

\[ \text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg (\text{lights}(\text{EastWest}) = \text{Green}) \]

If used as a term in a larger predicate, the above implication may need to be parenthesised.
A Safe state

The state invariant should be:

1. *false* for all unsafe states  *true* for all safe states
2. An initial attempt at an invariant might be

   \[ \neg (\text{lights}(\text{NorthSouth}) = \text{Green} \land \text{lights}(\text{EastWest}) = \text{Green}) \]

   which, using the predicate identities

   \[ \neg (P \land Q) \equiv \neg P \lor \neg Q \equiv P \implies \neg Q \]

   may be written

   \[ \text{lights}(\text{NorthSouth}) = \text{Green} \implies \neg (\text{lights}(\text{EastWest}) = \text{Green}) \]

If used as a term in a larger predicate, the above implication may need to be parenthesised.
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[ \neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\}) \land \text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\}) \equiv \]
\[ (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \neg (\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\})) \equiv \]
\[ (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{EastWest}) = \text{Red}) \]
**Strengthening the Invariant**

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[
\neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \land \text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\})
\equiv
\neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \neg (\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\}))
\equiv
(\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{EastWest}) = \text{Red})
\]
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[ \neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \land \text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\}) \equiv (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \neg (\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\}) \equiv (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{EastWest}) = \text{Red}) \]
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[ \neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \land \
\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\}) \equiv \\
(\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \\
\neg (\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\})) \equiv \\
(\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \\
\text{lights}(\text{EastWest}) = \text{Red}) \] (3)
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[
\neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green}, \text{Amber}\} \land \text{lights}(\text{EastWest}) \in \{\text{Green}, \text{Amber}\})
\]

\[
\equiv
\]

\[
(\text{lights}(\text{NorthSouth}) \in \{\text{Green}, \text{Amber}\} \implies
\neg (\text{lights}(\text{EastWest}) \in \{\text{Green}, \text{Amber}\}))
\]

\[
\equiv
\]

\[
(\text{lights}(\text{NorthSouth}) \in \{\text{Green}, \text{Amber}\} \implies \text{lights}(\text{EastWest}) = \text{Red})
\]
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[
\neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \land \text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\}) \\
\equiv \\
(\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \Rightarrow \\
\neg (\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\})) \\
\equiv \\
(\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \Rightarrow \\
\text{lights}(\text{EastWest}) = \text{Red})
\]
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[
\neg (\text{lights(} \text{NorthSouth}) \in \{\text{Green, Amber}\} \land \text{lights(} \text{EastWest}) \in \{\text{Green, Amber}\}) \\
\equiv \\
(\text{lights(} \text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \\
\neg (\text{lights(} \text{EastWest}) \in \{\text{Green, Amber}\})) \\
\equiv \\
(\text{lights(} \text{NorthSouth}) \in \{\text{Green, Amber}\} \implies \text{lights(} \text{EastWest}) = \text{Red})
\]
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[ \neg ( \text{lights}(\text{NorthSouth}) \in \{ \text{Green}, \text{Amber} \} \land \text{lights}(\text{EastWest}) \in \{ \text{Green}, \text{Amber} \} ) \equiv ( \text{lights}(\text{NorthSouth}) \in \{ \text{Green}, \text{Amber} \} \implies \neg ( \text{lights}(\text{EastWest}) \in \{ \text{Green}, \text{Amber} \} )) \equiv ( \text{lights}(\text{NorthSouth}) \in \{ \text{Green}, \text{Amber} \} \implies \text{lights}(\text{EastWest}) = \text{Red} ) \]
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

$$\neg(lights(NorthSouth) \in \{\text{Green, Amber}\} \land lights(EastWest) \in \{\text{Green, Amber}\})$$

$$\equiv$$

$$\neg(lights(EastWest) \in \{\text{Green, Amber}\})$$

$$\equiv$$

$$lights(NorthSouth) \in \{\text{Green, Amber}\} \implies \neg(lights(EastWest) \in \{\text{Green, Amber}\})$$

$$\equiv$$

$$lights(NorthSouth) \in \{\text{Green, Amber}\} \implies lights(EastWest) = \text{Red}$$  (3)
Strengthening the Invariant

Clearly, the light in both directions cannot be either Green or Amber.

<table>
<thead>
<tr>
<th></th>
<th>Red</th>
<th>Green</th>
<th>Amber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>safe</td>
<td>safe</td>
<td>safe</td>
</tr>
<tr>
<td>Green</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
<tr>
<td>Amber</td>
<td>safe</td>
<td>unsafe</td>
<td>unsafe</td>
</tr>
</tbody>
</table>

This leads to the invariant:

\[
\neg (\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \land \\
\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\}) \\
\equiv \\
(\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \Rightarrow \\
\neg (\text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\})) \\
\equiv \\
(\text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \Rightarrow \\
\text{lights}(\text{EastWest}) = \text{Red})
\]
Other Invariants

There are other invariants that adequately express safety for a two-way intersection:

\[ \text{lights}(\text{NorthSouth}) = \text{Red} \lor \text{lights}(\text{EastWest}) = \text{Red} \]

\[ \text{Red} \in \text{ran(} \text{lights} \text{)} \]

But these conditions do not generalise to intersections with more than two ways. Indeed the expression of the invariant that best generalises is

\[ \forall \text{dir}. \text{dir} \in \text{DIRECTION} \land \text{lights}(\text{dir}) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{OTHERDIR}(\text{dir})) = \text{Red} \] (4)
Other Invariants

There are other invariants that adequately express safety for a two-way intersection:

\[ \text{lights}(\text{NorthSouth}) = \text{Red} \lor \text{lights}(\text{EastWest}) = \text{Red} \]

\[ \text{Red} \in \text{ran}(\text{lights}) \]

But these conditions do not generalise to intersections with more than two ways. Indeed the expression of the invariant that best generalises is

\[ \forall \text{dir}. \text{dir} \in \text{DIRECTION} \land \text{lights}(\text{dir}) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{OTHERDIR}(\text{dir})) = \text{Red} \] (4)
Other Invariants

There are other invariants that adequately express safety for a two-way intersection:

\[
lights(NorthSouth) = \text{Red} \lor lights(EastWest) = \text{Red}
\]

\[
\text{Red} \in \text{ran}(lights)
\]

But these conditions do not generalise to intersections with more than two ways. Indeed the expression of the invariant that best generalises is

\[
\forall dir. dir \in \text{DIRECTION} \land lights(dir) \in \{\text{Green, Amber}\} \implies lights(OTHERDIR(dir)) = \text{Red}
\]
Other Invariants

There are other invariants that adequately express safety for a two-way intersection:

\[
lights(NorthSouth) = Red \lor lights(EastWest) = Red
\]

\[
Red \in \text{ran}(lights)
\]

But these conditions do not generalise to intersections with more than two ways. Indeed the expression of the invariant that best generalises is

\[
\forall \text{dir}. \text{dir} \in DIRECTION \land lights(\text{dir}) \in \{\text{Green, Amber}\} \implies lights(\text{OTHERDIR}(\text{dir})) = Red
\]
Other Invariants

There are other invariants that adequately express safety for a two-way intersection:

$$\text{lights}(\text{NorthSouth}) = \text{Red} \lor \text{lights}(\text{EastWest}) = \text{Red}$$

$$\text{Red} \in \text{ran}(\text{lights})$$

But these conditions do not generalise to intersections with more than two ways. Indeed the expression of the invariant that best generalises is

$$\forall \text{dir}. \text{dir} \in \text{DIRECTION} \land \text{lights}(\text{dir}) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{OTHERDIR}(\text{dir})) = \text{Red}$$

(4)
Other Invariants

There are other invariants that adequately express safety for a two-way intersection:

\[ \text{lights} (\text{NorthSouth}) = \text{Red} \lor \text{lights} (\text{EastWest}) = \text{Red} \]

\[ \text{Red} \in \text{ran} (\text{lights}) \]

But these conditions do not generalise to intersections with more than two ways. Indeed the expression of the invariant that best generalises is

\[ \forall \text{dir}. \text{dir} \in \text{DIRECTION} \land \text{lights} (\text{dir}) \in \{ \text{Green, Amber} \} \implies \text{lights} (\text{OTHERDIR(dir)}) = \text{Red} \]
Some Theorems

In this model of **TwoWay** we add the following alternative formulations of the invariant as theorems:

- \( \forall dir. (dir \in DIRECTION \land \text{lights}(dir) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{OTHERDIR}(dir)) = \text{Red}) \)

- \( \text{lights}(\text{EastWest}) \in \{\text{Green, Amber}\} \implies \text{lights}(\text{NorthSouth}) = \text{Red} \)

Theorems contain properties that are implied by the invariant, and hence discharging the proof obligations for the assertions proves that each conjunct in the assertions is implied by the invariant.
The ChangeLight Event

The ChangeLight event will have two parameters \( dir \) and \( light \). The event will change the lights in direction \( dir \) to colour \( light \)

\[
lights(dir) := light
\]

The guards need to be strong enough to ensure both safety and correct sequencing.

Safety can be ensured with the guard:

\[
(light \in \{\text{Green, Amber}\} \implies lights(\text{OTHERDIR}(dir)) = \text{Red})
\]
The ChangeLight Event

The ChangeLight event will have two parameters $dir$ and $light$. The event will change the lights in direction $dir$ to colour $light$.

$$\text{lights}(dir) := light$$

The guards need to be strong enough to ensure both safety and correct sequencing. Safety can be ensured with the guard:

$$(\text{light} \in \{\text{Green, Amber}\} \implies \text{lights}(\text{OTHERDIR}(dir)) = \text{Red})$$
The ChangeLight Event

The ChangeLight event will have two parameters \( dir \) and \( light \). The event will change the lights in direction \( dir \) to colour \( light \).

\[
lights(dir) := light
\]

The guards need to be strong enough to ensure both safety and correct sequencing. Safety can be ensured with the guard:

\[
(light \in \{\text{Green, Amber}\} \implies \text{lights} (\text{OTHERDIR}(dir)) = \text{Red})
\]
The ChangeLight Event

The ChangeLight event will have two parameters \textit{dir} and \textit{light}. The event will change the lights in direction \textit{dir} to colour \textit{light}

\[ \text{lights}(\text{dir}) := \text{light} \]

The guards need to be strong enough to ensure both safety and correct sequencing.

Safety can be ensured with the guard:

\[ (\text{light} \in \{\text{Green, Amber}\} \implies \text{lights}(\text{OTHERDIR(dir)}) = \text{Red}) \]
The ChangeLight Event

The ChangeLight event will have two parameters $dir$ and $light$. The event will change the lights in direction $dir$ to colour $light$

$$lights(dir) := light$$

The guards need to be strong enough to ensure both safety and correct sequencing.

Safety can be ensured with the guard:

$$(light \in \{\text{Green, Amber}\} \implies lights(\text{OTHERDIR}(dir)) = \text{Red})$$
The ChangeLight Event

The ChangeLight event will have two parameters \( dir \) and \( light \). The event will change the lights in direction \( dir \) to colour \( light \)

\[
lights(dir) := light
\]

The guards need to be strong enough to ensure both safety and correct sequencing.
Safety can be ensured with the guard:

\[
(light \in \{\text{Green, Amber}\} \implies lights(OTHERDIR(dir)) = \text{Red})
\]
Sequencing

Changing to

**Red**: the current colour should be *Amber*, so
\[ \text{light} = \text{Red} \implies \text{lights(dir)} = \text{Green} \]

**Green**: the current colour should be *Red*, so
\[ \text{light} = \text{Green} \implies \text{lights(dir)} = \text{Red} \]

**Amber**: the current colour should be *Green*, so
\[ \text{light} = \text{Amber} \implies \text{lights(dir)} = \text{Green} \]

Notice that the sequencing guards for both *Red* and *Amber* together with the invariant ensure safety, we only need to be concerned with safety for changing to *Green*. 
Sequencing

Changing to

**Red:** the current colour should be **Amber**, so
\[ \text{light} = \text{Red} \implies \text{lights}(\text{dir}) = \text{Green} \]

**Green:** the current colour should be **Red**, so
\[ \text{light} = \text{Green} \implies \text{lights}(\text{dir}) = \text{Red} \]

**Amber:** the current colour should be **Green**, so
\[ \text{light} = \text{Amber} \implies \text{lights}(\text{dir}) = \text{Green} \]

Notice that the sequencing guards for both **Red** and **Amber** together with the invariant ensure safety, we only need to be concerned with safety for changing to **Green**.
Sequencing

Changing to

**Red**: the current colour should be *Amber*, so 

\[ \text{light} = \text{Red} \implies \text{lights}(dir) = \text{Green} \]

**Green**: the current colour should be *Red*, so 

\[ \text{light} = \text{Green} \implies \text{lights}(dir) = \text{Red} \]

**Amber**: the current colour should be *Green*, so 

\[ \text{light} = \text{Amber} \implies \text{lights}(dir) = \text{Green} \]

Notice that the sequencing guards for both *Red* and *Amber* together with the invariant ensure safety, we only need to be concerned with safety for changing to *Green*. 
Sequencing

Changing to

**Red**: the current colour should be *Amber*, so

\[ \text{light} = \text{Red} \implies \text{lights}(\text{dir}) = \text{Green} \]

**Green**: the current colour should be *Red*, so

\[ \text{light} = \text{Green} \implies \text{lights}(\text{dir}) = \text{Red} \]

**Amber**: the current colour should be *Green*, so

\[ \text{light} = \text{Amber} \implies \text{lights}(\text{dir}) = \text{Green} \]

Notice that the sequencing guards for both *Red* and *Amber* together with the invariant ensure safety, we only need to be concerned with safety for changing to *Green*. 
Changing to

**Red:** the current colour should be **Amber**, so
\[ \text{light} = \text{Red} \implies \text{lights}(\text{dir}) = \text{Green} \]

**Green:** the current colour should be **Red**, so
\[ \text{light} = \text{Green} \implies \text{lights}(\text{dir}) = \text{Red} \]

**Amber:** the current colour should be **Green**, so
\[ \text{light} = \text{Amber} \implies \text{lights}(\text{dir}) = \text{Green} \]

Notice that the sequencing guards for both **Red** and **Amber** together with the invariant ensure safety, we only need to be concerned with safety for changing to **Green**.
The final guards that ensure both safety and correct sequencing are:

\[
\begin{align*}
\text{light} &= \text{Red} \quad \implies \quad \text{lights(dir)} = \text{Amber} \\
\text{light} &= \text{Green} \quad \implies \quad \text{lights(dir)} = \text{Red} \\
\text{light} &= \text{Green} \quad \implies \quad \text{lights(OTHERDIR(dir))} = \text{Red} \\
\text{light} &= \text{Amber} \quad \implies \quad \text{lights(dir)} = \text{Green}
\end{align*}
\]
Final Guards for ChangeLight

The final guards that ensure both safety and correct sequencing are:

- \( \text{light} = \text{Red} \implies \text{lights(dir)} = \text{Amber} \)
- \( \text{light} = \text{Green} \implies \text{lights(dir)} = \text{Red} \)
- \( \text{light} = \text{Green} \implies \text{lights(OTHERDIR(dir))} = \text{Red} \)
- \( \text{light} = \text{Amber} \implies \text{lights(dir)} = \text{Green} \)
Final Guards for ChangeLight

The final guards that ensure both safety and correct sequencing are:

\[
\begin{align*}
\text{light} = \text{Red} & \implies \text{lights}(dir) = \text{Amber} \\
\text{light} = \text{Green} & \implies \text{lights}(dir) = \text{Red} \\
\text{light} = \text{Green} & \implies \text{lights}(\text{OTHERDIR}(dir)) = \text{Red} \\
\text{light} = \text{Amber} & \implies \text{lights}(dir) = \text{Green}
\end{align*}
\]
The final guards that ensure both safety and correct sequencing are:

\[
\begin{align*}
\text{light} = \text{Red} & \quad \implies \quad \text{lights(dir)} = \text{Amber} \\
\text{light} = \text{Green} & \quad \implies \quad \text{lights(dir)} = \text{Red} \\
\text{light} = \text{Green} & \quad \implies \quad \text{lights(OTHERDIR(dir))} = \text{Red} \\
\text{light} = \text{Amber} & \quad \implies \quad \text{lights(dir)} = \text{Green}
\end{align*}
\]
Final Guards for ChangeLight

The final guards that ensure both safety and correct sequencing are:

\[
\begin{align*}
\text{light} = \text{Red} & \implies \text{lights}(\text{dir}) = \text{Amber} \\
\text{light} = \text{Green} & \implies \text{lights}(\text{dir}) = \text{Red} \\
\text{light} = \text{Green} & \implies \text{lights}(\text{OTHERDIR}(\text{dir})) = \text{Red} \\
\text{light} = \text{Amber} & \implies \text{lights}(\text{dir}) = \text{Green}
\end{align*}
\]
The ChangeLight Event I

MACHINE ChangeLights

SEES TrafficLights_ctx

VARIABLES

\( \text{lights} \)

INVARINANTS

\[ \text{inv1: } \text{lights} \in \text{DIRECTION} \rightarrow \text{LIGHTS} \]

\[ \text{inv2: } \text{lights}(\text{NorthSouth}) \in \{\text{Green, Amber}\} \]

\[ \Rightarrow \text{lights}(\text{EastWest}) = \text{Red} \]
The ChangeLight Event II

EVENTS

Initialisation
begin
act1: \( \text{lights} := \{\text{NorthSouth} \mapsto \text{Red}, \text{EastWest} \mapsto \text{Red}\} \)
end
The ChangeLight Event III

Event  ToAmber  ≜

any  dir

when

grd1:  dir ∈ DIRECTION

grd2:  lights(dir) = Green

then

act1:  lights(dir) := Amber

end
The ChangeLight Event IV

Event $ToGreen \triangleq$

any dir

when

$grd1$: $dir \in DIRECTION$

$grd2$: $\text{lights}(\text{OTHERDIR}(dir)) = \text{Red}$

$grd3$: $\text{lights}(dir) = \text{Red}$

then

$act1$: $\text{lights}(dir) := \text{Green}$

end
Event $ToRed \triangleq$

any $dir$

when

$grd1$: $dir \in DIRECTION$

$grd2$: $lights(dir) = Amber$

then

$act1$: $lights(dir) := Red$

end

END
Part II

A general multi-way intersection
A General Multi-Way Intersection

The New Safety Invariant

A Traffic Light Controller
We will now expand to a completely general intersection with many directions, denoted by the finite set $DIRECTION$. To define directions that conflict with one another we will use a relation $CONFLICT$ that maps each direction to all other directions, with which it conflicts. Clearly, $CONFLICT$ must have the following properties:

- No direction conflicts with itself.
- Conflicts are symmetric: if $dir_1$ conflicts with $dir_2$ then $dir_2$ conflicts with $dir_1$. 
We will now expand to a completely general intersection with many directions, denoted by the finite set $DIRECTION$. To define directions that conflict with one another we will use a relation $CONFLICT$ that maps each direction to all other directions, with which it conflicts.

Clearly, $CONFLICT$ must have the following properties:

- No direction conflicts with itself.
- Conflicts are symmetric: if $dir_1$ conflicts with $dir_2$ then $dir_2$ conflicts with $dir_1$. 
A General-Multi-Way Intersection

We will now expand to a completely general intersection with many directions, denoted by the finite set \( DIRECTION \). To define directions that conflict with one another we will use a relation \( CONFLICT \) that maps each direction to all other directions, with which it conflicts. Clearly, \( CONFLICT \) must have the following properties:

- No direction conflicts with itself.
- Conflicts are symmetric: if \( dir_1 \) conflicts with \( dir_2 \) then \( dir_2 \) conflicts with \( dir_1 \).
We will now expand to a completely general intersection with many directions, denoted by the finite set $DIRECTION$. To define directions that conflict with one another we will use a relation $CONFLICT$ that maps each direction to all other directions, with which it conflicts. Clearly, $CONFLICT$ must have the following properties:

- No direction conflicts with itself.
- Conflicts are symmetric: if $dir_1$ conflicts with $dir_2$ then $dir_2$ conflicts with $dir_1$. 


A General-Multi-Way Intersection

We will now expand to a completely general intersection with many directions, denoted by the finite set $DIRECTION$. To define directions that conflict with one another we will use a relation $CONFLICT$ that maps each direction to all other directions, with which it conflicts. Clearly, $CONFLICT$ must have the following properties:

- No direction conflicts with itself.
- Conflicts are symmetric: if $dir_1$ conflicts with $dir_2$ then $dir_2$ conflicts with $dir_1$. 
The New Safety Invariant

The safety invariant for our generalised intersection is

$$\forall d. d \in DIRECTION \land lights(d) \in \{\text{Green}, \text{Amber}\} \implies lights[CONFLICT[\{d\}] = \{\text{Red}\}$$  \hspace{1cm} (5)

This can be seen as a generalisation of the earlier safety invariant (4).
A General Multi-Way Intersection

TrafficLights1_ctx

CONTEXT TrafficLights1_ctx

SETS

LIGHTS
DIRECTION
TrafficLights1_ctx II

CONSTANTS

Red
Green
Amber
CONFLICT
adir
A General Multi-Way Intersection

TrafficLights1_ctx III

AXIOMS

axm1:  \( \text{partition(LIGHTS, \{Red\}, \{Green\}, \{Amber\})} \)

Three light colours

axm2:  \( \text{finite(DIRECTION)} \)

DIRECTION is a finite set of directions

axm3:  \( \text{CONFLICT} \in DIRECTION \iff DIRECTION \)

CONFLICT relates conflicting directions

axm4:  \( \text{CONFLICT} \cap (DIRECTION \triangle id) = \varnothing \)

a direction cannot conflict with itself

axm5:  \( \text{CONFLICT}^{-1} = \text{CONFLICT} \)

conflicts are symmetric

thm1:  \( \forall d \cdot d \in DIRECTION \Rightarrow d \notin \text{CONFLICT}[[\{d\}]] \)

thm2:  \( \forall d1, d2 \cdot d1 \notin \text{CONFLICT}[[\{d2\}] \Rightarrow d2 \notin \text{CONFLICT}[[\{d1\}]] \)
TrafficLights1_ctx IV

\[ \text{axm6: } adir \in \text{DIRECTION} \quad \text{any direction (used as a parameter)} \]

END
A Traffic Light Controller

We will now model a traffic light controller that responds to the following requirements:

1. A controller is required that can be used to control the whole of a general intersection.
2. The controller must be able to set the light in any direction to Green and must do so in a safe transition sequence.
3. The intersection must always be in a safe state.
A General Multi-Way Intersection

A Traffic Light Controller

We will now model a traffic light controller that responds to the following requirements:

1. A controller is required that can be used to control the whole of a general intersection.

2. The controller must be able to set the light in any direction to Green and must do so in a safe transition sequence.

3. The intersection must always be in a safe state.
We will now model a traffic light controller that responds to the following requirements:

1. A controller is required that can be used to control the whole of a general intersection.

2. The controller must be able to set the light in any direction to Green and must do so in a safe transition sequence.

3. The intersection must always be in a safe state.
A Traffic Light Controller

We will now model a traffic light controller that responds to the following requirements:

1. A controller is required that can be used to control the whole of a general intersection.
2. The controller must be able to set the light in any direction to Green and must do so in a safe transition sequence.
3. The intersection must always be in a safe state.
Our response to the preceding request is

1. to produce a machine with a single event that changes the light in any arbitrary direction, modelled by a constant \( a_{dir} \), to Green, setting all lights in conflicting directions to Red;
2. to model the top-level state as having only Red and Green, these being the “steady state” light colours;
3. to refine that machine to model the process of changing the state while maintaining a safe state.
4. towards safety, the transition from Green to Red will introduce the light colour Amber and delays between light transitions.
Our Response

Our response to the preceding request is

1. to produce a machine with a single event that changes the light in any arbitrary direction, modelled by a constant $adir$, to Green, setting all lights in conflicting directions to Red;

2. to model the top-level state as having only Red and Green, these being the “steady state” light colours;

3. to refine that machine to model the process of changing the state while maintaining a safe state.

4. towards safety, the transition from Green to Red will introduce the light colour Amber and delays between light transitions.
Our response to the preceding request is

1. to produce a machine with a single event that changes the light in any arbitrary direction, modelled by a constant $adir$, to Green, setting all lights in conflicting directions to Red;

2. to model the top-level state as having only Red and Green, these being the “steady state” light colours;

3. to refine that machine to model the process of changing the state while maintaining a safe state.

4. towards safety, the transition from Green to Red will introduce the light colour Amber and delays between light transitions.
Our response to the preceding request is

1. to produce a machine with a single event that changes the light in any arbitrary direction, modelled by a constant $\text{adir}$, to Green, setting all lights in conflicting directions to Red;
2. to model the top-level state as having only Red and Green, these being the “steady state” light colours;
3. to refine that machine to model the process of changing the state while maintaining a safe state.
4. towards safety, the transition from Green to Red will introduce the light colour Amber and delays between light transitions.
Our response to the preceding request is

1. to produce a machine with a single event that changes the light in any arbitrary direction, modelled by a constant $adir$, to Green, setting all lights in conflicting directions to Red;

2. to model the top-level state as having only Red and Green, these being the “steady state” light colours;

3. to refine that machine to model the process of changing the state while maintaining a safe state.

4. towards safety, the transition from Green to Red will introduce the light colour Amber and delays between light transitions.
Our response to the preceding request is

1. to produce a machine with a single event that changes the light in any arbitrary direction, modelled by a constant $adir$, to \textbf{Green}, setting all lights in conflicting directions to \textbf{Red};

2. to model the top-level state as having only \textbf{Red} and \textbf{Green}, these being the “steady state” light colours;

3. to refine that machine to model the process of changing the state while maintaining a safe state.

4. towards safety, the transition from \textbf{Green} to \textbf{Red} will introduce the light colour \textbf{Amber} and delays between light transitions.
MACHINE ChangeLight1

SEES TrafficLights1_ctx

VARIABLES

\[ lights \]

INVARIANTS

\[ \text{inv1: } lights \in DIRECTION \rightarrow \{ \text{Red, Green} \} \]

\[ \text{inv2: } \forall d \cdot d \in DIRECTION \land lights(d) = \text{Green} \Rightarrow lights[\text{CONFLICT}\{d\}] \subseteq \{ \text{Red} \} \]
EVENTS

Initialisation

begin

act1: \textit{lights} : |

\begin{align*}
\text{lights'} & \in \text{DIRECTION} \rightarrow \{\text{Red, Green}\} \\
& \wedge (\forall d \cdot d \in \text{DIRECTION} \\
& \wedge \text{lights'}(d) = \text{Green} \\
& \Rightarrow \text{lights'}[\text{CONFLICT}([d])] \subseteq \{\text{Red}\})
\end{align*}

end
Event \( ToGreen \) \( \iff \)

when

\( grd1: \) \( lights(adir) = Red \)
then

\( act1: \) \( lights := lights \)
\( \leftarrow (CONFLICT[\{adir\}] \times \{Red\}) \)
\( \leftarrow \{adir \mapsto Green\} \)

end

END
The first stage is still abstract and would be very unsafe, if implemented literally according to the model, as it is not safe to change lights instantaneously from Green to Red. This refinement introduces Amber into the lights sequence and the following slave events:

- **ToAmber**: changes, in arbitrary sequence, all the currently Green lights in conflicting directions to Amber;
- **ToRed**: changes the Amber lights to Red;
- **Delay**: models a delay between Amber and Red and between Red and the final setting of the light in the adir direction to Green.

The refinement of ToGreen waits until all the conflicting directions have been changed to Red and then sets the light in the adir direction to Green.
The first stage is still abstract and would be very unsafe, if implemented literally according to the model, as it is not safe to change lights instantaneously from Green to Red. This refinement introduces Amber into the lights sequence and the following slave events:

- **ToAmber** changes, in arbitrary sequence, all the currently Green lights in conflicting directions to Amber;
- **ToRed**: changes the Amber lights to Red;
- **Delay**: models a delay between Amber and Red and between Red and the final setting of the light in the adir direction to Green.

The refinement of ToGreen waits until all the conflicting directions have been changed to Red and then sets the light in the adir direction to Green.
The first stage is still abstract and would be very unsafe, if implemented literally according to the model, as it is not safe to change lights instantaneously from Green to Red. This refinement introduces Amber into the lights sequence and the following slave events:

- **ToAmber**: changes, in arbitrary sequence, all the currently Green lights in conflicting directions to Amber;
- **ToRed**: changes the Amber lights to Red;
- **Delay**: models a delay between Amber and Red and between Red and the final setting of the light in the adir direction to Green.

The refinement of ToGreen waits until all the conflicting directions have been changed to Red and then sets the light in the adir direction to Green.
A General Multi-Way Intersection

ChangeLight1R refinement 1

MACHINE ChangeLight1R
REFINES ChangeLight1
SEES TrafficLights1_ctx

VARIABLES

xlights
Extended lights, Red, Green and Amber lights
delay
delay between Amber and Red, and between Red and Green
INVARIANTS

inv1: \( xlights \in DIRECTION \rightarrow LIGHTS \)

inv2: 
\[
\forall d \cdot d \in DIRECTION \land xlights[{\{ d \}]} \subseteq \{ \text{Green, Amber} \} \\
\Rightarrow \\
xlights[\text{CONFLICT}[\{ d \}]] \subseteq \{ \text{Red} \}
\]

inv3: 
\[
xlights \triangleq (\text{CONFLICT}[\{ adir \}] \times \{ \text{Red} \}) \\
= \\
lights \triangleq (\text{CONFLICT}[\{ adir \}] \times \{ \text{Red} \})
\]

inv4: \( xlights(adir) = \text{Green} \Rightarrow lights = xlights \)

inv5: \( delay \subseteq DIRECTION \)
A General Multi-Way Intersection

ChangeLight1R refinement III

**thm1:** \( \text{finite}(x\text{lights}) \)

**thm2:**
\[ \text{CONFLICT}\left[\{\text{adir}\}\right] \triangleleft \text{lights} = \text{CONFLICT}\left[\{\text{adir}\}\right] \triangleleft x\text{lights} \]

**thm3:**
\[
\forall d, b, a \cdot d \in \text{DIRECTION} \\
\land b \in \text{LIGHTS} \land a \in \text{LIGHTS} \land a \neq b \land x\text{lights}(d) = b \\
\Rightarrow \\
\text{card}\left(\left(x\text{lights} \triangleleft \{d \mapsto a\}\right) \triangleright \{b\}\right) \\
= \\
\text{card}\left(x\text{lights} \triangleright \{b\}\right) - 1
\]

changing light in direction \(d\) from \(b\) (= before) to \(a\) (= after) decreases number of colour \(b\) lights by 1
ChangeLight1R refinement IV

\textit{thm4:}

\[ \forall d, b, a \cdot d \in \text{DIRECTION} \]
\[ \land b \in \text{LIGHTS} \land a \in \text{LIGHTS} \land a \neq b \land xlights(d) = b \]
\[ \Rightarrow \]
\[ \text{card}(\{d \mapsto a\} \triangleright \{a\}) \]
\[ = \]
\[ \text{card}(xlights \triangleright \{a\}) + 1 \]

changing light in direction $d$ from $b$ (= before) to $a$ (=after) increases number of colour $a$ lights by 1
ChangeLight1R refinement V

\textbf{thm5:} \quad \forall d, b, a, c \cdot d \in DIRECTION \\
\land b \in LIGHTS \land a \in LIGHTS \land c \in LIGHTS \\
\land xlights(d) = b \land c \neq a \land c \neq b \\
\Rightarrow \\
\text{card}((xlights \leftrightarrow \{d \mapsto a\}) \triangleright \{c\}) \\
= \\
\text{card}(xlights \triangleright \{c\}) \\
\text{changing light in direction d from b (= before) to a (=after) does not change number of colour c, c /= a, c /= b}
EVENTS
Initialisation
begin
with

lights': \( lights' = xlights' \)

\textbf{act1}: \( xlights : | \)
\( xlights' \in DIRECTION \rightarrow \{ Red, Green \} \)
\( \land (\forall d \cdot d \in DIRECTION \land xlights'(d) = Green \Rightarrow xlights'[CONFLICT[{d}]] \subseteq \{ Red \}) \)

\textbf{act2}: \( delay := \emptyset \)

end
Event $ToGreen \equiv$
refines $ToGreen$

when

$grd1$: $xlights(adir) = \text{Red}$
$grd2$: $xlights[\text{CONFLICT}\{\{adir\}\}] \subseteq \{\text{Red}\}$
$grd3$: $delay = \emptyset$

then

$act1$: $xlights := xlights \leftrightarrow \{adir \mapsto \text{Green}\}$

end
ChangeLight1R refinement VIII

Event  $\text{GreenToAmber} \triangleq$

Status  convergent

any  $\text{dir}$

when

$grd1$:  $\text{dir} \in \text{CONFLICT} [\{\text{adir}\}]$

$grd2$:  $\text{xlights} (\text{dir}) = \text{Green}$

$grd3$:  $\text{xlights} (\text{adir}) \neq \text{Green}$

$grd4$:  $\text{adir} \notin \text{delay}$

then

$act1$:  $\text{xlights} (\text{dir}) := \text{Amber}$

$act2$:  $\text{delay} := \text{delay} \cup \{\text{dir}\}$

end
A General Multi-Way Intersection

ChangeLight1R refinement IX

Event  \( \text{AmberToRed} \)

Status  convergent

any  \( \text{dir} \)

when

\( \text{grd1: } \text{dir} \in \text{CONFLICT}[^{\{\text{adir}\}}] \)
\( \text{grd2: } \text{xlights}(\text{dir}) = \text{Amber} \)
\( \text{grd3: } \text{dir} \notin \text{delay} \)
\( \text{grd4: } \text{xlights}(\text{adir}) \neq \text{Green} \)

then

\( \text{act1: } \text{xlights}(\text{dir}) := \text{Red} \)
\( \text{act2: } \text{delay} := \text{delay} \cup \{\text{dir}\} \)

end
Event  \( Delay \triangleq \)

Status  convergent

any  \( dir \)

when

\( grd1: \)  \( dir \in delay \)

then

\( act1: \)  \( delay := delay \setminus \{dir\} \)

end
ChangeLight1R refinement XI

VARIANT

$4 \times \text{card}(xlights \uparrow \{\text{Green}\}) + 2 \times \text{card}(xlights \uparrow \{\text{Amber}\}) + \text{card}(\text{delay})$

END
The events *GreenToAmber*, *AmberToRed* and *Delay* are slave events; that is they are not the main event, which is *ToGreen*. Consequently they must not be able to be enabled forever; that is they must be convergent.

In EventB this is verified by providing a variant expression: an expression that has a lower bound and must strictly decrease everytime a convergent event fires.

In this model the variant is an expression that yields a natural number —hence lower bound 0— that strictly decreases.
The events *GreenToAmber*, *AmberToRed* and *Delay* are *slave* events; that is they are not the main event, which is *ToGreen*. Consequently they must not be able to be enabled forever; that is they must be *convergent*.

In EventB this is verified by providing a *variant* expression: an expression that has a lower bound and must strictly decrease everytime a convergent event fires.

In this model the variant is an expression that yields a natural number —hence lower bound 0— that strictly decreases.
The events *GreenToAmber*, *AmberToRed* and *Delay* are slave events; that is they are not the main event, which is *ToGreen*.

Consequently they must not be able to be enabled forever; that is they must be **convergent**.

In EventB this is verified by providing a **variant** expression: an expression that has a lower bound and must strictly decrease everytime a convergent event fires.

In this model the variant is an expression that yields a natural number —hence lower bound 0— that strictly decreases.
The events *GreenToAmber*, *AmberToRed* and *Delay* are slave events; that is they are not the main event, which is *ToGreen*. Consequently they must not be able to be enabled forever; that is they must be convergent.

In EventB this is verified by providing a variant expression: an expression that has a lower bound and must strictly decrease everytime a convergent event fires.

In this model the variant is an expression that yields a natural number —hence lower bound 0— that strictly decreases.
The Variant

The variant is a sum of the following:

- 4 times the number of Red lights;
- 2 times the number of Amber lights;
- 1 times the number of current delays

This is derived from the *GreenToAmber* event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the *AmberToRed* event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
The variant is a sum of the following:

4 times the number of Red lights;
2 times the number of Amber lights;
1 times the number of current delays

This is derived from the GreenToAmber event that
• decreases the number of Red lights by 1;
• increases the number of Amber lights by 1;
• increases the number of delays by 1.

and the AmberToRed event that
• decreases the number of Amber lights by 1;
• increases the number of delays by 1.
The Variant

The variant is a sum of the following:

4 times the number of Red lights;
2 times the number of Amber lights;
1 times the number of current delays

This is derived from the GreenToAmber event that

• decreases the number of Red lights by 1;
• increases the number of Amber lights by 1;
• increases the number of delays by 1.

and the AmberToRed event that

• decreases the number of Amber lights by 1;
• increases the number of delays by 1.
The Variant

The variant is a sum of the following:

- **4 times** the number of **Red** lights;
- **2 times** the number of **Amber** lights;
- **1 times** the number of current delays

This is derived from the *GreenToAmber* event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the *AmberToRed* event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
The Variant

The variant is a sum of the following:

- 4 times the number of Red lights;
- 2 times the number of Amber lights;
- 1 times the number of current delays

This is derived from the *GreenToAmber* event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the *AmberToRed* event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
The Variant

The variant is a sum of the following:

- 4 times the number of Red lights;
- 2 times the number of Amber lights;
- 1 times the number of current delays

This is derived from the GreenToAmber event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the AmberToRed event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
The Variant

The variant is a sum of the following:

4 times the number of Red lights;
2 times the number of Amber lights;
1 times the number of current delays

This is derived from the GreenToAmber event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the AmberToRed event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
The Variant

The variant is a sum of the following:

- 4 times the number of Red lights;
- 2 times the number of Amber lights;
- 1 times the number of current delays

This is derived from the *GreenToAmber* event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the *AmberToRed* event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
The Variant

The variant is a sum of the following:

- 4 times the number of Red lights;
- 2 times the number of Amber lights;
- 1 times the number of current delays

This is derived from the *GreenToAmber* event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the *AmberToRed* event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
The Variant

The variant is a sum of the following:

4 times the number of Red lights;
2 times the number of Amber lights;
1 times the number of current delays

This is derived from the GreenToAmber event that

• decreases the number of Red lights by 1;
• increases the number of Amber lights by 1;
• increases the number of delays by 1.

and the AmberToRed event that

• decreases the number of Amber lights by 1;
• increases the number of delays by 1.
The Variant

The variant is a sum of the following:

- 4 times the number of Red lights;
- 2 times the number of Amber lights;
- 1 times the number of current delays

This is derived from the *GreenToAmber* event that

- decreases the number of Red lights by 1;
- increases the number of Amber lights by 1;
- increases the number of delays by 1.

and the *AmberToRed* event that

- decreases the number of Amber lights by 1;
- increases the number of delays by 1.
A general multi-way intersection parametric controller
A General Multi-Way Intersection Parametric Controller
Extending the model

In this development a parameterised version of the preceding traffic light control system is presented. The difference will start to be apparent when you look at the new context in which you will notice that the constant $adir$ is missing.

When you look at the new ChangeLight machine you will notice a few differences. First, there are some new events, or rather one renamed event $ToGreen$, which renames $ChangeLight$, and a new event $ToRed$ that changes a green light to red. Notice that both of these events have parameters, so the new $ToGreen$ and $ToRed$ events are now genuinely parameterised and don’t depend on a single constant value.
Extending the model

In this development a parameterised version of the preceding traffic light control system is presented. The difference will start to be apparent when you look at the new context in which you will notice that the constant $adir$ is missing.

When you look at the new ChangeLight machine you will notice a few differences. First, there are some new events, or rather one renamed event $\text{ToGreen}$, which renames $\text{ChangeLight}$, and a new event $\text{ToRed}$ that changes a green light to red. Notice that both of these events have parameters, so the new $\text{ToGreen}$ and $\text{ToRed}$ events are now genuinely parameterised and don’t depend on a single constant value.
The change to parameterisation has virtually no effect on the ChangeLight machine but has significant affects on the refinement. The refinement now has a variable, \textit{rdir}, which is used to the parameter for both the ToGreen and ToRed events. Also notice that there are two new variables \textit{togreen} and \textit{tored}. The invariant reveals that both of these variables are of type \textit{BOOL}. The purpose of these two variables is will be explained a little later.

Both BOOL variables are initialised to FALSE. Notice that different names have been chosen for the events in the refinement to reduce confusion now that we are refining two abstract operations.

Again, notice that the refinement of the ToGreen event fires only when the conflicting directions have been set to Red, but also notice that this event will only fire if the BOOL variable togreen is TRUE.
The change to parameterisation has virtually no effect on the ChangeLight machine but has significant affects on the refinement. The refinement now has a variable, \( rdir \), which is used to the parameter for both the ToGreen and ToRed events. Also notice that there are two new variables \( togreen \) and \( tored \). The invariant reveals that both of these variables are of type \( BOOL \). The purpose of these two variables is will be explained a little later.

Both \( BOOL \) variables are initialised to FALSE. Notice that different names have been chosen for the events in the refinement to reduce confusion now that we are refining two abstract operations.

Again, notice that the refinement of the ToGreen event fires only when the conflicting directions have been set to Red, but also notice that this event will only fire if the \( BOOL \) variable \( togreen \) is TRUE.
The change to parameterisation has virtually no effect on the ChangeLight machine but has significant affects on the refinement. The refinement now has a variable, $rdir$, which is used to the parameter for both the ToGreen and ToRed events. Also notice that there are two new variables $togreen$ and $tored$. The invariant reveals that both of these variables are of type $BOOL$. The purpose of these two variables is will be explained a little later.

Both $BOOL$ variables are initialised to FALSE. Notice that different names have been chosen for the events in the refinement to reduce confusion now that we are refining two abstract operations.

Again, notice that the refinement of the ToGreen event fires only when the conflicting directions have been set to Red, but also notice that this event will only fire if the $BOOL$ variable $togreen$ is TRUE.
A new event **ToGreenInit** appears. The purpose of this event is to initialise the state for the sequence of events that effectively refine the ToGreen event. **ToGreenInit** can only fire when the BOOL variables `togreen` and `tored` are both FALSE.

New events **GreenToAmber** and **AmberToRed** produce transitions of the Green conflicting lights through to Red. Each of these events can only fire when `togreen` is TRUE. Notice a similar initialisation event **ToRedInit** for the refinement of the ToRed event.

The BOOL variables are required because we are refining two atomic events **ToGreen** and **ToRed** and the refinement involves a sequence of events. We need to prevent interference and preserve the atomicity of the **ToGreen** and **ToRed** events. The BOOL variables ensure that the complete sequence of events making up a refinement are completed before any other event can be triggered. This problem did not arise in the previous development because the **ToGreen** event had a fixed parameter and there was no possibility for interference.
A new event $\text{ToGreenInit}$ appears. The purpose of this event is to initialise the state for the sequence of events that effectively refine the ToGreen event. $\text{ToGreenInit}$ can only fire when the BOOL variables $\text{togreen}$ and $\text{tored}$ are both FALSE.

New events $\text{GreenToAmber}$ and $\text{AmberToRed}$ produce transitions of the $\text{Green}$ conflicting lights through to $\text{Red}$. Each of these events can only fire when $\text{togreen}$ is TRUE. Notice a similar initialisation event $\text{ToRedInit}$ for the refinement of the $\text{ToRed}$ event.

The BOOL variables are required because we are refining two atomic events $\text{ToGreen}$ and $\text{ToRed}$ and the refinement involves a sequence of events. We need to prevent interference and preserve the atomicity of the $\text{ToGreen}$ and $\text{ToRed}$ events. The BOOL variables ensure that the complete sequence of events making up a refinement are completed before any other event can be triggered. This problem did not arise in the previous development because the $\text{ToGreen}$ event had a fixed parameter and there was no possibility for interference.
A new event **ToGreenInit** appears. The purpose of this event is to initialise the state for the sequence of events that effectively refine the ToGreen event. **ToGreenInit** can only fire when theBOOL variables *togreen* and *tored* are both FALSE.

New events **GreenToAmber** and **AmberToRed** produce transitions of the *Green* conflicting lights through to *Red*. Each of these events can only fire when *togreen* is TRUE. Notice a similar initialisation event **ToRedInit** for the refinement of the **ToRed** event.

The BOOL variables are required because we are refining two atomic events **ToGreen** and **ToRed** and the refinement involves a sequence of events. We need to prevent interference and preserve the atomicity of the **ToGreen** and **ToRed** events. The BOOL variables ensure that the complete sequence of events making up a refinement are completed before any other event can be triggered. This problem did not arise in the previous development because the **ToGreen** event had a fixed parameter and there was no possibility for interference.
TrafficLights2_ctx context 1

CONTEXT TrafficLights2_ctx

SETS

LIGHTS
DIRECTION
TrafficLights2_ctx context II

CONSTANTS

Red
Green
Amber
CONFLICT
A General Multi-Way Intersection Parametric Controller

TrafficLights2_ctx context III

AXIOMS

axm1: \( \text{partition}(\text{LIGHTS}, \{\text{Red}\}, \{\text{Green}\}, \{\text{Amber}\}) \)

axm2: \( \text{finite}(\text{DIRECTION}) \)  
DIRECTION is a finite set of directions

axm3: \( \text{CONFLICT} \in \text{DIRECTION} \leftrightarrow \text{DIRECTION} \)  
CONFLICT relates conflicting directions

axm4: \( \text{CONFLICT} \cap (\text{DIRECTION} \setminus \text{id}) = \emptyset \)  
a direction cannot conflict with itself

axm5: \( \text{CONFLICT}^{-1} = \text{CONFLICT} \)  
conflicts are symmetric

thm1: \( \forall d \cdot d \in \text{DIRECTION} \Rightarrow d \not\in \text{CONFLICT}[[d]] \)

thm2: \( \forall d_1, d_2 \cdot d_1 \not\in \text{CONFLICT}[[d_2]] \Rightarrow d_2 \not\in \text{CONFLICT}[[d_1]] \)

END
MACHINE ChangeLight2
SEES TrafficLights2_ctx

VARIABLES

\textit{lights}

INvariants

\textit{inv1}: \quad \text{\it lights} \in DIRECTION \rightarrow \{\textit{Red}, \textit{Green}\}

\textit{inv2}: \quad \forall d. \quad d \in DIRECTION \land \text{\it lights}(d) = \textit{Green} \Rightarrow \text{\it lights}[\textit{CONFLICT}[[d]]] \subseteq \{\textit{Red}\}

\textit{thm1}: \quad \text{finite(\textit{lights})}
EVENTS
Initialisation
begin
act1: \( \text{lights} : \{ \text{lights}' \in \text{DIRECTION} \rightarrow \{ \text{Red}, \text{Green} \} \wedge (\forall d \cdot d \in \text{DIRECTION} \wedge \text{lights}'(d) = \text{Green} \Rightarrow \text{lights}'[\text{CONFLICT}[^{\{d\}}]] \subseteq \{ \text{Red} \}) \) 
end
ChangeLight2 machine III

Event \( \text{ToGreen} \doteq \)
- \( \text{any adir} \)

when

\( \text{grd1: lights(adir) = Red} \)

then

\( \text{act1: lights := lights} \)
\( \leftarrow (\text{CONFLICT}\{\text{adir}\} \times \{\text{Red}\}) \)
\( \leftarrow \{\text{adir} \leftrightarrow \text{Green}\} \)

end
ChangeLight2 machine IV

Event $ToRed \equiv$

any $adir$

when

grd1: $lights(adir) = Green$

then

act1: $lights(adir) := Red$

end

END
A General Multi-Way Intersection Parametric Controller

**ChangeLight2R refinement I**

MACHINE ChangeLight2R
REFINES ChangeLight2
SEES TrafficLights2_ctx
VARIABLES

- \( xlights \)  
  Extended lights, Red, Green and Amber lights
- \( delay \)  
  delay between Amber and Red, Red and Green
- \( rdir \)  
  current argument of ToGreen or ToRed
- \( togreen \)
- \( tored \)
IN VariantS

inv1: $xlights \in DIRECTION \rightarrow LIGHTS$

inv2:

$\forall d \cdot d \in DIRECTION \land xlights[\{d\}] \subseteq \{\text{Green, Amber}\}$

$\Rightarrow$

$xlights[\text{CONFLICT}[\{d\}]] \subseteq \{\text{Red}\}$

inv3: $\text{togreen} = \text{FALSE} \land \text{tored} = \text{FALSE}$

$\Rightarrow$

$\text{lights} = xlights$

inv4: $\text{rdir} \in DIRECTION$

inv5: $\text{delay} \subseteq DIRECTION$

inv6: $\text{togreen} \in BOOL$

inv7: $\text{tored} \in BOOL$
ChangeLight2R refinement III

\[\text{inv8: } \text{togreen} = \text{TRUE} \Rightarrow \text{tored} = \text{FALSE}\]

\[\text{inv9: } \text{togreen} = \text{TRUE} \Rightarrow \text{lights}(rdir) = \text{Red}\]

\[\text{inv10: } \]

\[\text{togreen} = \text{TRUE} \Rightarrow \]

\[\text{xlights} \leftrightarrow (\text{CONFLICT}\{rdir\} \times \{\text{Red}\}) \leftrightarrow \{rdir \mapsto \text{Green}\} = \]

\[\text{lights} \leftrightarrow (\text{CONFLICT}\{rdir\} \times \{\text{Red}\}) \leftrightarrow \{rdir \mapsto \text{Green}\}\]

\[\text{thm1: } \text{togreen} = \text{TRUE} \]

\[\Rightarrow \]

\[\text{CONFLICT}\{rdir\} \leftrightarrow (\{rdir\} \leftrightarrow \text{xlights}) = \]

\[\text{CONFLICT}\{rdir\} \leftrightarrow (\{rdir\} \leftrightarrow \text{lights})\]
ChangeLight2R refinement IV

*inv11*: \( tored = \text{TRUE} \Rightarrow \text{lights}(rdir) = \text{Green} \)

*inv12*: \( tored = \text{TRUE} \Rightarrow \text{xlights} \Leftarrow \{ rdir \mapsto \text{Red} \} = \text{lights} \Leftarrow \{ rdir \mapsto \text{Red} \} \)

*thm2*: \( tored = \text{TRUE} \Rightarrow \{ rdir \} \Leftarrow \text{lights} = \{ rdir \} \Leftarrow \text{xlights} \)
A General Multi-Way Intersection Parametric Controller

**ChangeLight2R refinement V**

**thm3:** \( \text{finite}(xlights) \)

**thm4:** \( \forall d, b, a \cdot a \in LIGHTS \land a \neq b \land xlights(d) = b \Rightarrow \text{card}((xlights \leftarrow \{d \mapsto a\}) \triangleright \{b\}) = \text{card}(xlights \triangleright \{b\}) - 1 \)

changing light in direction \( d \) from \( b \) (= before) to \( a \) (= after) decreases number of colour \( b \) lights by 1

**thm5:** \( \forall d, b, a \cdot a \in LIGHTS \land a \neq b \land xlights(d) = b \Rightarrow \text{card}((xlights \leftarrow \{d \mapsto a\}) \triangleright \{a\}) = \text{card}(xlights \triangleright \{a\}) + 1 \)

changing light in direction \( d \) from \( b \) (= before) to \( a \) (= after) increases number of colour \( a \) lights by 1
ChangeLight2R refinement VI

\[\text{thm6: } \forall d, b, a, c \cdot a \in \text{LIGHTS} \land c \in \text{LIGHTS} \land c \neq a \land c \neq b \land \text{xlights}(d) = b \Rightarrow \text{card}((\text{xlights} \leftrightarrow \{d \mapsto a\}) \triangleright \{c\}) = \text{card}((\text{xlights} \triangleright \{c\}) \]

changing light in direction \(d\) from \(b\) (= before) to \(a\) (=after) does not change number of colour \(c\), \(c \neq a\), \(c \neq b\)
EVENTS
Initialisation
begin
with

\textit{lights'}: \textit{lights'} = x\textit{lights'}

\textit{act1}: \quad x\textit{lights'} : |x\textit{lights'} \in \textit{DIRECTION} \rightarrow \{\textit{Red}, \textit{Green}\}
\land (\forall d \cdot x\textit{lights'}(d) = \textit{Green})
\Rightarrow
\quad x\textit{lights'}[\textit{CONFLICT}[\{d\}]] \subseteq \{\textit{Red}\})

\textit{act2}: \quad \textit{delay} := \emptyset

\textit{act3}: \quad \textit{togreen}, \textit{tored} := \text{\textit{FALSE}}, \text{\textit{FALSE}}

\textit{act5}: \quad \textit{rdir} \in \textit{DIRECTION}

end
Event $ToGreen \sqsupseteq$
refines $ToGreen$

when

$grd1$: $\text{togreen} = \text{TRUE}$

$grd2$: $xlights[\text{CONFLICT}[\{\text{rdir}\}]] \subseteq \{\text{Red}\}$

$grd3$: $\text{rdir} \notin \text{delay}$

with

$adir$: $adir = rdir$

then

$act1$: $xlights(\text{rdir}) := \text{Green}$

$act2$: $\text{togreen} := \text{FALSE}$

end
A General Multi-Way Intersection Parametric Controller

ChangeLight2R refinement IX

Event \( \text{ToGreenInit} \triangleq \)

any

\( \text{adir} \)

when

\( \text{grd1:} \quad \text{togreen} = \text{FALSE} \)

\( \text{grd2:} \quad \text{tored} = \text{FALSE} \)

\( \text{grd3:} \quad \text{xlights}(\text{adir}) = \text{Red} \)

then

\( \text{act1:} \quad \text{rdir} := \text{adir} \)

\( \text{act2:} \quad \text{togreen} := \text{TRUE} \)

end
Event \( \text{GreenToAmber} \supseteq \)

Status convergent

any

\( \text{dir} \)

when

\( \text{grd1:} \quad \text{togreen} = \text{TRUE} \)

\( \text{grd2:} \quad \text{dir} \in \text{CONFLICT} [\{\text{rdir}\}] \)

\( \text{grd3:} \quad xlights(\text{dir}) = \text{Green} \)

\( \text{grd4:} \quad \text{dir} \notin \text{delay} \)

then

\( \text{act1:} \quad xlights(\text{dir}) := \text{Amber} \)

\( \text{act2:} \quad \text{delay} := \text{delay} \cup \{\text{dir}\} \)

end
ChangeLight2R refinement XI

Event $AmberToRed \supseteq$

Status convergent
  any
  $dir$
when
  $grd1$: $\text{togreen} = \text{TRUE}$
  $grd2$: $dir \in \text{CONFLICT}[\{rdir\}]$
  $grd3$: $xlights(dir) = \text{Amber}$
  $grd4$: $dir \notin \text{delay}$
then
  $act1$: $xlights(dir) := \text{Red}$
  $act2$: $\text{delay} := \text{delay} \cup \{rdir\}$
end
Event \( \text{Delay} \cong \)

Status convergent

any

\( \text{dir} \)

when

\( \text{grd1: dir} \in \text{delay} \)

then

\( \text{act1: delay} := \text{delay} \setminus \{ \text{dir} \} \)

end
ChangeLight2R refinement XIII

Event $ToRed \supseteq$
refines $ToRed$

when

$grd1$: $tored = \text{TRUE}$
$grd2$: $xlights(rdir) = \text{Amber}$
$grd3$: $rdir \notin \text{delay}$

with

$adir$: $adir = rdir$

then

$act1$: $xlights(rdir) := \text{Red}$
$act2$: $tored := \text{FALSE}$

end
ChangeLight2R refinement XIV

Event \( ToRedInit \triangleq \)

\( \text{any} \)

\( adir \)

when

\( \text{grd1: } xlights(adir) = \text{Green} \)

\( \text{grd2: } tored = \text{FALSE} \)

\( \text{grd3: } togreen = \text{FALSE} \)

then

\( \text{act1: } \text{rdir } := \text{adir} \)

\( \text{act2: } \text{tored } := \text{TRUE} \)

end
Event $ToAmber \equiv$

when

$grd1$: $tored = TRUE$
$grd2$: $xlights(rdir) = Green$
$grd3$: $rdir \notin delay$

then

$act1$: $xlights(rdir) := Amber$
$act2$: $delay := delay \cup \{rdir\}$

end
ChangeLight2R refinement XVI

VARIANT

$4 \times \text{card}(\text{xlights} \triangleright \{ \text{Green} \})$
$+ 2 \times \text{card}(\text{xlights} \triangleright \{ \text{Amber} \})$
$+ \text{card}(\text{delay})$

END