1 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

2 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.

3 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.

CONTEXT TrafficLights_ctx
SETS LIGHTS DIRECTION
CONSTANTS Red Green Amber NorthSouth EastWest OTHERDIR
AXIOMS
axm1: LIGHTS = {Red, Green, Amber}
axm2: Red ≠ Green
axm3: Red ≠ Amber
axm4: Green ≠ Amber
axm5: DIRECTION = {NorthSouth, EastWest}
axm6: NorthSouth ≠ EastWest
axm7: OTHERDIR ∈ DIRECTION → DIRECTION
axm8: OTHERDIR(NorthSouth) = EastWest
axm9: OTHERDIR(EastWest) = NorthSouth

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

\textbf{END}

The above can be expressed more simply as

\textbf{AXIOMS}

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

\textbf{axiom:} \( \text{partition}(\text{DIRECTION}, \{\text{NorthSouth}\}, \{\text{EastWest}\}) \)

\textbf{The Simple TwoWay Machine}

The \textbf{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 \textit{ChangeLight} to change the lights;
3. ensures that lights change in the sequence \textit{Red}, \textit{Green}, \textit{Amber}, \ldots;
4. maintains a safe intersection;

\section{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}.
   \[ \neg(\text{safe}) \implies \neg(\text{invariant}) \quad (1) \]
3. Conversely, whenever the invariant is \textit{true}, the state should be safe.
   \[ \text{invariant} \implies \text{safe} \quad (2) \]
4. Of course, \([1]\text{ and }[2]\) 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.
4.1 A Safe state

The state invariant should be:

1. \textit{false for all unsafe states} \hspace{0.5cm} \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

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

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.

4.2 Strengthening the Invariant

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

\begin{center}
\begin{tabular}{ccc}
Red & Green & Amber \\
Red & safe & safe \\
Green & safe & unsafe \\
Amber & safe & unsafe \\
\end{tabular}
\end{center}

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)

4.3 Other Invariants

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

\[ \text{lights}(\text{NorthSouth}) = \text{Red} \lor \text{lights}(\text{EastWest}) = \text{Red} \]
But these conditions do not generalise to intersections with more than two ways. Indeed the expression of the invariant that best generalises is

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

(4)

### 4.4 Some Theorems

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

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

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

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.

### 5 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

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

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

Safety can be ensured with the guard:

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

5.1 Sequencing

Changing to

**Red**: the current colour should be Amber, so light = Red $$\implies$$ lights(dir) = Amber

**Green**: the current colour should be Red, so light = Green $$\implies$$ lights(dir) = Red

**Amber**: the current colour should be Green, so light = Amber $$\implies$$ lights(dir) = 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.
Final Guards for ChangeLight

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

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

The ChangeLight Event

**MACHINE** ChangeLights

**SEES** TrafficLights_ctx

**VARIABLES** lights

**ININVARIANTS**

\(\text{inv1: } \text{lights} \in \text{DIRECTION} \to \text{LIGHTS}\)

\(\text{inv2: } \text{lights}(\text{NorthSouth}) \in \{\text{Green}, \text{Amber}\} \implies \text{lights}(\text{EastWest}) = \text{Red}\)

**EVENTS**

**Initialisation**

\begin{align*}
\text{begin} \\
\text{act1: } \text{lights} := \{\text{NorthSouth} \mapsto \text{Red}, \text{EastWest} \mapsto \text{Red}\} \\
\text{end}
\end{align*}

**Event** ToAmber

\begin{align*}
\text{any } \text{dir} \\
\text{when} \\
\text{grd1: } \text{dir} \in \text{DIRECTION} \\
\text{grd2: } \text{lights(dir)} = \text{Green} \\
\text{then} \\
\text{act1: } \text{lights(dir)} := \text{Amber} \\
\text{end}
\end{align*}

**Event** ToGreen

\begin{align*}
\text{any } \text{dir} \\
\text{when} \\
\text{grd1: } \text{dir} \in \text{DIRECTION}
\end{align*}
grd2: \( \text{lights(OTHERDIR(dir))} = \text{Red} \)

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

then

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

end

Event \( \text{ToRed} \equiv \)

any dir

when

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

grd2: \( \text{lights(dir)} = \text{Amber} \)

then

act1: \( \text{lights(dir)} := \text{Red} \)

end

END

6 A General Multi-Way Intersection

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

- No direction conflicts with itself.
- Conflicts are symmetric: if \( \text{dir}_1 \) conflicts with \( \text{dir}_2 \) then \( \text{dir}_2 \) conflicts with \( \text{dir}_1 \).

6.1 The New Safety Invariant

The safety invariant for our generalised intersection is

\[
\forall d \in \text{DIRECTION} \land \text{lights}(d) \in \{\text{Green, Amber}\} \implies \\
\text{lights}(\text{CONFLICT}[[d]]) = \{\text{Red}\}
\]

This can be seen as a generalisation of the earlier safety invariant [4].
TrafficLights1_ctx

CONTEXT TrafficLights1_ctx

SETS LIGHTS DIRECTION

CONSTANTS Red Green Amber CONFLICT adir

AXIOMS

avm1: partition(LIGHTS, {Red}, {Green}, {Amber})  Three light colours
avm2: finite(DIRECTION)  DIRECTION is a finite set of directions
avm3: CONFLICT ∈ DIRECTION ↔ DIRECTION  CONFLICT relates conflicting directions
avm4: CONFLICT ∩ (DIRECTION ∪ id) = ∅  a direction cannot conflict with itself
avm5: CONFLICT⁻¹ = CONFLICT  conflicts are symmetric

thm1: ∀d·d ∈ DIRECTION ⇒ d ∉ CONFLICT[{d}]

thm2: ∀d1,d2·d1 ∉ CONFLICT[{d2}] ⇒ d2 ∉ CONFLICT[{d1}]

avm6: adir ∈ DIRECTION  any direction (used as a parameter)

END

6.2 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

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.
ChangeLight1 machine

MACHINE ChangeLight1

SEES TrafficLights1_ctx

VARIABLES lights

INVARIANTS

inv1: \( \text{lights} \in \text{DIRECTION} \rightarrow \{\text{Red}, \text{Green}\} \)

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

EVENTS

Initialisation

begin

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

end

Event ToGreen ≡

when

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

then

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

end

END

The Refinement Model

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 \textit{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 \textit{adir} direction to Green.

\textbf{ChangeLight1R refinement}

\textbf{MACHINE} ChangeLight1R

\textbf{REFINES} ChangeLight1

\textbf{SEES} TrafficLights1\_ctx

\textbf{VARIABLES} \textit{xlights} \quad \text{Extended lights, Red, Green and Amber lights} \quad \textit{delay} \quad \text{delay between Amber and Red, and between Red and Green}

\textbf{INVARIANTS}

\textit{inv1:} \quad \textit{xlights} \in \textit{DIRECTION} \rightarrow \textit{LIGHTS}

\textit{inv2:} \quad \forall \textit{d-d} \in \textit{DIRECTION} \land \textit{xlights}\{\textit{d}\} \subseteq \{\textit{Green, Amber}\} \Rightarrow \textit{xlights}\{\textit{CONFLICT}\{\textit{d}\}\} \subseteq \{\textit{Red}\}

\textit{inv3:} \quad \textit{xlights} \not\in (\textit{CONFLICT}\{\textit{adir}\} \times \{\textit{Red}\}) \Rightarrow \\
\textit{lights} \not\in (\textit{CONFLICT}\{\textit{adir}\} \times \{\textit{Red}\})

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

\textit{inv5:} \quad \textit{delay} \subseteq \textit{DIRECTION}

\textbf{thm1:} \quad \text{finite}(\textit{xlights})

\textbf{thm2:} \quad \textit{CONFLICT}\{\textit{adir}\} \not\in \textit{lights} = \textit{CONFLICT}\{\textit{adir}\} \not\in \textit{xlights}

\textbf{thm3:} \quad \forall \textit{d,b,a-d} \in \textit{DIRECTION} \land \textit{b} \in \textit{LIGHTS} \land \textit{a} \in \textit{LIGHTS} \land \textit{a} \neq \textit{b} \land \textit{xlights}(\textit{d}) = \textit{b} \Rightarrow \\
\quad \text{card}((\textit{xlights} \not\in \{\textit{d-a}\}) \triangleright \{\textit{b}\}) = \\
\quad \text{card}(\textit{xlights} \triangleright \{\textit{b}\}) - 1

from \textit{b} (= before) to \textit{a} (= after) decreases number of colour \textit{b} lights by 1

\textbf{thm4:} \quad \forall \textit{d,b,a-d} \in \textit{DIRECTION} \land \textit{b} \in \textit{LIGHTS} \land \textit{a} \in \textit{LIGHTS} \land \textit{a} \neq \textit{b} \land \textit{xlights}(\textit{d}) = \textit{b} \Rightarrow \\
\quad \text{card}((\textit{xlights} \not\in \{\textit{d-a}\}) \triangleright \{\textit{a}\}) = \\
\quad \text{card}(\textit{xlights} \triangleright \{\textit{a}\}) + 1

from \textit{b} (= before) to \textit{a} (= after) increases number of colour \textit{a} lights by 1
thm5: \( \forall d, a, c \cdot d \in DIRECTION \wedge b \in LIGHTS \wedge a \in LIGHTS \wedge c \in LIGHTS \wedge xlights(d) = b \wedge c \neq a \wedge c \neq b \Rightarrow \)
\[ \text{card}(\{xlights(d) \leftarrow \{d \mapsto a\} \triangleright \{c\}) = \text{card}(xlights \triangleright \{c\}) \]
changing light in direction d from b to a does not change number of colour c, c \neq a, c \neq b

EVENTS

Initialisation

begin
with

lights\': lights' = xlights'

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

act2: delay := \emptyset

end

Event ToGreen \( \hat{=} \)
refines ToGreen

when

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

grd2: xlights[\text{CONFLICT}([adir])] \subseteq \{\text{Red}\}

grd3: delay = \emptyset

then

act1: xlights := xlights \leftarrow \{adir \mapsto \text{Green}\}

end

Event GreenToAmber \( \hat{=} \)

Status convergent

any dir

when

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

11
\( \text{grd2: } \text{xlights(dir) = Green} \)

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

\( \text{grd4: } \text{adir \notin delay} \)

\text{then}

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

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

\text{end}

\text{Event } \text{AmberToRed} \equiv \text{Status convergent any dir}

\text{when}

\( \text{grd1: } \text{dir } \in \text{CONFLICT}\{\text{adir}\} \)

\( \text{grd2: } \text{xlights(dir) = Amber} \)

\( \text{grd3: } \text{adir \notin delay} \)

\( \text{grd4: } \text{xlights(adir) \neq Green} \)

\text{then}

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

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

\text{end}

\text{Event } \text{Delay} \equiv \text{Status convergent any dir}

\text{when}

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

\text{then}

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

\text{end}

\text{VARIANT} \quad 4 \ast \text{card(xlights } \triangleright \{\text{Green}\})

\quad + 2 \ast \text{card(xlights } \triangleright \{\text{Amber}\})

\quad + \text{card(delay)}

\text{END}
The Variant

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.

7 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.

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, rd, 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 \textit{BOOL}. The purpose of these two variables is will be explained a little later.

Both \textit{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 \textit{BOOL} variable togreen is TRUE.

A new event \textit{ToGreenInit} appears. The purpose of this event is to initialise the state for the sequence of events that effectively refine the ToGreen event. \textit{ToGreenInit} can only fire when the \textit{BOOL} variables togreen and tored are both FALSE.

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

The \textit{BOOL} variables are required because we are refining two atomic events \textit{ToGreen} and \textit{ToRed} and the refinement involves a sequence of events. We need to prevent interference and preserve the atomicity of the \textit{ToGreen} and \textit{ToRed} events. The \textit{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 \textit{ToGreen} event had a fixed parameter and there was no possibility for interference.

\textbf{TrafficLights2\_ctx context}

\begin{verbatim}
CONTEXT TrafficLights2\_ctx

SETS LIGHTS DIRECTION

CONSTANTS Red Green Amber CONFLICT

AXIOMS

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

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

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

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

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

thm1: \forall d \in DIRECTION \Rightarrow d \notin CONFLICT[\{d\}]

thm2: \forall d1, d2 \cdot d1 \notin CONFLICT[\{d2\}] \Rightarrow d2 \notin CONFLICT[\{d1\}]

END
\end{verbatim}
ChangeLight2 machine

MACHINE  ChangeLight2
SEES     TrafficLights2_ctx
VARIABLES  lights

ININVARIANTS
inv1:  lights ∈ DIRECTION → {Red, Green}

inv2:  ∀d·d ∈ DIRECTION ∧ lights(d) = Green
        ⇒ lights[CONFLICT[{d}]] ⊆ {Red}

thm1:  finite(lights)

EVENTS

Initialisation

begin

act1:  lights : lights' ∈ DIRECTION → {Red, Green}
        ∧ (∀d·d ∈ DIRECTION ∧ lights'(d) = Green
            ⇒ lights'[CONFLICT[{d}]] ⊆ {Red})

end

Event  ToGreen ≜

any  adir

when

grd1:  lights(adir) = Red

then

act1:  lights := lights
        ↦ (CONFLICT[{adir}] × {Red})
        ↦ {adir ↦ Green}

end

Event  ToRed ≜

any  adir

when

grd1:  lights(adir) = Green

then

act1:  lights(adir) := Red

end

END
ChangeLight2R refinement

**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`

**INVARIANTS**

1. \(\text{inv1}: \text{xlights} \in \text{DIRECTION} \rightarrow \text{LIGHTS}\)
2. \(\text{inv2}: \forall d \in \text{DIRECTION}, \text{xlights}[\{d\}] \subseteq \{\text{Green, Amber}\} \Rightarrow \text{xlights[CONFLICT}\{d\}]} \subseteq \{\text{Red}\}\)
3. \(\text{inv3}: \text{togreen} = \text{FALSE} \land \text{tored} = \text{FALSE} \Rightarrow \text{lights} = \text{xlights}\)
4. \(\text{inv4}: \text{rdir} \in \text{DIRECTION}\)
5. \(\text{inv5}: \text{delay} \subseteq \text{DIRECTION}\)
6. \(\text{inv6}: \text{togreen} \in \text{BOOL}\)
7. \(\text{inv7}: \text{tored} \in \text{BOOL}\)
8. \(\text{inv8}: \text{togreen} = \text{TRUE} \Rightarrow \text{tored} = \text{FALSE}\)
9. \(\text{inv9}: \text{togreen} = \text{TRUE} \Rightarrow \text{lights(rdir)} = \text{Red}\)
10. \(\text{inv10}: \text{togreen} = \text{TRUE} \Rightarrow \text{xlights} \equiv \{\text{CONFLICT}\{\text{rdir}\}} \times \{\text{Red}\} \equiv \{\text{rdir} \mapsto \text{Green}\} = \text{lights} \equiv \{\text{CONFLICT}\{\text{rdir}\}} \times \{\text{Red}\} \equiv \{\text{rdir} \mapsto \text{Green}\}\)
11. \(\text{thm1}: \text{togreen} = \text{TRUE} \Rightarrow \text{CONFLICT}\{\text{rdir}\} \equiv \{\text{rdir} \mapsto \text{xlights}\} = \text{CONFLICT}\{\text{rdir}\} \equiv \{\text{rdir} \mapsto \text{lights}\}\)
12. \(\text{inv11}: \text{tored} = \text{TRUE} \Rightarrow \text{lights(rdir)} = \text{Green}\)
13. \(\text{inv12}: \text{tored} = \text{TRUE} \Rightarrow \text{xlights} \equiv \{\text{rdir} \mapsto \text{Red}\} = \text{lights} \equiv \{\text{rdir} \mapsto \text{Red}\}\)
thm2:  \( \text{tored} = \text{TRUE} \)
\[ \Rightarrow \]
\( \{rdir\} \ll \text{lights} \)
\[ = \]
\( \{rdir\} \ll \text{xlights} \)

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

thm4:  \( \forall d, b, a \cdot a \in \text{LIGHTS} \land a \neq b \land \text{xlights} (d) = b \Rightarrow \text{card} (\text{xlights} \ll \{d \mapsto a\} \triangleright \{b\}) = \text{card} (\text{xlights} \triangleright \{b\}) - 1 \)
(= after) decreases number of colour b lights by 1

thm5:  \( \forall d, b, a \cdot a \in \text{LIGHTS} \land a \neq b \land \text{xlights} (d) = b \Rightarrow \text{card} (\text{xlights} \ll \{d \mapsto a\} \triangleright \{a\}) = \text{card} (\text{xlights} \triangleright \{a\}) + 1 \)
(= after) increases number of colour a lights by 1

thm6:  \( \forall d, b, a, c \cdot a \in \text{LIGHTS} \land c \in \text{LIGHTS} \land c \neq a \land c \neq b \land \text{xlights} (d) = b \Rightarrow \text{card} (\text{xlights} \ll \{d \mapsto a\} \triangleright \{c\}) = \text{card} (\text{xlights} \triangleright \{c\}) \)
to a (= after) does not change number of colour c, c /= a, c /= b

EVENTS

Initialisation

begin

with

\text{lights}' : \text{lights}' = \text{xlights}'

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

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

act3:  \( \text{togreen, tored} := \text{FALSE, FALSE} \)

act5:  \( \text{rdir} \in \text{DIRECTION} \)

end

Event  \( \text{ToGreen} \)
refines ToGreen

when

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

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

\( \text{grd3: } \text{rdir} \notin \text{delay} \)

with

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

then

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

\( \text{act2: } \text{togreen} := \text{FALSE} \)

end

Event \( \text{ToGreenInit} \)

any

\( \text{adir} \)

when

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

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

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

then

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

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

end

Event \( \text{GreenToAmber} \)

Status convergent

any

\( \text{dir} \)

when

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

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

\( \text{grd3: } \text{xlights}(\text{dir}) = \text{Green} \)
grd4: \( \text{dir} \notin \text{delay} \)

then

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

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

end

Event \( \text{AmberToRed} \equiv \)

Status convergent

any

dir

when

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

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

grd3: \( xlights(\text{dir}) = \text{Amber} \)

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

then

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

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

end

Event \( \text{Delay} \equiv \)

Status convergent

any

dir

when

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

then

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

end

Event \( \text{ToRed} \equiv \)

refines \( \text{ToRed} \)

when


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

\[ \text{with} \]
\[ \text{adir} : \text{adir} = \text{rdir} \]

\[ \text{then} \]
\[ \text{act1: } \text{xlights}(\text{rdir}) := \text{Red} \]
\[ \text{act2: } \text{tored} := \text{FALSE} \]

\[ \text{end} \]

\[ \text{Event } \text{ToRedInit} \triangleq \]

\[ \text{any} \]
\[ \text{adir} \]

\[ \text{when} \]
\[ \text{grd1: } \text{xlights}(\text{adir}) = \text{Green} \]
\[ \text{grd2: } \text{tored} = \text{FALSE} \]
\[ \text{grd3: } \text{togreen} = \text{FALSE} \]

\[ \text{then} \]
\[ \text{act1: } \text{rdir} := \text{adir} \]
\[ \text{act2: } \text{tored} := \text{TRUE} \]

\[ \text{end} \]

\[ \text{Event } \text{ToAmber} \triangleq \]

\[ \text{when} \]
\[ \text{grd1: } \text{tored} = \text{TRUE} \]
\[ \text{grd2: } \text{xlights}(\text{rdir}) = \text{Green} \]
\[ \text{grd3: } \text{rdir} \notin \text{delay} \]

\[ \text{then} \]
\[ \text{act1: } \text{xlights}(\text{rdir}) := \text{Amber} \]
\[ \text{act2: } \text{delay} := \text{delay} \cup \{\text{rdir}\} \]

\[ \text{end} \]

\[ \text{VARIANT} \quad 4 \ast \text{card}(\text{xlights} \triangleright \{\text{Green}\}) \]
\[ + 2 \ast \text{card}(\text{xlights} \triangleright \{\text{Amber}\}) \]
\[ + \text{card}(\text{delay}) \]

\[ \text{END} \]