Safe Intersections:

At the Crossing of Hybrid Systems and Verification

Sarah M. Loos and André Platzer

Computer Science Department

Carnegie Mellon University

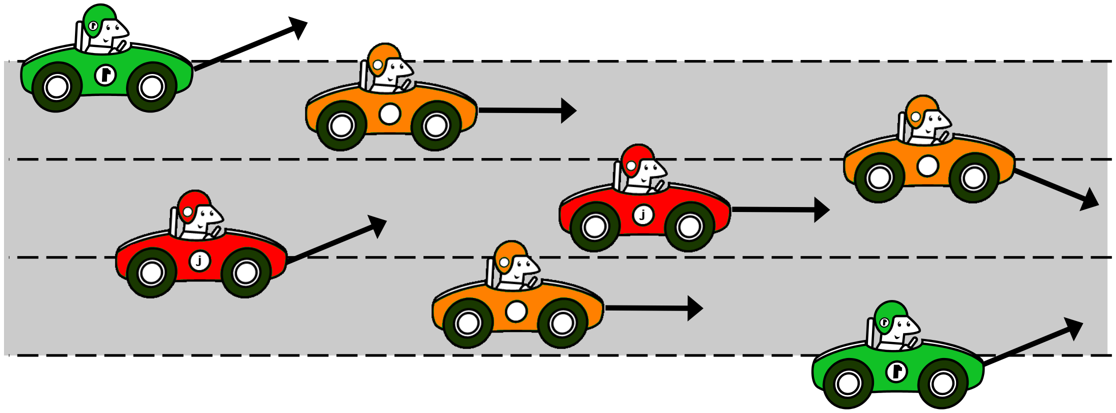
October, 2011

Ultimately...

Simplifying Assumptions

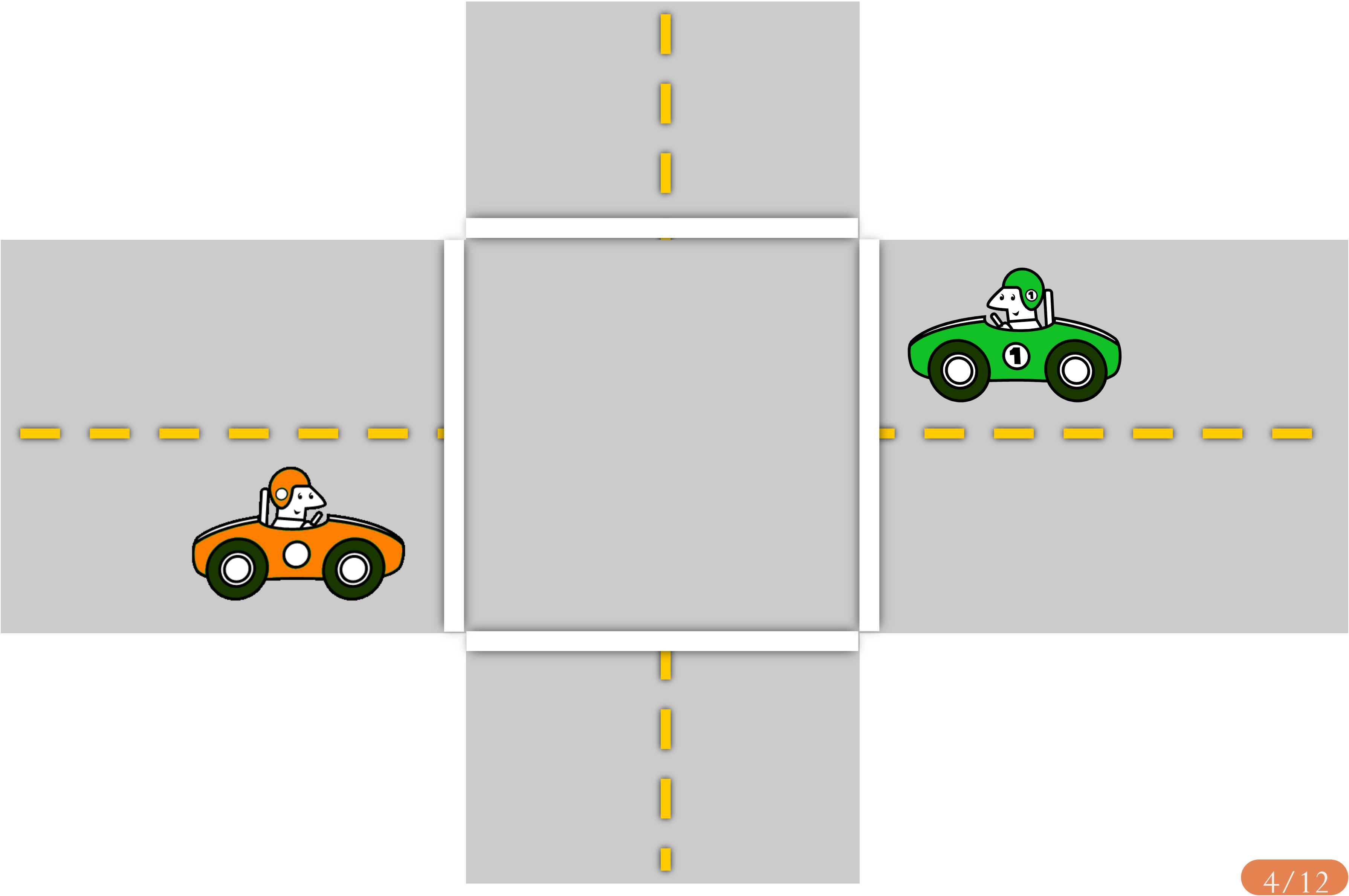
- Vehicles have positive velocity
- Accurate sensing
- Instantaneous braking and acceleration
- Time synchronization
- Delay for sensor updates is bounded
- Straight lane dynamics
- Cars represented as points, lanes as lines

Previous Work: Highway Control

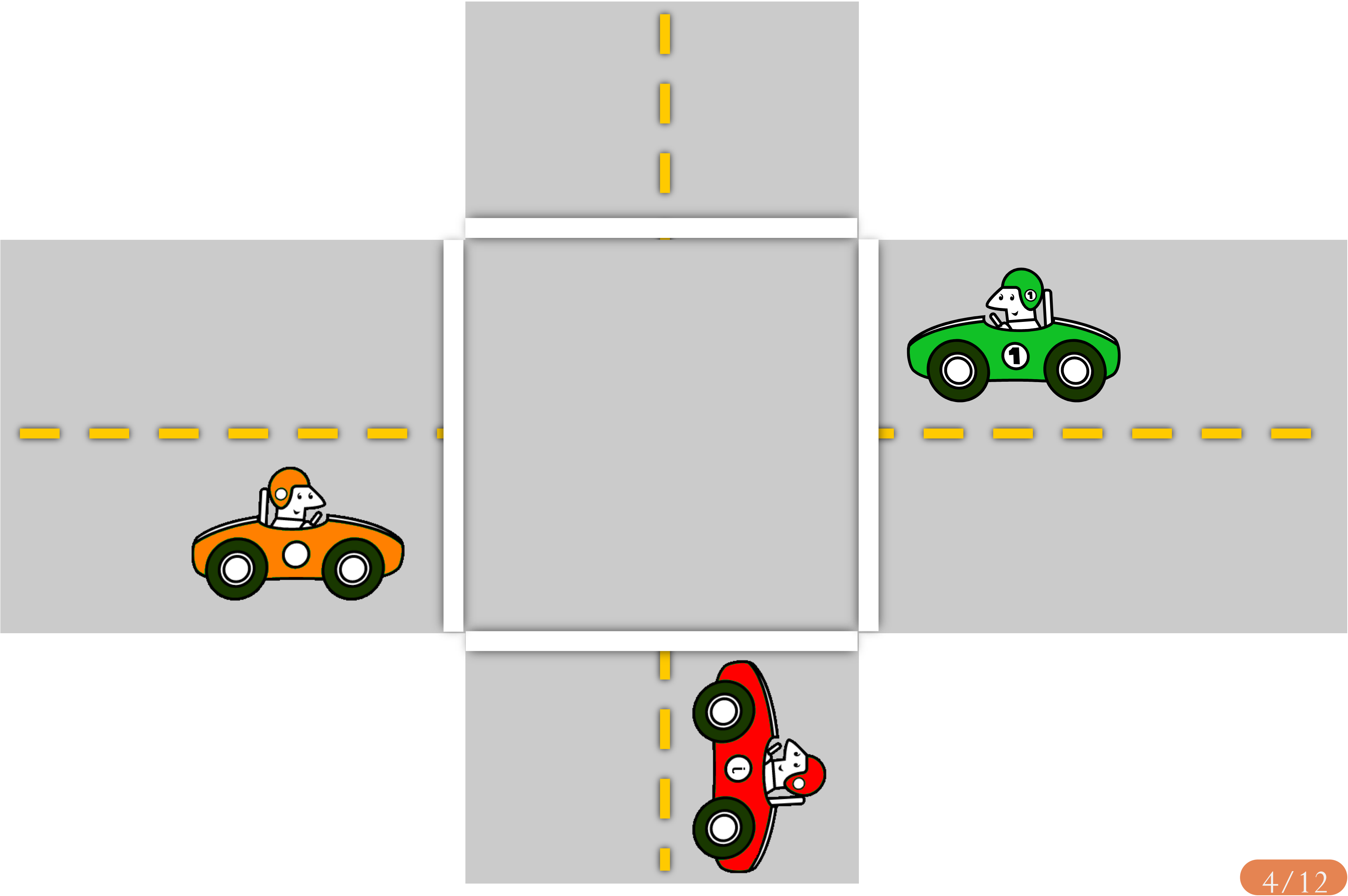


- Verified multilane highway system
- Arbitrary number of cars
- Arbitrary number of lanes
- Proof of safety for distributed control built from two-car “building blocks.”

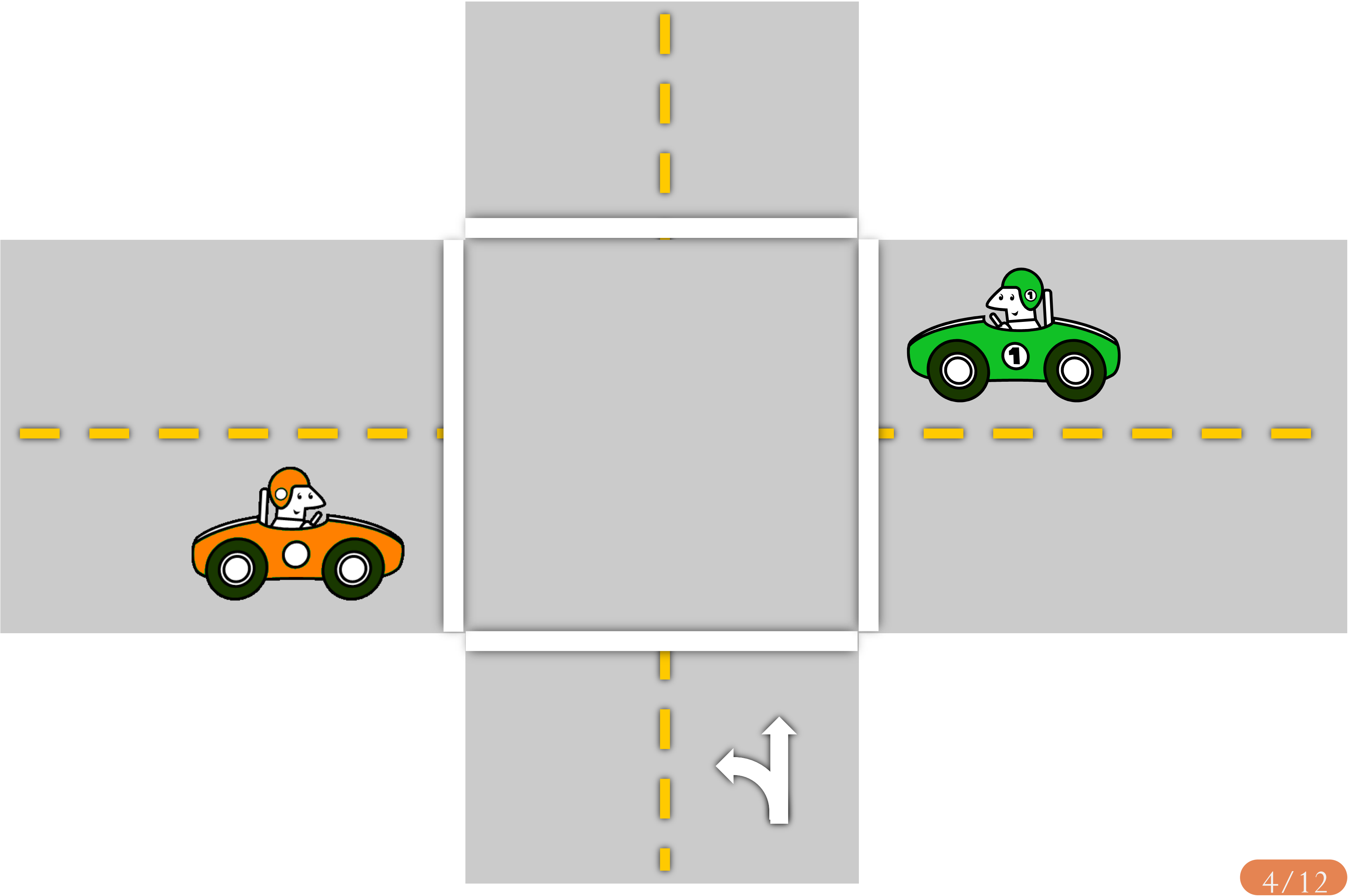
Intersection Building Blocks



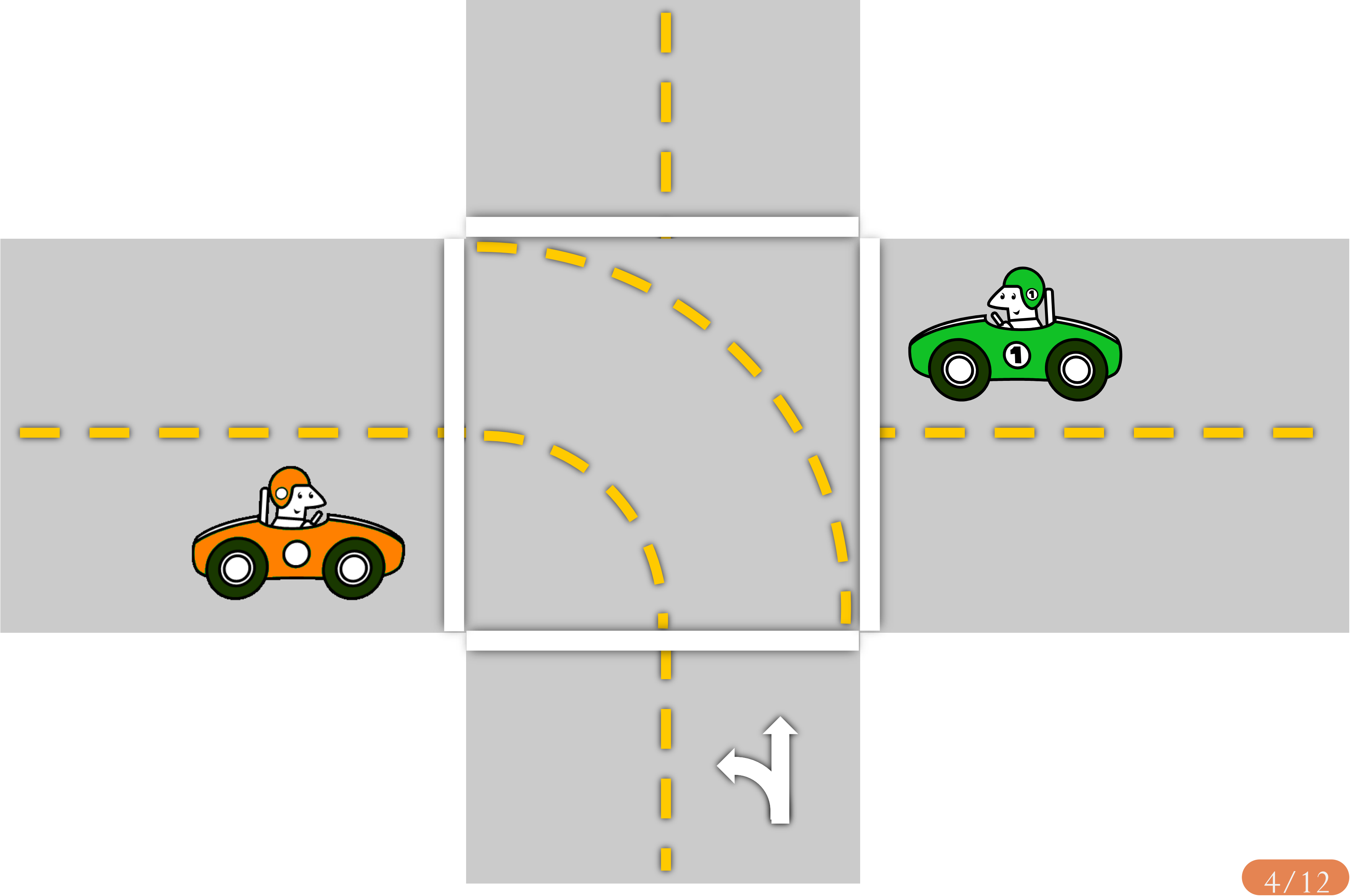
Intersection Building Blocks



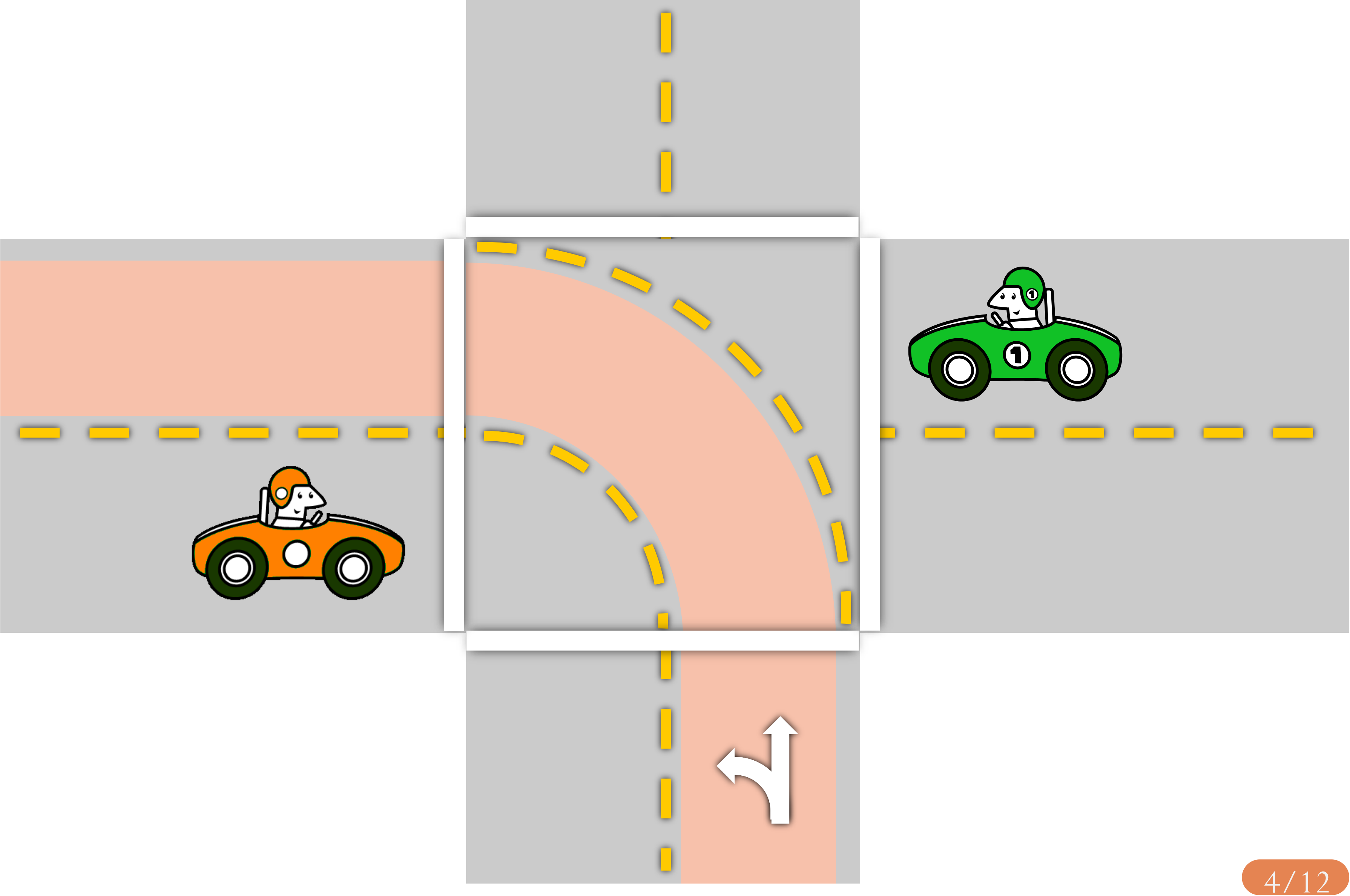
Intersection Building Blocks



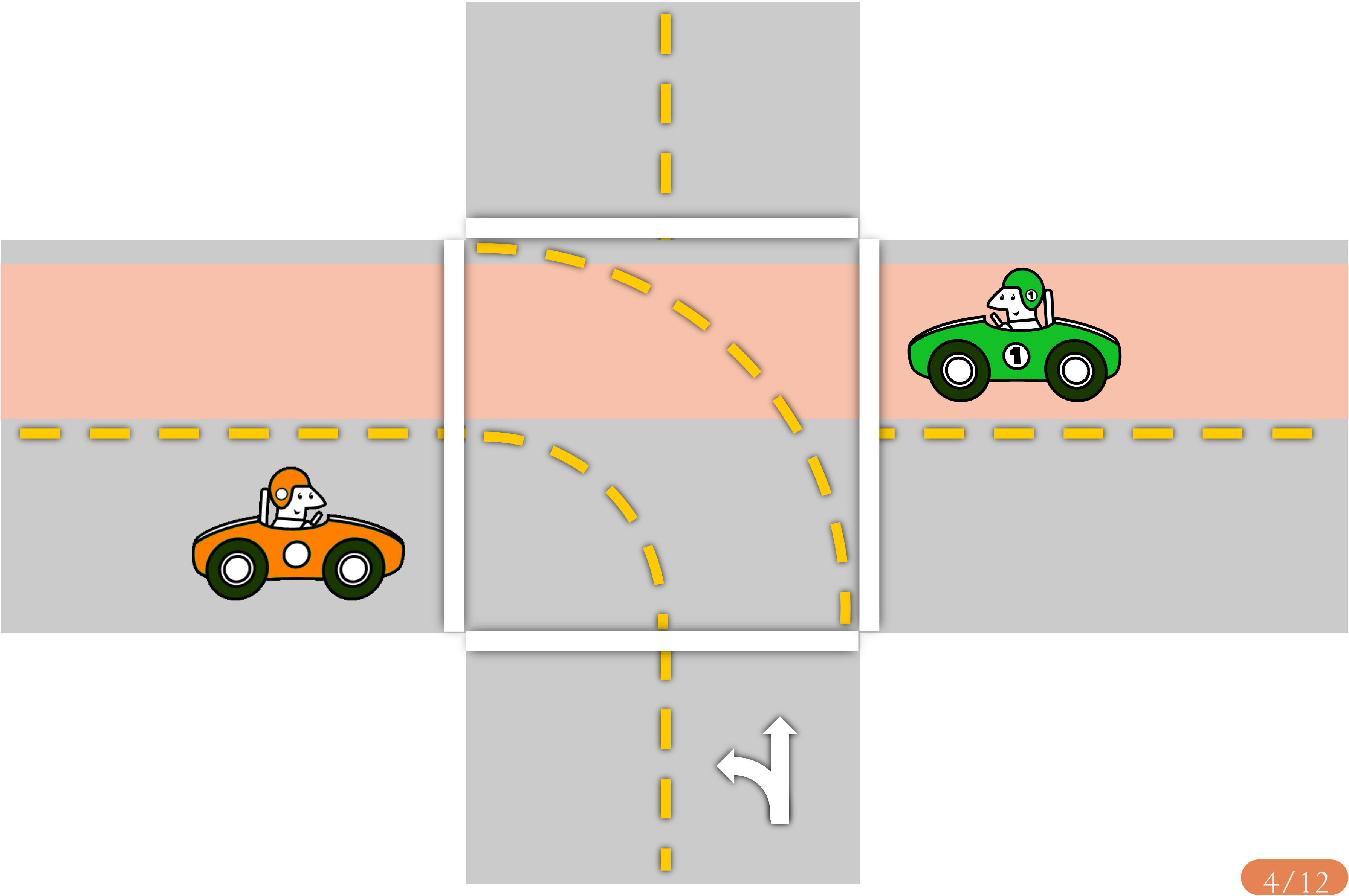
Intersection Building Blocks



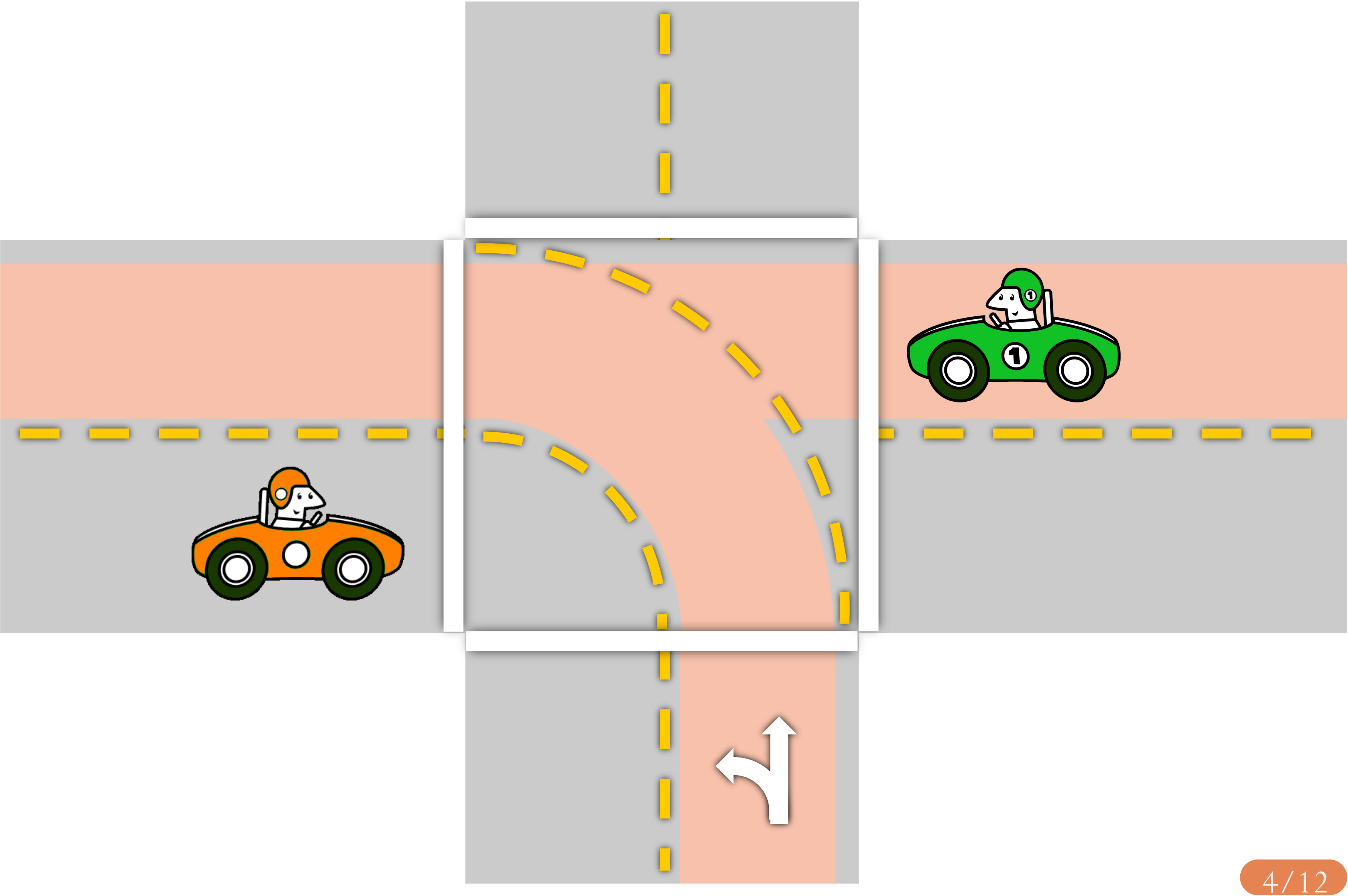
Intersection Building Blocks



Intersection Building Blocks

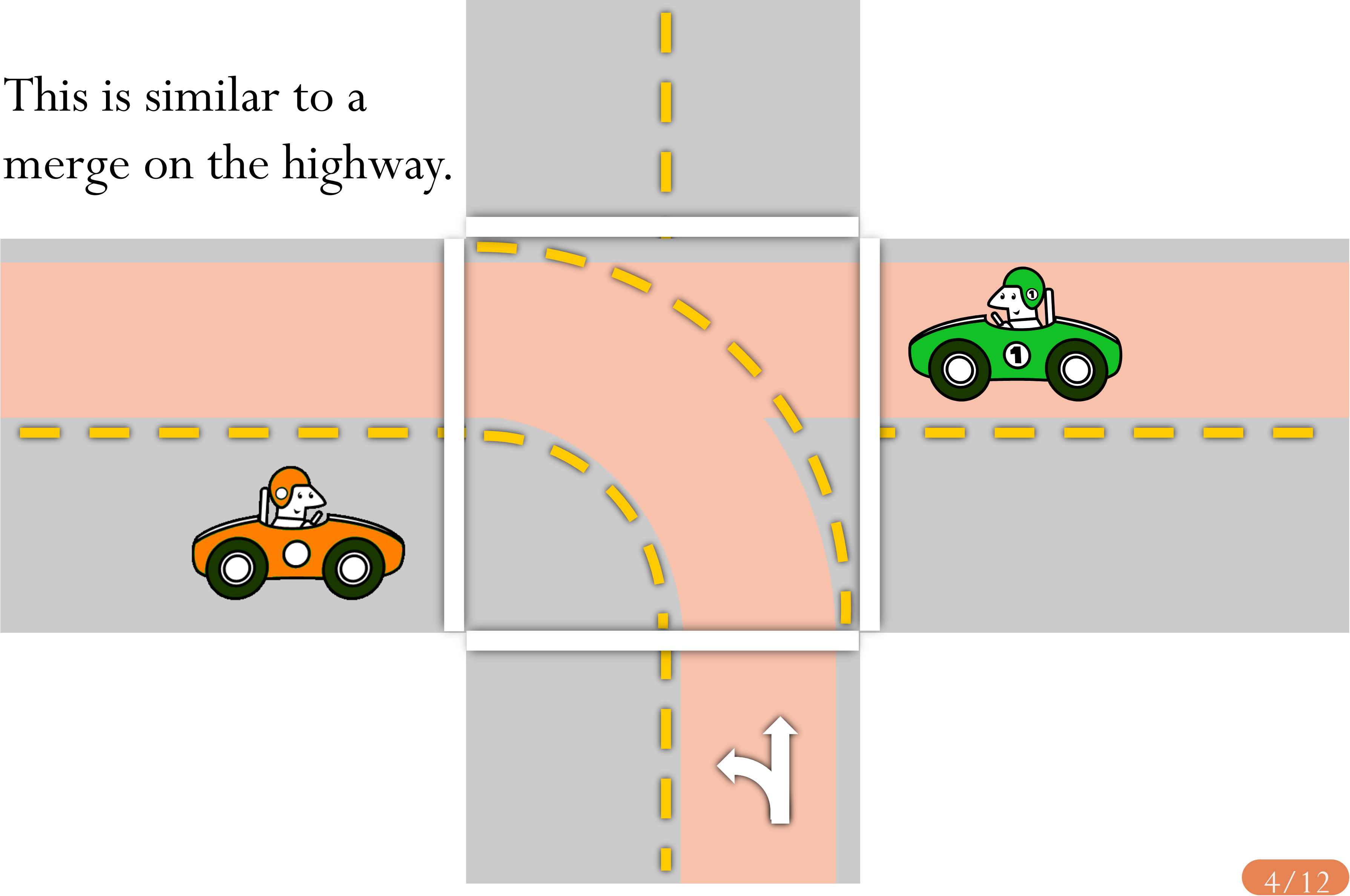


Intersection Building Blocks

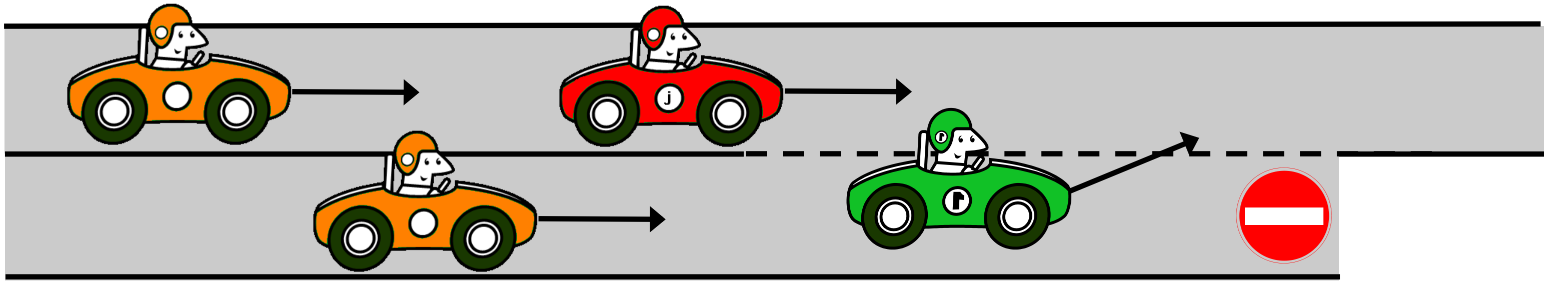


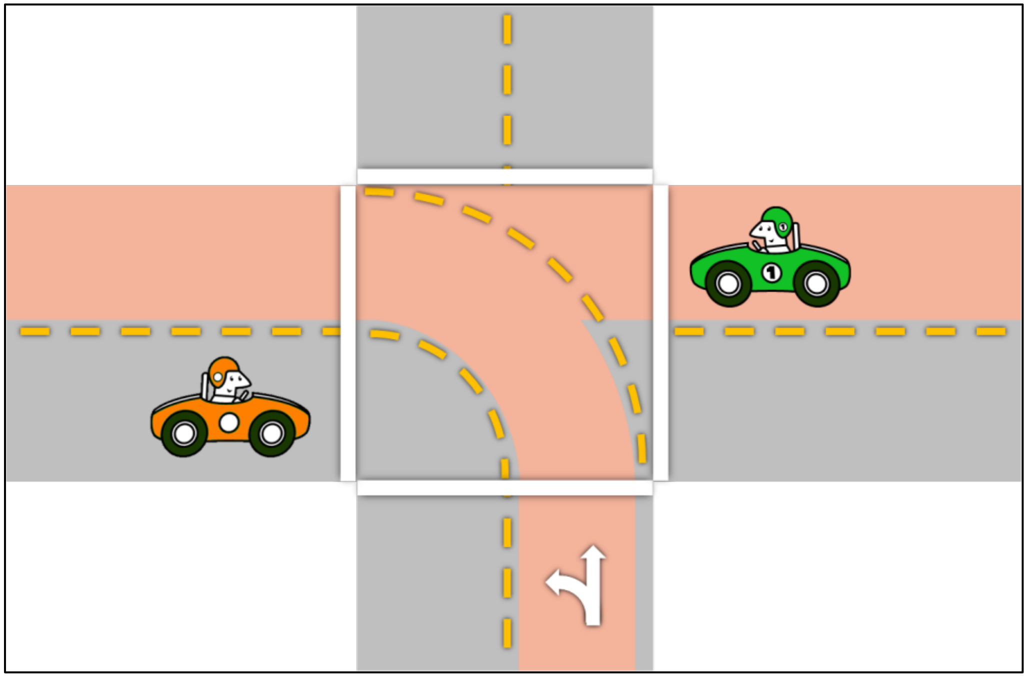
Intersection Building Blocks

This is similar to a merge on the highway.

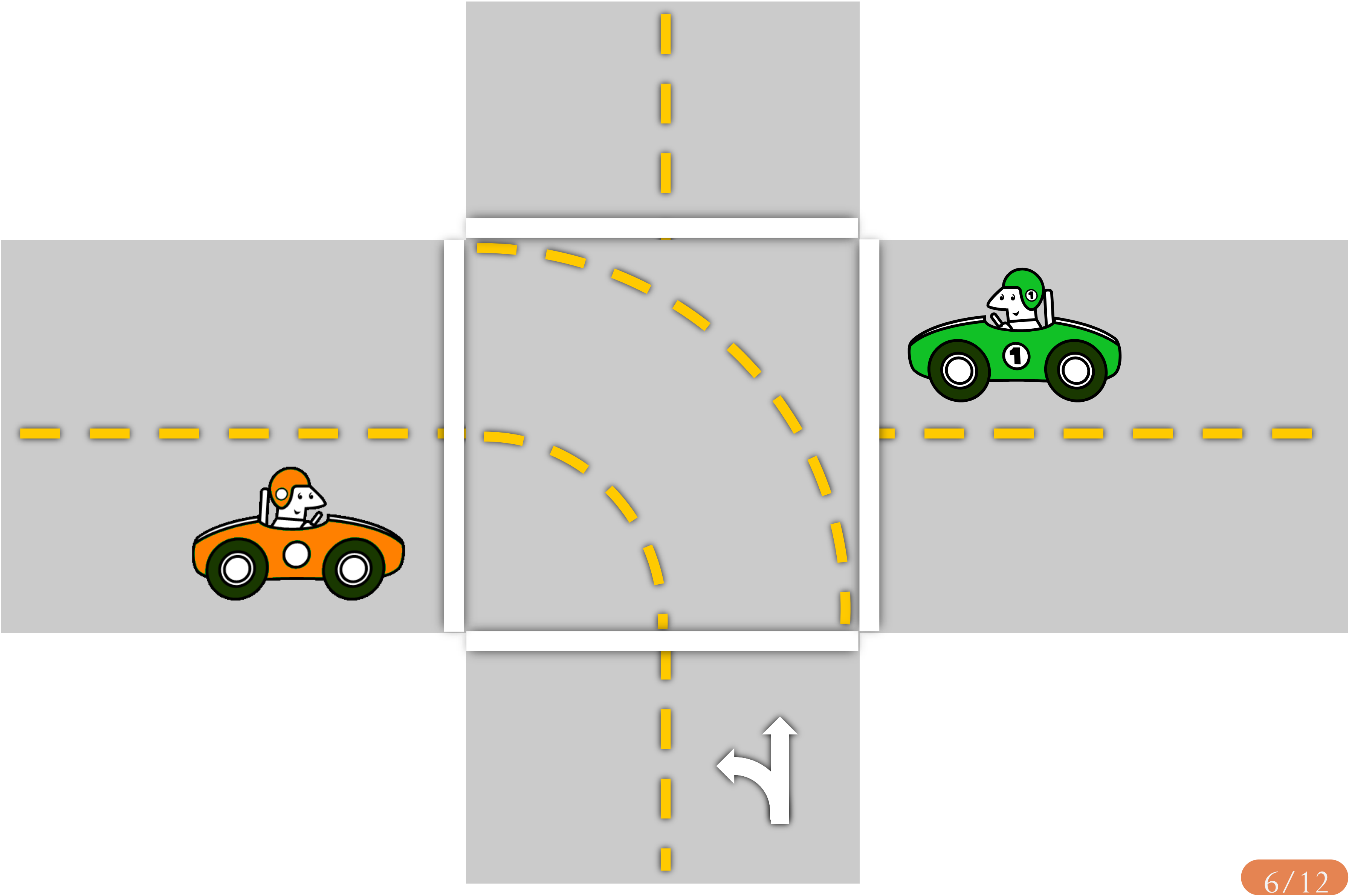


T-Intersection Building Block

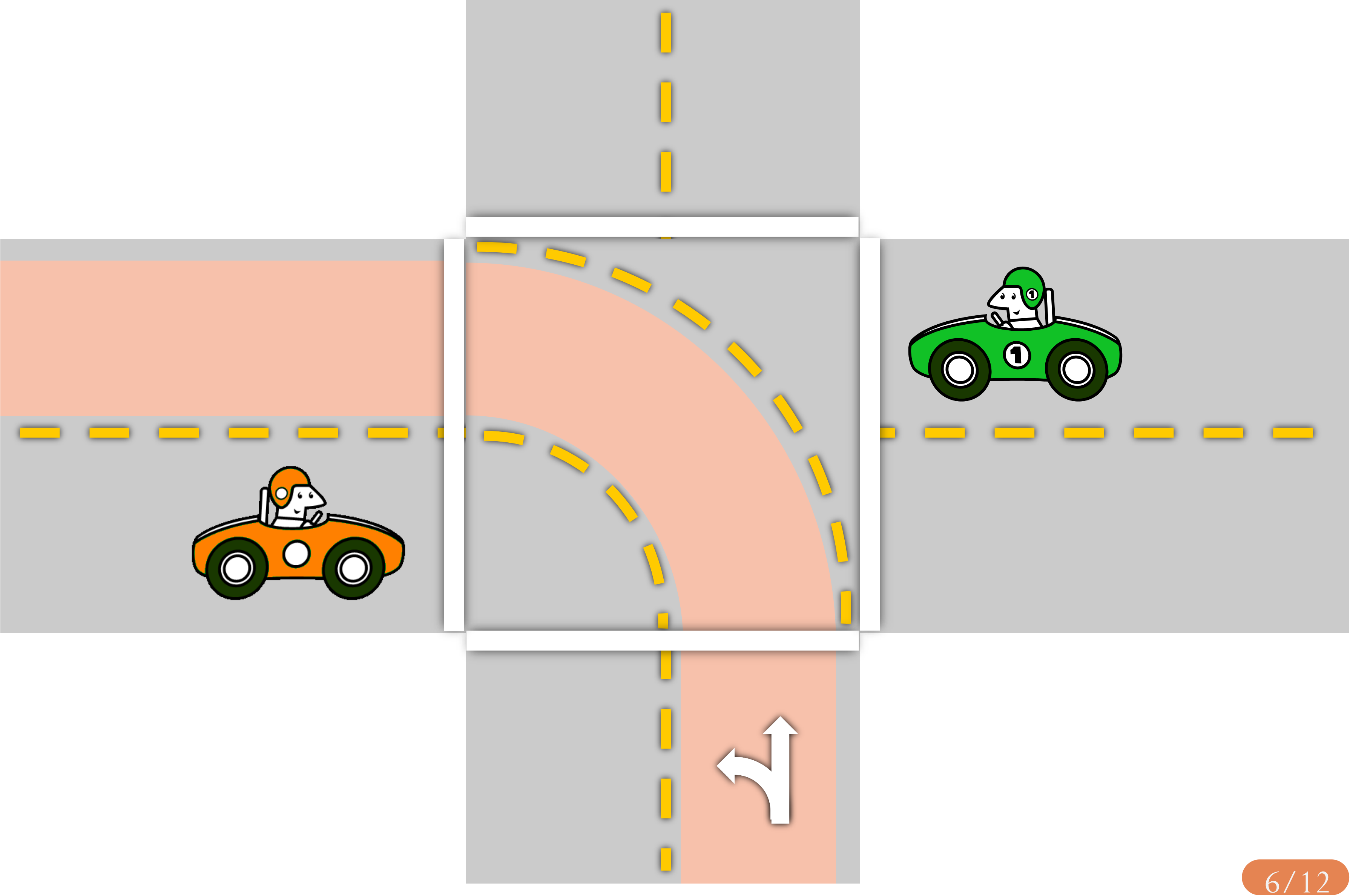




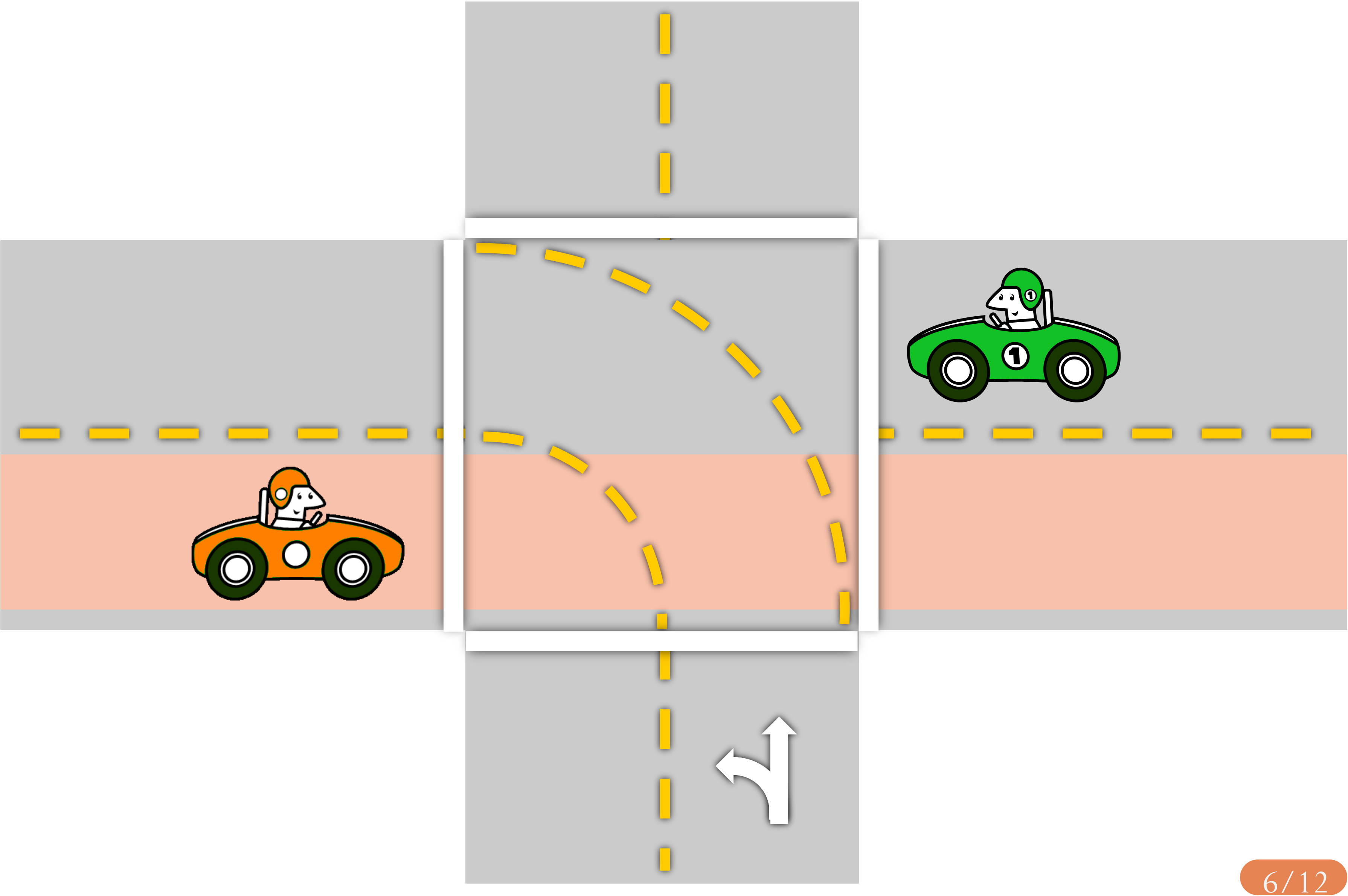
Intersection Building Blocks



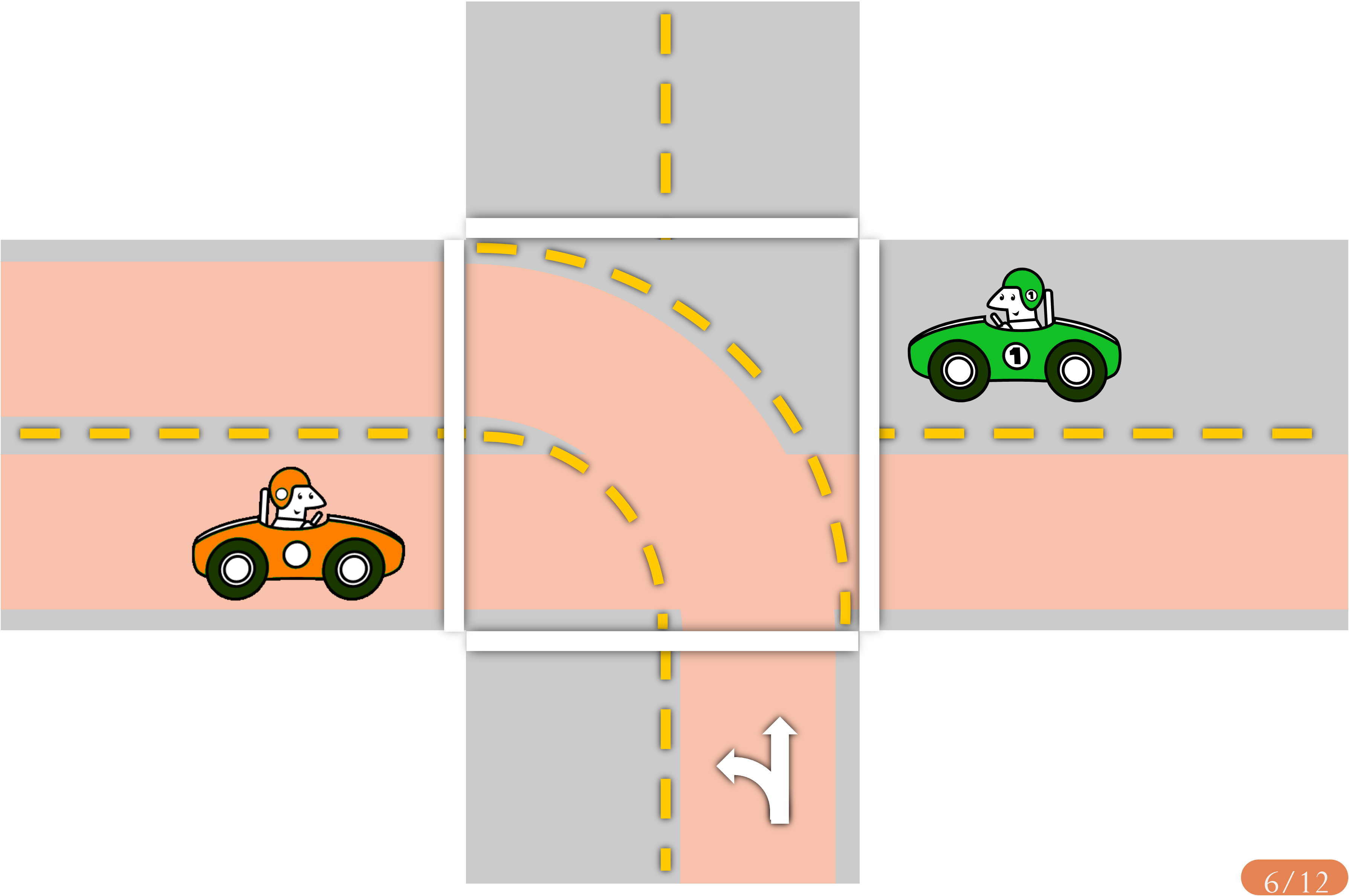
Intersection Building Blocks



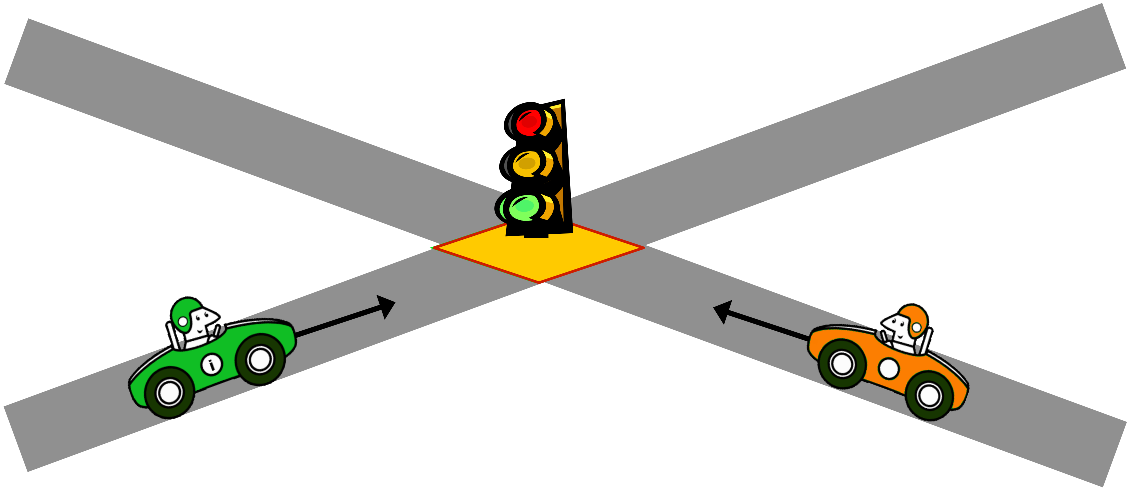
Intersection Building Blocks

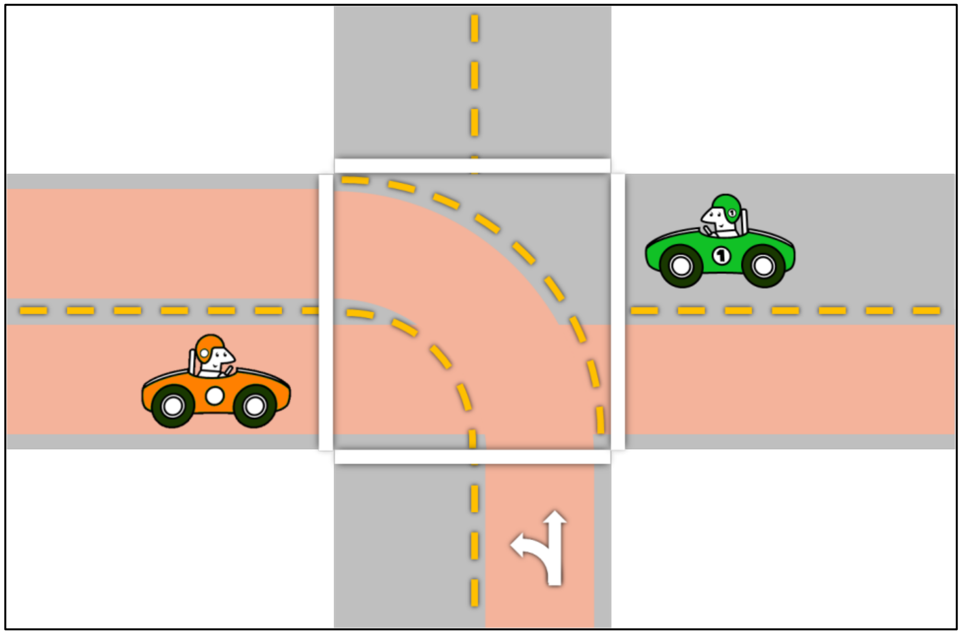


Intersection Building Blocks



Straight Lane Building Block





Differential Dynamic Logic*

*The short version.

$$\text{Initial Conditions} \rightarrow [\text{Model}]\ \text{Requirements}$$

Differential Dynamic Logic

Initial Conditions → [Model] Requirements

Differential Dynamic Logic

Initial Conditions → [Model] Requirements

logical formula

logical formula

Differential Dynamic Logic

$$\underbrace{(x_f \leq x_\ell)}_{\text{logical formula}} \rightarrow [\text{Model}] \underbrace{(x_f \leq x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{(x_f \leq x_\ell)}_{\text{logical formula}} \rightarrow [\text{Model}]\ \underbrace{(x_f \leq x_\ell)}_{\text{logical formula}}$$

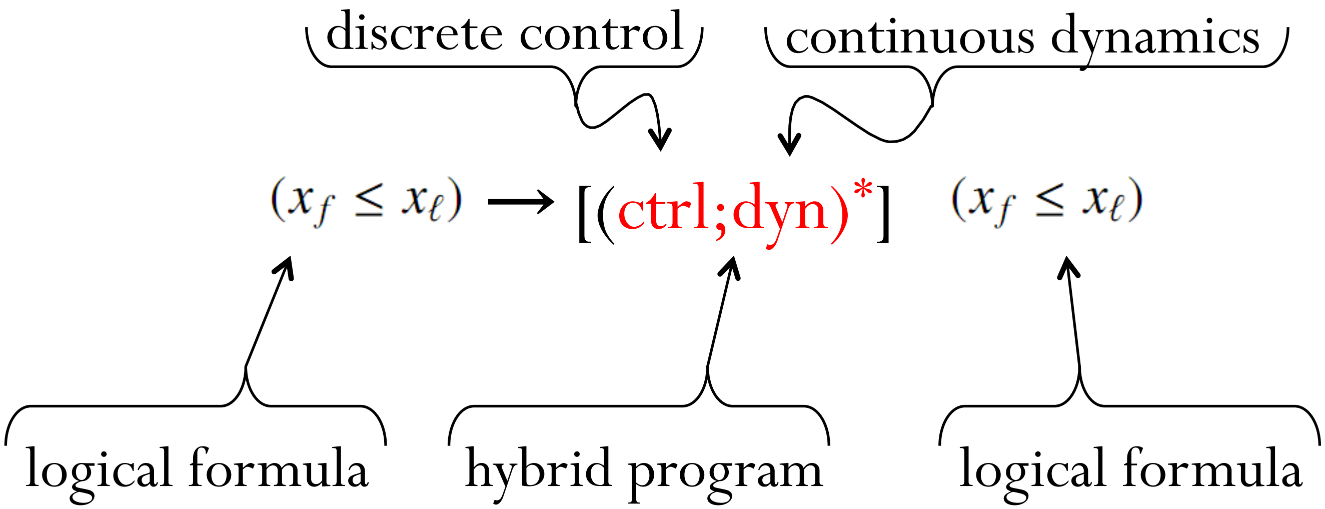
Differential Dynamic Logic

$$\underbrace{(x_f \leq x_\ell)}_{\text{logical formula}} \rightarrow [\underbrace{\text{Model}}_{\text{hybrid program}}] \underbrace{(x_f \leq x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic

$$\underbrace{(x_f \le x_\ell)}_{\text{logical formula}} \rightarrow \underbrace{[\overset{\text{discrete control} \quad \text{continuous dynamics}}{\text{Model}}]}_{\text{hybrid program}} \underbrace{(x_f \le x_\ell)}_{\text{logical formula}}$$

Differential Dynamic Logic



discrete control

continuous dynamics

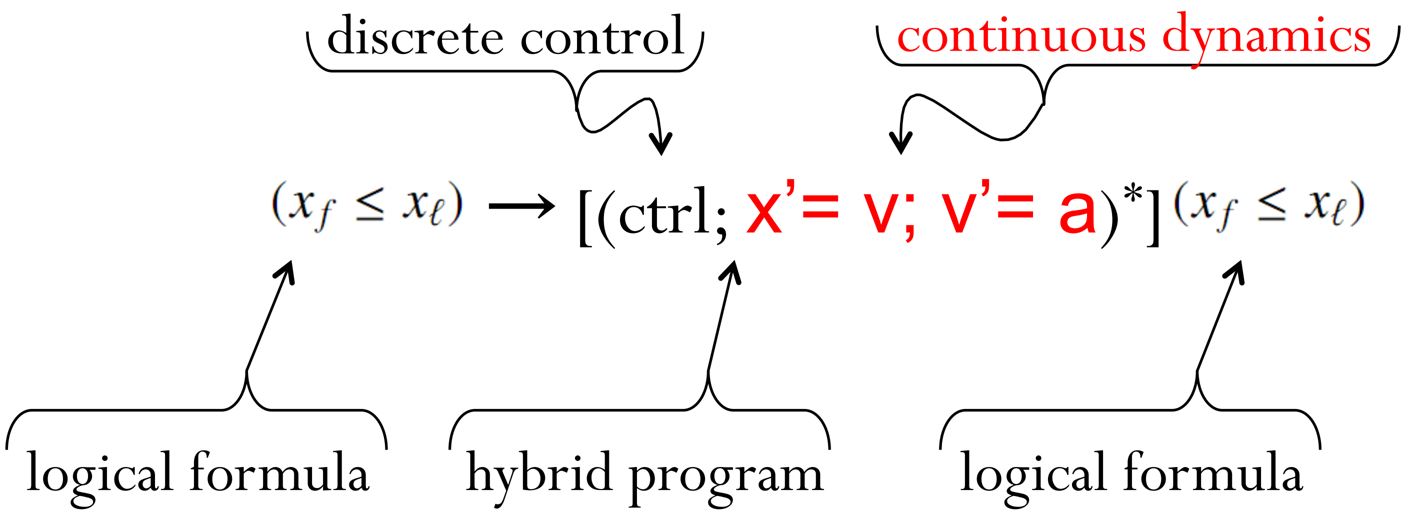
$$(x_f \leq x_\ell) \rightarrow [(\mathrm{ctrl};\mathrm{dyn})^*]\ (x_f \leq x_\ell)$$

logical formula

hybrid program

logical formula

Differential Dynamic Logic



discrete control

continuous dynamics

$$(x_f \leq x_\ell) \longrightarrow [(\text{ctrl};\ x' = v;\ v' = a)^*]\,(x_f \leq x_\ell)$$

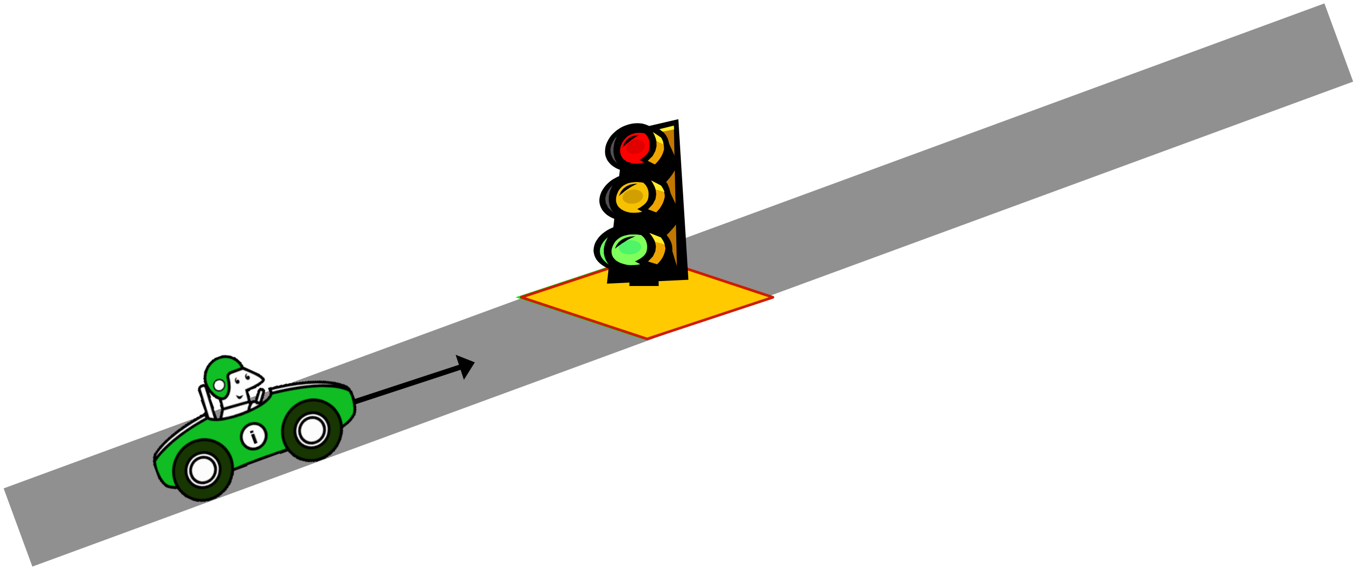
logical formula

hybrid program

logical formula

Single Lane Stoplight

To Prove: $\left(I = red \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

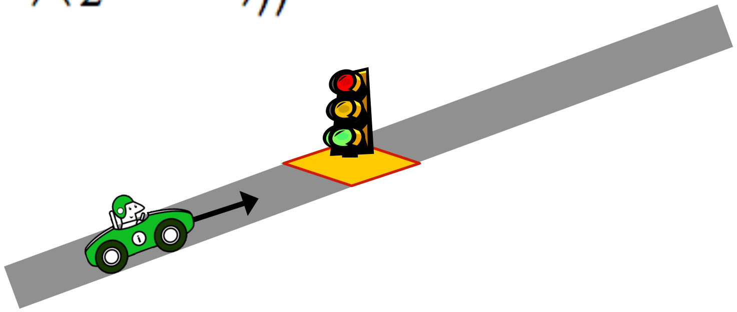


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \;\land\; \left(xI < x \;\lor\; xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\mathtt{lane} \equiv\;& (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\;& (?(I = green);\; I := yellow \\
& \cup\; ?(I = yellow \\
& \quad \land \left(xI < x \lor xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)); \\
& \quad I := red \\
& \cup\; ?(I = red);\; I := green \\
& \cup\; ?true) \\
CCtrl \equiv\;& (?(I = green \lor xI = x);\; a := A \\
& \cup\; ?(v = 0 \land xI \neq x);\; a := 0 \\
& \cup\; ?(v = V \land (I = green \lor xI = x));\; a := 0 \\
& \cup\; a := -B) \\
dyn \equiv\;& (t := 0; x' = v, v' = a \;\&\; v \geq 0 \land v \leq V \land t \leq \varepsilon)
\end{aligned}
$$

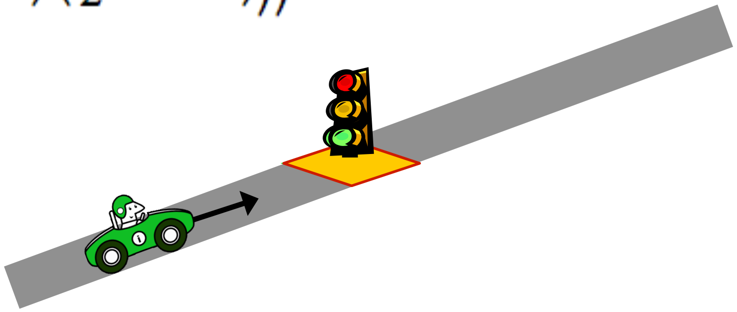


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \;\wedge\; \left(xI < x \;\vee\; xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\texttt{lane}]\left(I = red \rightarrow xI \neq x\right)$

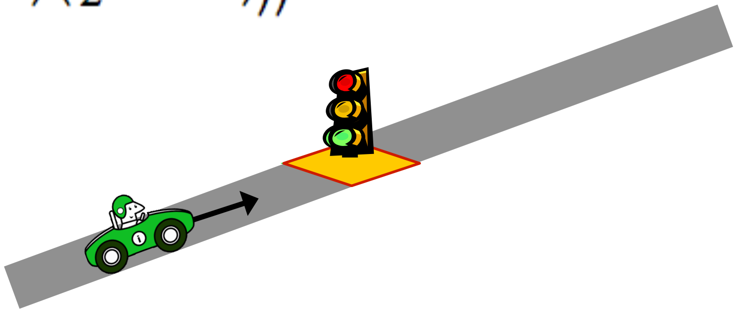
$$
\begin{aligned}
\texttt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?(I = yellow \\
& \qquad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)); \\
& \qquad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \vee xI = x);\ a := A \\
& \cup\ ?(v = 0 \wedge xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \wedge (I = green \vee xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a \mathbin{\&} v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$



Single Lane Stoplight

To Prove: $\left(I = red \ \wedge \ \left(xI < x \ \vee \ xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\mathtt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?\,(I = yellow \\
& \qquad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)); \\
& \qquad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \vee xI = x);\ a := A \\
& \cup\ ?(v = 0 \wedge xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \wedge (I = green \vee xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a\ \&\ v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

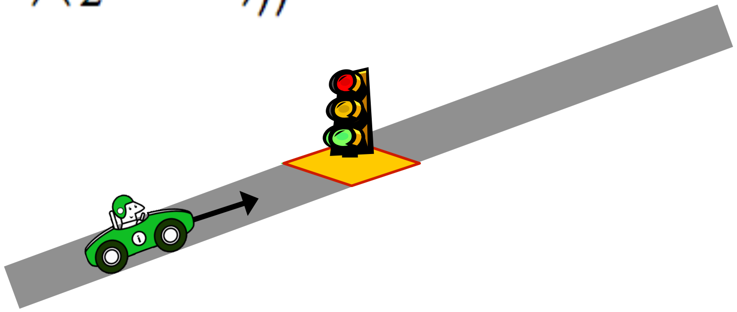


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \ \wedge \ \left(xI < x \ \vee \ xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\mathtt{lane} \equiv \ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv \ & (?(I = green); \ I := yellow \\
& \cup \ ?(I = yellow \\
& \qquad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)\Big); \\
& \qquad I := red \\
& \cup \ ?(I = red); \ I := green \\
& \cup \ ?true) \\
CCtrl \equiv \ & (?(I = green \vee xI = x); \ a := A \\
& \cup \ ?(v = 0 \wedge xI \neq x); \ a := 0 \\
& \cup \ ?(v = V \wedge (I = green \vee xI = x)); \ a := 0 \\
& \cup \ a := -B) \\
dyn \equiv \ & (t := 0; x' = v, v' = a \ \& \ v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

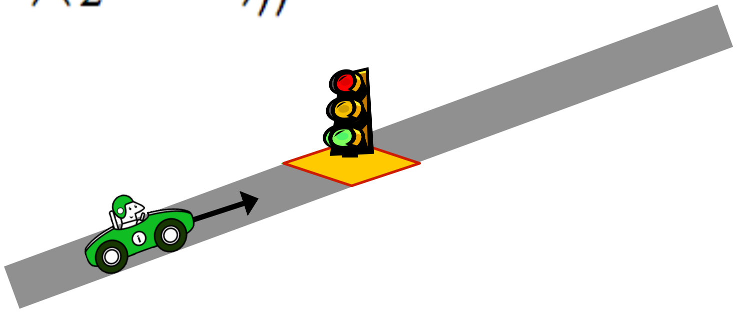


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \;\wedge\; \left(xI < x \;\vee\; xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\mathtt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?(I = yellow \\
& \quad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)); \\
& \quad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \vee xI = x);\ a := A \\
& \cup\ ?(v = 0 \wedge xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \wedge (I = green \vee xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a\ \&\ v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

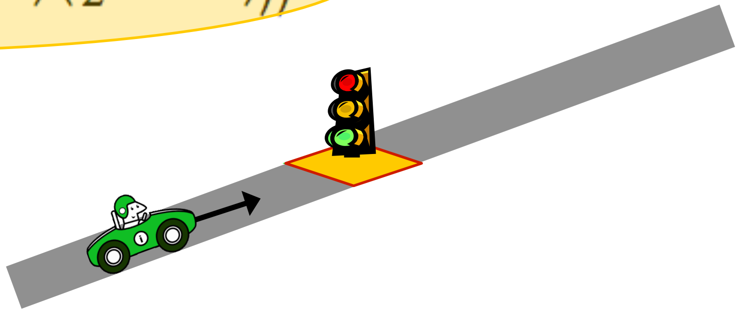


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \;\wedge\; \left(xI < x \;\vee\; xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\texttt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\texttt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?(I = yellow \\
& \quad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right));\\
& \quad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \vee xI = x);\ a := A \\
& \cup\ ?(v = 0 \wedge xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \wedge (I = green \vee xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a \;\&\; v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$



Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \;\wedge\; \left(xI < x \;\vee\; xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$\mathtt{lane} \equiv (ICtrl; CCtrl; dyn)^*$$

$$ICtrl \equiv (?(I = green);\; I := yellow$$

$$\cup\; ?(I = yellow$$

$$\wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right));$$

$$I := red$$

$$\cup\; ?(I = red);\; I := green$$

$$\cup\; ?true)$$

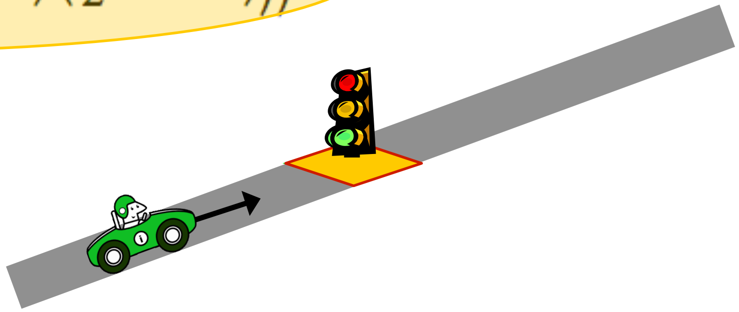
$$CCtrl \equiv (?(I = green \vee xI = x);\; a := A$$

$$\cup\; ?(v = 0 \wedge xI \neq x);\; a := 0$$

$$\cup\; ?(v = V \wedge (I = green \vee xI = x));\; a := 0$$

$$\cup\; a := -B)$$

$$dyn \equiv (t := 0; x' = v, v' = a \;\&\; v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)$$

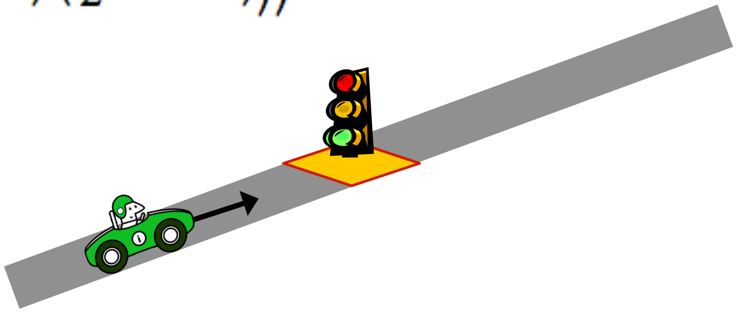


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \ \land \ \left(xI < x \ \lor \ xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\texttt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$\begin{aligned}
\texttt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?(I = yellow \\
& \qquad \land \left(xI < x \lor xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)); \\
& \qquad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \lor xI = x);\ a := A \\
& \cup\ ?(v = 0 \land xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \land (I = green \lor xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a\ \&\ v \geq 0 \land v \leq V \land t \leq \varepsilon)
\end{aligned}$$

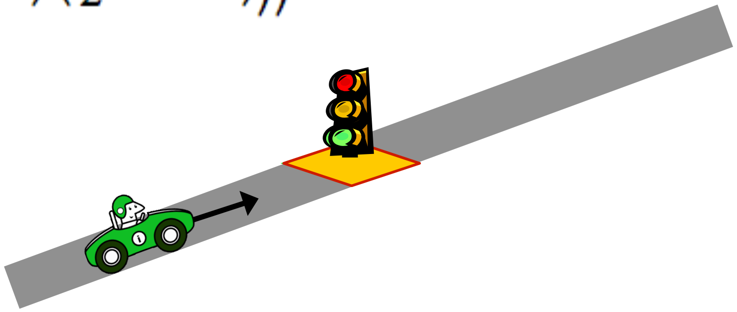


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \ \land \ \left(xI < x \ \lor \ xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\mathtt{lane} \equiv \ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv \ & (?(I = green); \ I := yellow \\
& \cup \ ?(I = yellow \\
& \quad \land \left(xI < x \lor xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)); \\
& \quad I := red \\
& \cup \ ?(I = red); \ I := green \\
& \cup \ ?true) \\
CCtrl \equiv \ & (?(I = green \lor xI = x); \ a := A \\
& \cup \ ?(v = 0 \land xI \neq x); \ a := 0 \\
& \cup \ ?(v = V \land (I = green \lor xI = x)); \ a := 0 \\
& \cup \ a := -B) \\
dyn \equiv \ & (t := 0; x' = v, v' = a \ \& \ v \geq 0 \land v \leq V \land t \leq \varepsilon)
\end{aligned}
$$

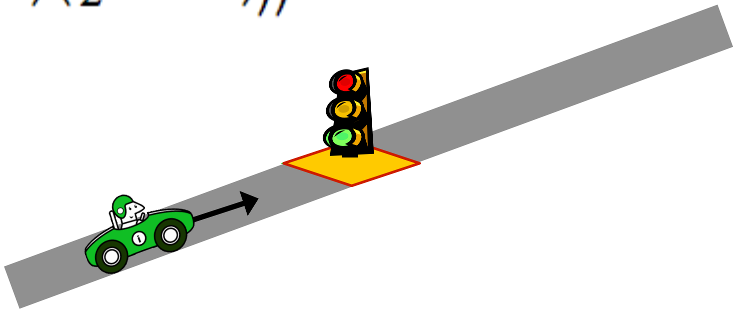


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \ \wedge \ \left(xI < x \ \vee \ xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\texttt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\texttt{lane} &\equiv (ICtrl; CCtrl; dyn)^* \\
ICtrl &\equiv (?(I = green);\ I := yellow \\
&\quad \cup\ ?(I = yellow \\
&\qquad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right));\\
&\qquad I := red \\
&\quad \cup\ ?(I = red);\ I := green \\
&\quad \cup\ ?true) \\
CCtrl &\equiv (?(I = green \vee xI = x);\ a := A \\
&\quad \cup\ ?(v = 0 \wedge xI \neq x);\ a := 0 \\
&\quad \cup\ ?(v = V \wedge (I = green \vee xI = x));\ a := 0 \\
&\quad \cup\ a := -B) \\
dyn &\equiv (t := 0; x' = v, v' = a\ \&\ v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

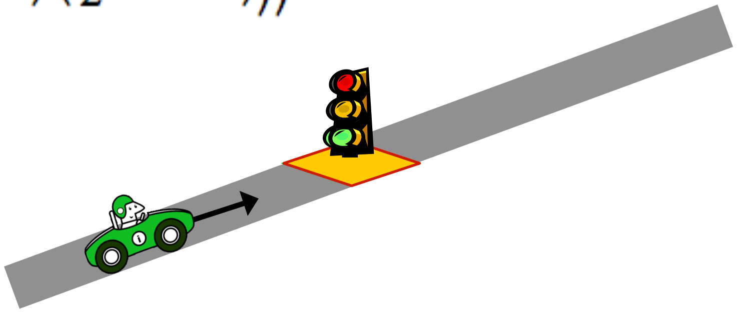


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \land \left(xI < x \lor xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\mathtt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?\,(I = yellow \\
& \qquad \land \left(xI < x \lor xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right));\\
& \qquad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \lor xI = x);\ a := A \\
& \cup\ ?(v = 0 \land xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \land (I = green \lor xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a\ \&\ v \geq 0 \land v \leq V \land t \leq \varepsilon)
\end{aligned}
$$

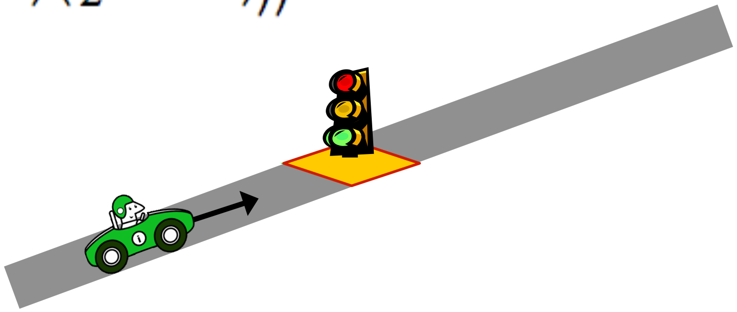


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \;\wedge\; \left(xI < x \;\vee\; xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$
\begin{aligned}
\mathtt{lane} \equiv\;& (ICtrl; CCtrl; dyn)^*\\
ICtrl \equiv\;& (?(I = green);\; I := yellow\\
&\cup\; ?\,(I = yellow\\
&\qquad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)\Big);\\
&\qquad I := red\\
&\cup\; ?(I = red);\; I := green\\
&\cup\; ?true)\\
CCtrl \equiv\;& (?(I = green \vee xI = x);\; a := A\\
&\cup\; ?(v = 0 \wedge xI \neq x);\; a := 0\\
&\cup\; ?(v = V \wedge (I = green \vee xI = x));\; a := 0\\
&\cup\; a := -B)\\
dyn \equiv\;& (t := 0; x' = v, v' = a \;\&\; v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

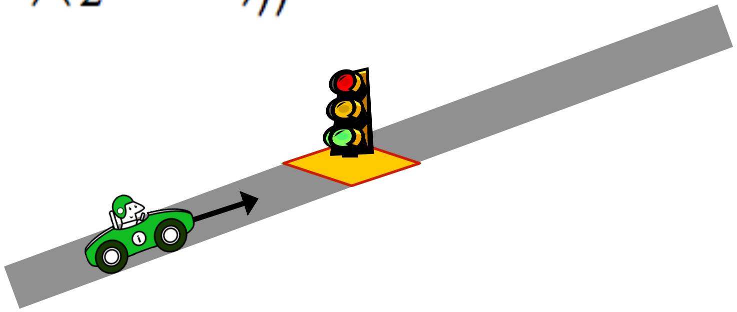


Initial Conditions → [Model] Requirements

Single Lane Stoplight

To Prove: $\left(I = red \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\texttt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$\begin{aligned}
\texttt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?(I = yellow \\
& \quad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right));\\
& \quad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \vee xI = x);\ a := A \\
& \cup\ ?(v = 0 \wedge xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \wedge (I = green \vee xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a\ \&\ v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}$$

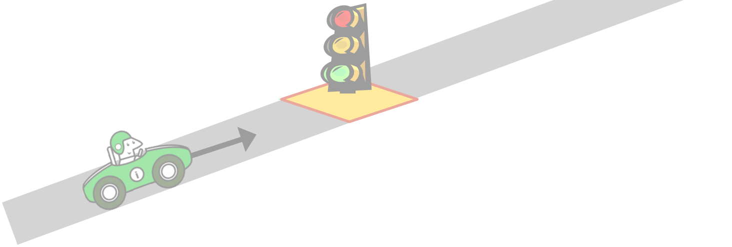


Single Lane Stoplight

To Prove: $\left(I = red \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B}\right)\right) \rightarrow [\mathtt{lane}]\left(I = red \rightarrow xI \neq x\right)$

$$\begin{aligned}
\mathtt{lane} \equiv\ & (ICtrl; CCtrl; dyn)^* \\
ICtrl \equiv\ & (?(I = green);\ I := yellow \\
& \cup\ ?(I = yellow \\
& \qquad \wedge \left(xI < x \vee xI > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)); \\
& \qquad I := red \\
& \cup\ ?(I = red);\ I := green \\
& \cup\ ?true) \\
CCtrl \equiv\ & (?(I = green \vee xI = x);\ a := A \\
& \cup\ ?(v = 0 \wedge xI \neq x);\ a := 0 \\
& \cup\ ?(v = V \wedge (I = green \vee xI = x));\ a := 0 \\
& \cup\ a := -B) \\
dyn \equiv\ & (t := 0; x' = v, v' = a\ \&\ v \geq 0 \wedge v \leq V \wedge t \leq \varepsilon)
\end{aligned}$$

✓ **Verified in KeYmaera**

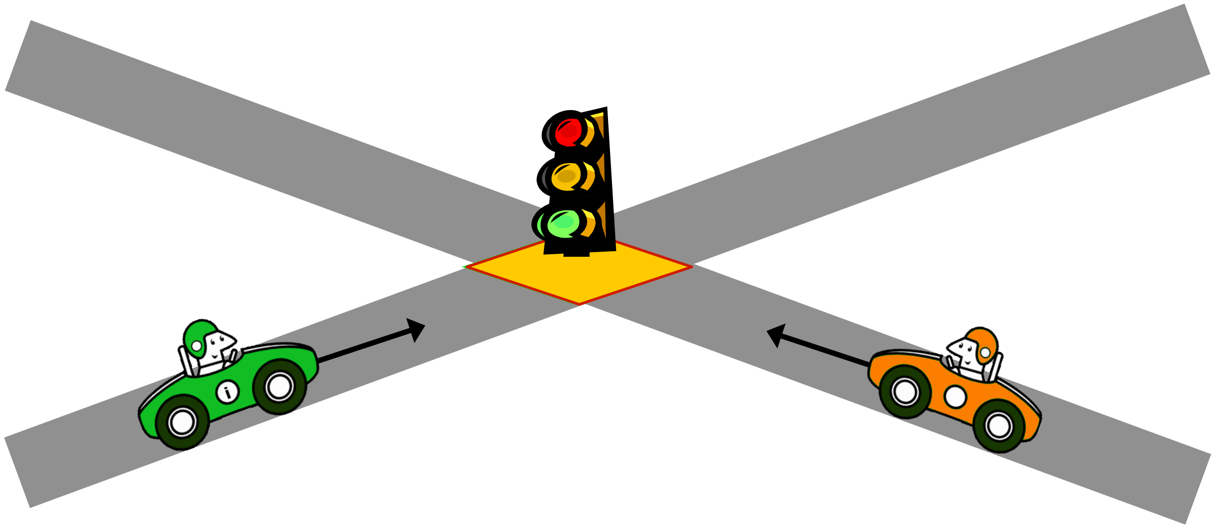


Initial Conditions → [Model] Requirements

Intersection

To Prove:

$$\begin{array}{l}\Big(I(1) = red \;\land\; \big(xI(1) < x(1) \lor xI(1) > x(1) + \dfrac{v(1)^2}{2B}\big) \\ \land\; I(2) = red \;\land\; \big(xI(2) < x(2) \lor xI(2) > x(2) + \dfrac{v(2)^2}{2B}\big)\Big)\end{array} \to \begin{array}{l}[\texttt{ic}]\Big(\,(I(1) = red \to xI(1) \neq x(1)) \\ \quad \land\; (I(2) = red \to xI(2) \neq x(2)) \\ \quad \land\; (I(1) = red \lor I(2) = red)\,\Big)\end{array}$$

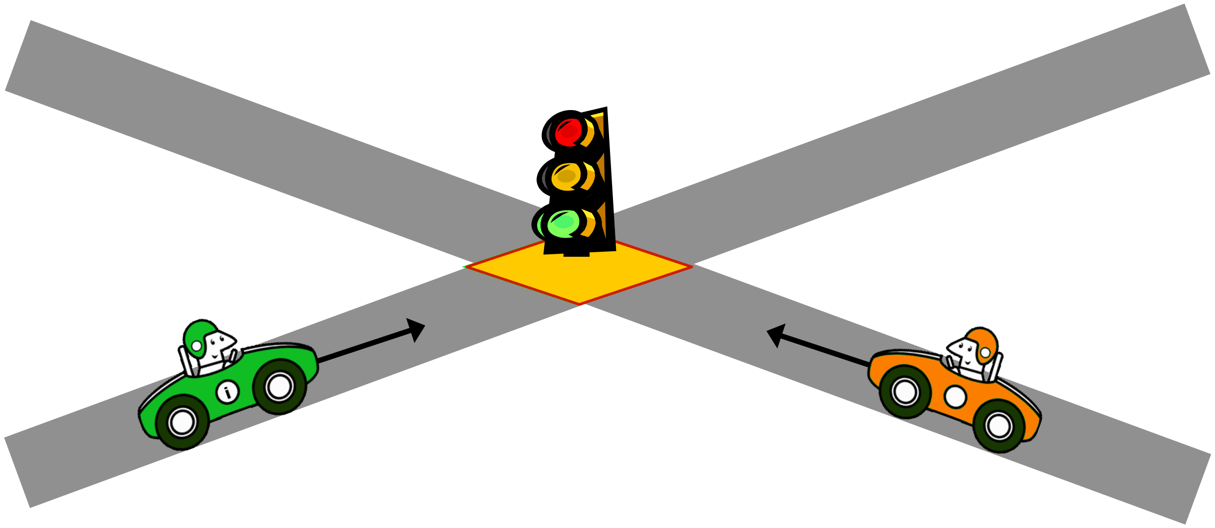


Intersection

To Prove:

Cars can stop initially $\longrightarrow$

$$[\texttt{ic}]\Big((I(1) = red \rightarrow xI(1) \neq x(1)) \\ \wedge (I(2) = red \rightarrow xI(2) \neq x(2)) \\ \wedge (I(1) = red \vee I(2) = red) \Big)$$

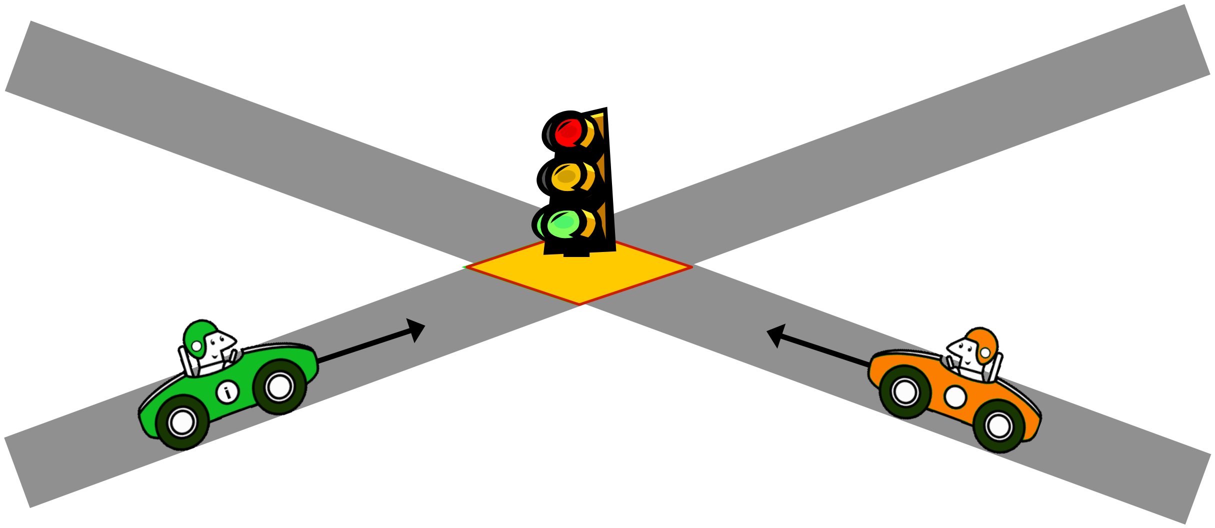


Initial Conditions ⟶ [Model] Requirements

Intersection

To Prove:

Cars can stop initially → [ic] No collision



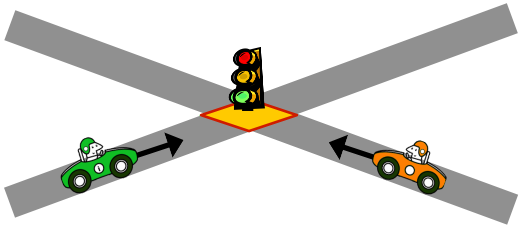
Intersection

To Prove:

Cars can stop initially

→

[ic] No collision



Initial Conditions → [Model] Requirements

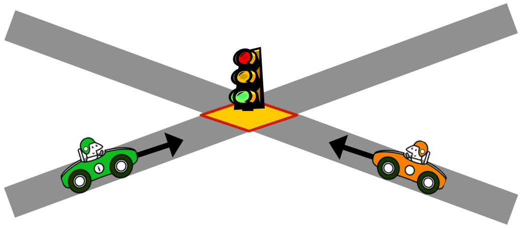
Intersection

To Prove:

Cars can stop initially

→

$\texttt{[ic]}$ No collision



$$\begin{aligned}
\texttt{ic} \equiv\ & (ICtrl(1); ICtrl(2); CCtrl(1); CCtrl(2); dyn)^* \\
ICtrl(i) \equiv\ & (?(I(i) = green);\ I(i) := yellow \\
& \cup\ ?\Big(I(i) = yellow \\
& \qquad \wedge (xI(i) < x \\
& \qquad\quad \vee \left(xI(i) > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)\Big)\Big);\ I(i) := red \\
& \cup\ ?\left(\bigwedge_j I(j) = red\right);\ I(i) := green \\
& \cup\ ?true) \\
CCtrl(i) \equiv\ & (?(I(i) = green \vee xI(i) = x(i));\ a(i) := A \\
& \cup\ ?(v(i) = 0 \wedge xI(i) \neq x(i));\ a(i) := 0 \\
& \cup\ ?(v(i) = V \wedge \\
& \qquad (I(i) = green \vee xI(i) = x(i)));\ a(i) := 0 \\
& \cup\ a(i) := -B) \\
dyn \equiv\ & (t := 0; x'(1) = v(1), v'(1) = a(1), \\
& \qquad x'(2) = v(2), v'(2) = a(2) \\
& \qquad \&\ v(1) \geq 0 \wedge v(2) \geq 0 \\
& \qquad \wedge v(1) \leq V \wedge v(2) \leq V \wedge t \leq \varepsilon)
\end{aligned}$$

Initial Conditions → [Model] Requirements

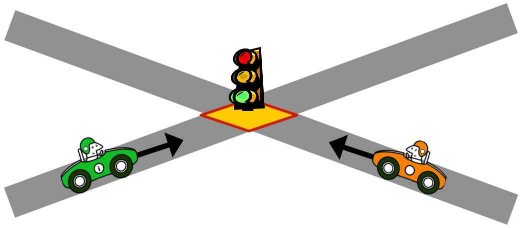
Intersection

To Prove:

Cars can stop initially

→

$[\texttt{ic}]$ No collision



$$
\begin{aligned}
\texttt{ic} \equiv\ & (ICtrl(1); ICtrl(2); CCtrl(1); CCtrl(2); dyn)^* \\
ICtrl(i) \equiv\ & (?(I(i) = green);\ \ I(i) := yellow \\
& \cup\ ?\big(I(i) = yellow \\
& \quad \wedge (xI(i) < x \\
& \quad\quad \vee \left(xI(i) > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)\big);\ \ I(i) := red \\
& \cup\ ?\left(\bigwedge_j I(j) = red\right);\ \ I(i) := green \\
& \cup\ ?true) \\
CCtrl(i) \equiv\ & (?(I(i) = green \vee xI(i) = x(i));\ \ a(i) := A \\
& \cup\ ?(v(i) = 0 \wedge xI(i) \neq x(i));\ \ a(i) := 0 \\
& \cup\ ?(v(i) = V \wedge \\
& \quad (I(i) = green \vee xI(i) = x(i)));\ \ a(i) := 0 \\
& \cup\ a(i) := -B) \\
dyn \equiv\ & (t := 0; x'(1) = v(1), v'(1) = a(1), \\
& \quad x'(2) = v(2), v'(2) = a(2) \\
& \quad \&\ v(1) \geq 0 \wedge v(2) \geq 0 \\
& \quad \wedge v(1) \leq V \wedge v(2) \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

Initial Conditions → [Model] Requirements

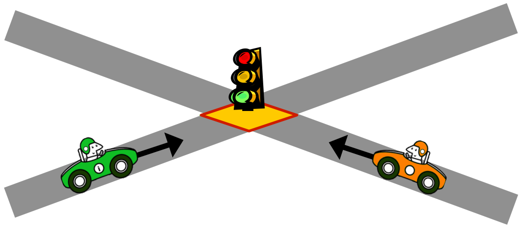
Intersection

To Prove:

Cars can stop initially

→

`[ic]` No collision



$$
\begin{aligned}
\texttt{ic} \equiv\ & (ICtrl(1); ICtrl(2); CCtrl(1); CCtrl(2); dyn)^{*} \\
ICtrl(i) \equiv\ & (?(I(i) = green);\ I(i) := yellow \\
& \cup\ ?\Big(I(i) = yellow \\
& \qquad \wedge (xI(i) < x \\
& \qquad\quad \vee \left(xI(i) > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)\Big);\ I(i) := red \\
& \cup\ ?\left(\bigwedge_j I(j) = red\right);\ I(i) := green \\
& \cup\ ?true) \\
CCtrl(i) \equiv\ & (?(I(i) = green \vee xI(i) = x(i));\ a(i) := A \\
& \cup\ ?(v(i) = 0 \wedge xI(i) \neq x(i));\ a(i) := 0 \\
& \cup\ ?(v(i) = V \wedge \\
& \qquad (I(i) = green \vee xI(i) = x(i)));\ a(i) := 0 \\
& \cup\ a(i) := -B) \\
dyn \equiv\ & (t := 0; x'(1) = v(1), v'(1) = a(1), \\
& \qquad x'(2) = v(2), v'(2) = a(2) \\
& \qquad \&\ v(1) \geq 0 \wedge v(2) \geq 0 \\
& \qquad \wedge v(1) \leq V \wedge v(2) \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

Initial Conditions → [Model] Requirements

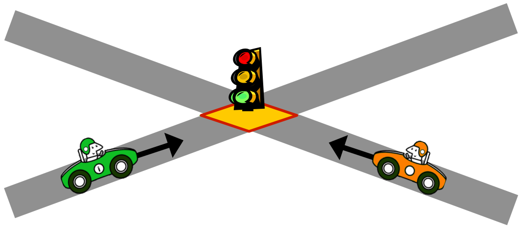
Intersection

To Prove:

Cars can stop initially

$\rightarrow$

$[\mathtt{ic}]$ No collision



$$
\begin{aligned}
\mathtt{ic} \equiv\ & (ICtrl(1); ICtrl(2); CCtrl(1); CCtrl(2); dyn)^{*} \\
ICtrl(i) \equiv\ & (?(I(i) = green);\ \ I(i) := yellow \\
& \cup\ ?\big(I(i) = yellow \\
& \qquad \wedge (xI(i) < x \\
& \qquad\quad \vee \Big(xI(i) > x + \frac{v^2}{2B} + \Big(\frac{A}{B} + 1\Big)\Big(\frac{A}{2}\varepsilon^2 + v\varepsilon\Big)\Big)\Big)\big);\ \ I(i) := red \\
& \cup\ ?\Big(\bigwedge_j I(j) = red\Big);\ I(i) := green \\
& \cup\ ?true) \\
CCtrl(i) \equiv\ & (?(I(i) = green \vee xI(i) = x(i));\ \ a(i) := A \\
& \cup\ ?(v(i) = 0 \wedge xI(i) \neq x(i));\ \ a(i) := 0 \\
& \cup\ ?(v(i) = V \wedge \\
& \qquad (I(i) = green \vee xI(i) = x(i)));\ \ a(i) := 0 \\
& \cup\ a(i) := -B) \\
dyn \equiv\ & (t := 0; x'(1) = v(1), v'(1) = a(1), \\
& \qquad x'(2) = v(2), v'(2) = a(2) \\
& \qquad \&\ v(1) \geq 0 \wedge v(2) \geq 0 \\
& \qquad \wedge v(1) \leq V \wedge v(2) \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

Initial Conditions → [Model] Requirements

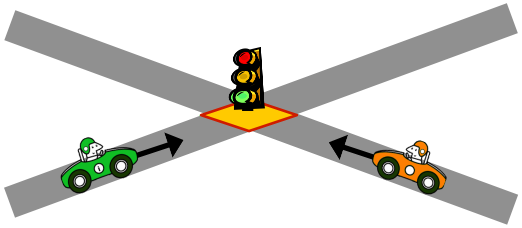
Intersection

To Prove:

Cars can stop initially

→

$[\mathtt{ic}]$ No collision



$$
\begin{aligned}
\mathtt{ic} \equiv\ & (\mathit{ICtrl}(1); \mathit{ICtrl}(2); \mathit{CCtrl}(1); \mathit{CCtrl}(2); \mathit{dyn})^* \\
\mathit{ICtrl}(i) \equiv\ & (?(I(i) = \mathit{green});\ I(i) := \mathit{yellow} \\
& \cup\ ?\Big(I(i) = \mathit{yellow} \\
& \quad \wedge (xI(i) < x \\
& \qquad \vee \Big(xI(i) > x + \frac{v^2}{2B} + \Big(\frac{A}{B} + 1\Big)\Big(\frac{A}{2}\varepsilon^2 + v\varepsilon\Big)\Big)\Big)\Big);\ I(i) := \mathit{red} \\
& \cup\ ?\Big(\bigwedge_j I(j) = \mathit{red}\Big);\ I(i) := \mathit{green} \\
& \cup\ ?\mathit{true}) \\
\mathit{CCtrl}(i) \equiv\ & (?(I(i) = \mathit{green} \vee xI(i) = x(i));\ a(i) := A \\
& \cup\ ?(v(i) = 0 \wedge xI(i) \neq x(i));\ a(i) := 0 \\
& \cup\ ?(v(i) = V \wedge \\
& \quad (I(i) = \mathit{green} \vee xI(i) = x(i)));\ a(i) := 0 \\
& \cup\ a(i) := -B) \\
\mathit{dyn} \equiv\ & (t := 0; x'(1) = v(1), v'(1) = a(1), \\
& \quad x'(2) = v(2), v'(2) = a(2) \\
& \quad \&\ v(1) \geq 0 \wedge v(2) \geq 0 \\
& \quad \wedge v(1) \leq V \wedge v(2) \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

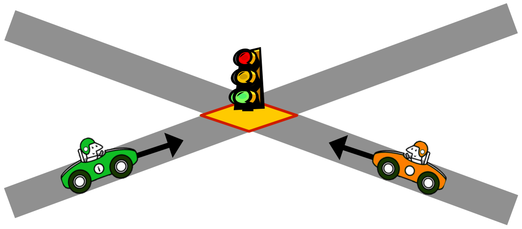
Intersection

To Prove:

Cars can stop initially

→

[ic] No collision



$$
\begin{aligned}
\texttt{ic} \equiv\ & (ICtrl(1); ICtrl(2); CCtrl(1); CCtrl(2); dyn)^* \\
ICtrl(i) \equiv\ & (?(I(i) = green);\ \ I(i) := yellow \\
& \cup\ ?\big(I(i) = yellow \\
& \qquad \wedge (xI(i) < x \\
& \qquad\quad \vee \left(xI(i) > x + \frac{v^2}{2B} + \left(\frac{A}{B} + 1\right)\left(\frac{A}{2}\varepsilon^2 + v\varepsilon\right)\right)\big);\ \ I(i) := red \\
& \cup\ ?\left(\bigwedge_j I(j) = red\right);\ \ I(i) := green \\
& \cup\ ?true) \\
CCtrl(i) \equiv\ & (?(I(i) = green \vee xI(i) = x(i));\ \ a(i) := A \\
& \cup\ ?(v(i) = 0 \wedge xI(i) \neq x(i));\ \ a(i) := 0 \\
& \cup\ ?(v(i) = V \wedge \\
& \qquad (I(i) = green \vee xI(i) = x(i)));\ \ a(i) := 0 \\
& \cup\ a(i) := -B) \\
dyn \equiv\ & (t := 0; x'(1) = v(1), v'(1) = a(1), \\
& \qquad x'(2) = v(2), v'(2) = a(2) \\
& \qquad \&\ v(1) \geq 0 \wedge v(2) \geq 0 \\
& \qquad \wedge v(1) \leq V \wedge v(2) \leq V \wedge t \leq \varepsilon)
\end{aligned}
$$

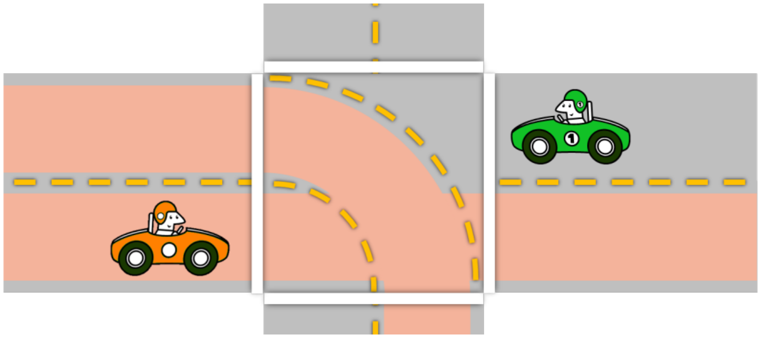
✔ Verified in KeYmaera

Initial Conditions → [Model] Requirements

Future Work

- Curved road dynamics
- Distributed car dynamics
- Combinations of merge and cross protocols
- Noisy and delayed sensor data
- Delayed braking and acceleration reaction
- Non-synchronized time
- Non-zero car lengths and lane widths

Conclusions



Challenges

- Infinite, continuous, and evolving state space, $\mathbf{R}^{\infty}$
- Simulation and testing only partially prove safety
- Continuous dynamics
- Discrete control decisions
- Large branching factor

Solutions

- We give a formal proof for a two-lane intersection with one car on each lane
- Semi-automated proof generation
- Variations in system design
- Demonstrated potential for formal safety verification in car control, even when models have high branching factor

Thank You!

SAVE ENVIRONMENT

SUSTAINABLE

SAFE

SECURE

SAVE ENERGY

IEEE

Reference

The full length paper for this research can be found here:

Sarah M. Loos and André Platzer.
Safe Intersections: At the Crossing of Hybrid Systems and Verification.
In the *14th International IEEE Conference on Intelligent Transportation Systems, ITSC 2011,Washington, D.C., USA, Proceedings, 2011*.