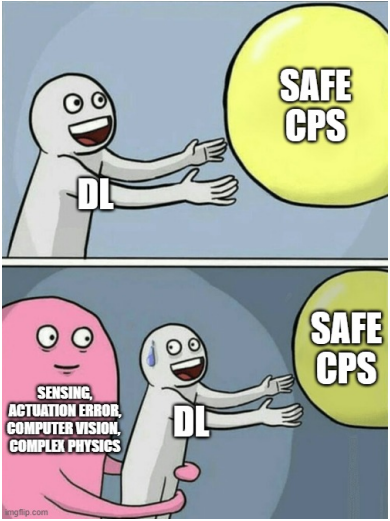
Verification, Synthesis, and Simulation

Brandon Bohrer

LFCPS

November 20, 2020

Does Anything Matter?



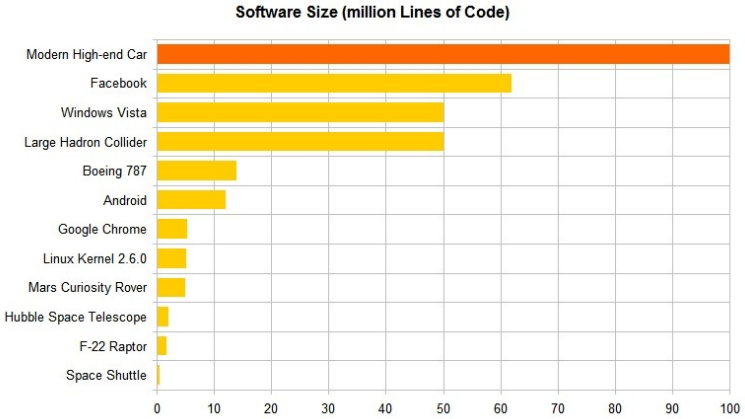
Can Model and Reality Get Along?

Hybrid Systems
Theorem Proving

velocity := *;
?(velocityOk);
{position'=...}

Cyber Physical System

Real CPS are Complex



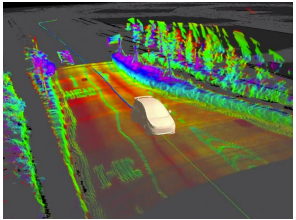
[1]

[1] https://www.linkedin.com/pulse/20140626152045-3625632-car-software-100m-lines-of-code-and-counting/

We Can't Fix Everything

[2]

[3]



[4] [WHM19]

[2] https://weather.com/science/weather-explainers/news/black-ice-winter-weather-explainer

[3] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[4] https://newsroom.intel.com/editorials/autonomous-cars-arent-dangerous-humans/

But We Can Fix a Lot

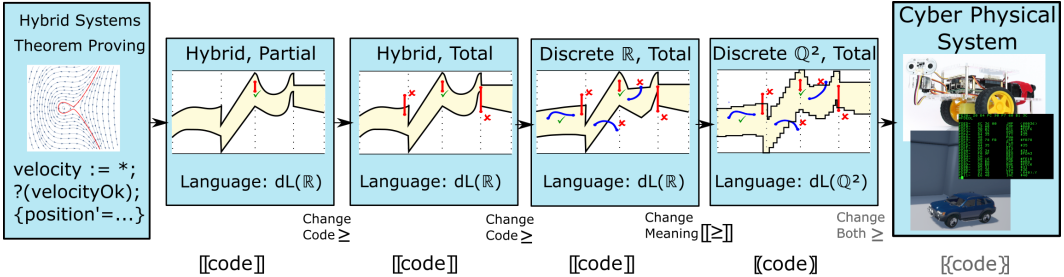
- Catch bad control choices, replace them with good ones
- Catch bad physical models during testing
- Ensure correct compilation from models to code

But We Can Fix a Lot

- Catch bad control choices, replace them with good ones
- Catch bad physical models during testing
- Ensure correct compilation from models to code

Learning Objectives: Learn how to validate models experimentally, learn to build useful simulations

VeriPhy Connects the Ends



Language changes, each semantics refines the last

Outline: Each Step Preserves Safety

$$\omega \in \underbrace{[\![[(\mathsf{ctrl};\mathsf{physics})^*]\psi]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\mathtt{total}(\mathsf{ctrl});\mathsf{physics})^*]\psi]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\mathtt{total}(\mathsf{ctrl});\mathtt{discrete}(\mathsf{physics}))^*]\psi]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$(\omega,\nu) \in \underbrace{[\![(\mathtt{total}(\mathsf{ctrl});\mathtt{discrete}(\mathsf{physics}))^*]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Uparrow$$

$$(\omega_I,\nu_I) \in \underbrace{[\![(\mathtt{total}(\mathsf{ctrl});\mathtt{discrete}(\mathsf{physics}))^*]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{Q}^2)}$$

$$\Uparrow$$

$$(\omega_I,\nu_I) \in \underbrace{\{\!|\mathtt{Compile}((\mathtt{total}(\mathsf{ctrl}),\mathtt{discrete}(\mathsf{physics}))^*)|\!\}}_{\mathsf{ARM\ or\ x64}}$$

$$\Rightarrow \quad \nu \in [\![\psi]\!]$$

Real arithmetic, hybrid, trusted control

Real arithmetic, hybrid, untrusted control

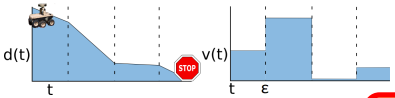
Real arithmetic, discrete, untrusted control

Real arithmetic, discrete, untrusted control

Interval arith., discrete, untrusted control

Interval word arithmetic, machine-executable

Example: 1D Car



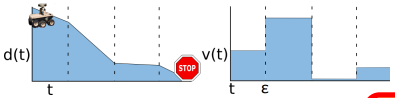
$$\text{safe} \equiv (\text{init} \rightarrow [\alpha]d \geq 0)$$

Never exceed destination

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{\textit{control}};\ t := 0;$$

$$\overbrace{\{d' = -v,\ t' = 1 \,\&\, t \leq \varepsilon\}@\text{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{\textit{physics}}\Big)^*$$

Example: 1D Car



Never exceed destination

$$\text{safe} \equiv (\text{init} \rightarrow [\alpha]d \geq 0)$$

Velocity chosen

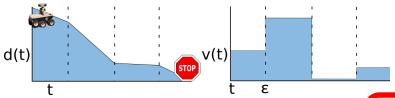
Far Enough?

Velocity Envelope

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{\textit{control}};\ t := 0;$$

$$\overbrace{\{d' = -v,\ t' = 1 \,\&\, t \leq \varepsilon\}@\text{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{\textit{physics}}\Big)^*$$

Example: 1D Car



$$\text{safe} \equiv (\text{init} \rightarrow [\alpha]d \geq 0)$$

Never exceed destination

Velocity chosen

Far Enough?

Velocity Envelope

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{\textit{control}};\ t := 0;$$

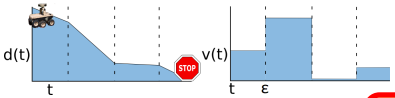
$$\overbrace{\{d' = -v,\ t' = 1\ \&\ t \leq \varepsilon\}@\text{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{\textit{physics}}\Big)^*$$

Physics

Constraint

Repeat

Example: 1D Car



Never exceed destination

$$\text{safe} \equiv (\text{init} \rightarrow [\alpha]d \geq 0)$$

Velocity chosen

Far Enough?

Velocity Envelope

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{\textit{control}};\ t := 0;$$

$$\overbrace{\{d' = -v,\ t' = 1\ \&\ t \leq \varepsilon\}@\text{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{\textit{physics}}\Big)^*$$

Physics

Constraint

Invariant

Repeat

Sandbox Makes Control Total

- Controller model trusts implementation to choose safe velocity v.
- Sandbox `total`(ctrl) uses fallback if v unsafe.
- Fallback changes execution but not denotation! ($[\![\text{control} \cup \text{fallback}]\!] = [\![\text{control}]\!]$)

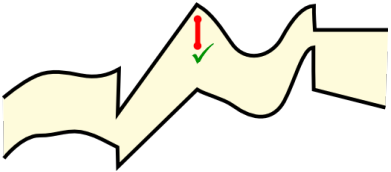
$$\omega \in \underbrace{[\![[(\text{ctrl}; \text{phys})^*]\psi]\!]}_{\text{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\texttt{total}(\text{ctrl}); \text{phys})^*]\psi]\!]}_{\text{d}\mathcal{L}\ (\mathbb{R})}$$

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{control};\ t := 0;$$

$$\overbrace{\{d' = -v,\ t' = 1\ \&\ t \leq \varepsilon\}@\text{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{physics}\Big)^*$$



$$v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V$$

$$\rightsquigarrow$$

$$v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V \cup \overbrace{v := 0}^{fallback}$$

Sandbox Makes Control Total

- Controller model trusts implementation to choose safe velocity v.
- Sandbox `total`(ctrl) uses fallback if v unsafe.
- Fallback changes execution but not denotation! ($[\![\text{control} \cup \text{fallback}]\!] = [\![\text{control}]\!]$)

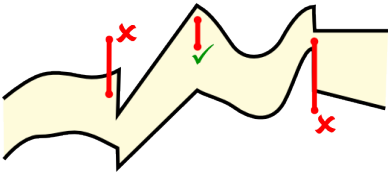
$$\omega \in \underbrace{[\![[(\text{ctrl}; \text{phys})^*]\psi]\!]}_{\text{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\texttt{total}(\text{ctrl}); \text{phys})^*]\psi]\!]}_{\text{d}\mathcal{L}\ (\mathbb{R})}$$

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{\textit{control}};\ t := 0;$$

$$\overbrace{\{d' = -v,\ t' = 1 \,\&\, t \leq \varepsilon\}@\text{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{\textit{physics}}\Big)^*$$



$$v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V$$

$$\rightsquigarrow$$

$$v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V \cup \overbrace{v := 0}^{\textit{fallback}}$$

$\boxed{\texttt{total}(\text{ctrl})}$

Invariants Make ODEs Go

- Differential equations are hard to compute
- Exact solutions are not met by real sensors
- Invariants are computable, monitorable, safe

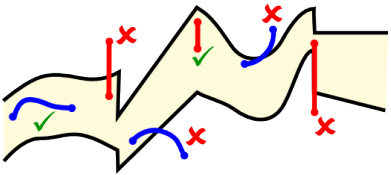
$$\omega \in \underbrace{[\![[(\mathtt{total}(\mathtt{ctrl}); \mathtt{phys})^*]\psi]\!]}_{\mathrm{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\mathtt{total}(\mathtt{ctrl}); \mathtt{mon}(\mathtt{phys}))^*]\psi]\!]}_{\mathrm{d}\mathcal{L}\ (\mathbb{R})}$$

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{\textit{control}};\ t := 0;$$

$$\overbrace{\{d' = -v,\ t' = 1\ \&\ t \leq \varepsilon\}@\mathrm{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{\textit{physics}}\Big)^*$$



$$d' = -v,\ t' = 1 \& t \leq \varepsilon$$

$$\rightsquigarrow$$

$$d := *; t := *; ?0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v;$$

Invariants Make ODEs Go

- Differential equations are hard to compute
- Exact solutions are not met by real sensors
- Invariants are computable, monitorable, safe

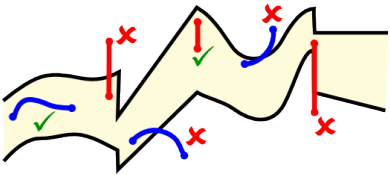
$$\omega \in \underbrace{[\![[(\texttt{total}(\texttt{ctrl}); \texttt{phys})^*]\psi]\!]}_{\mathrm{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\texttt{total}(\texttt{ctrl}); \texttt{mon}(\texttt{phys}))^*]\psi]\!]}_{\mathrm{d}\mathcal{L}\ (\mathbb{R})}$$

$$\alpha \equiv \Big(\overbrace{(v := *;\ ?d \geq \varepsilon v \wedge 0 \leq v \leq V)}^{\textit{control}};\ t := 0;$$

$$\overbrace{\{d' = -v,\ t' = 1\ \&\ t \leq \varepsilon\}@\mathrm{inv}(0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v)}^{\textit{physics}}\Big)^*$$



$$d' = -v,\ t' = 1 \& t \leq \varepsilon$$

$$\rightsquigarrow$$

$$d := *;\ t := *;\ ?0 \leq t \leq \varepsilon \wedge d \geq (\varepsilon - t) \cdot v;$$

Sense State

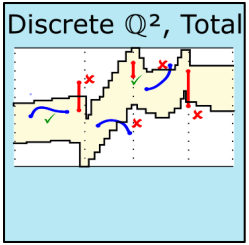
Test invariant

$\texttt{discrete}(\text{physics})$

Sandbox Now Verified

$$
\begin{array}{l}
\big(\big(\big(\; v := *; ?\mathsf{ctrlMon}(d, t, v, d^+, t^+, v^+);\big) \\
\qquad \cup\, v := 0;\big) \\
\quad t := 0; \\
\quad d := *; \;\; t := *; ?\big(0 \leq t \leq \varepsilon \wedge d \geq v(\varepsilon - t)\big)\big);\big)^*
\end{array}
$$

Intervals Make Real Numbers Rational

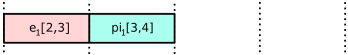


Example: Compare π and e, soundly.
Solution: Conservative interval approximation

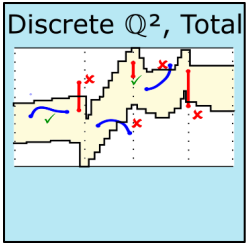
Example

Let $\nu_I = \{pi_1 \mapsto [3,4], \quad e_1 \mapsto [2,3],$
$pi_{0.1} \mapsto [3.1, 3.2], e_{0.1} \mapsto [2.7, 2.8]\}$, then

- $\nu_I[\![(pi_1 \geq e_1)]\!]$ is true ($\top$)



Intervals Make Real Numbers Rational

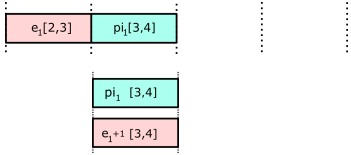


Example: Compare π and e, soundly.
Solution: Conservative interval approximation

Example

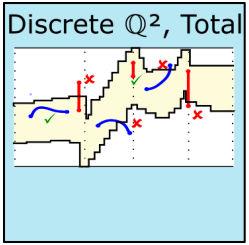
Let $\nu_I = \{pi_1 \mapsto [3,4], \quad e_1 \mapsto [2,3],$
$pi_{0.1} \mapsto [3.1, 3.2], e_{0.1} \mapsto [2.7, 2.8]\}$, then

- $\nu_I[\![(pi_1 \geq e_1)]\!]$ is true ($\top$)



- $\nu_I[\![(pi_1 \geq e_1 + 1)]\!]$ is ???

Intervals Make Real Numbers Rational

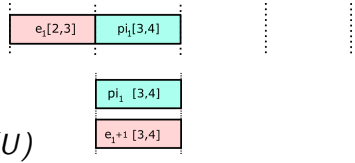


Example: Compare π and e, soundly.
Solution: Conservative interval approximation

Example

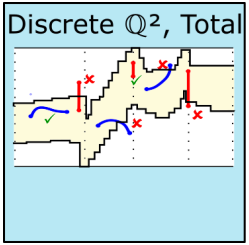
Let $\nu_I = \{pi_1 \mapsto [3,4], \quad e_1 \mapsto [2,3],$
$pi_{0.1} \mapsto [3.1, 3.2], e_{0.1} \mapsto [2.7, 2.8]\}$, then

- $\nu_I[\![(pi_1 \geq e_1)]\!]$ is true ($\top$)



- $\nu_I[\![(pi_1 \geq e_1 + 1)]\!]$ is *a known unknown (U)*

Intervals Make Real Numbers Rational

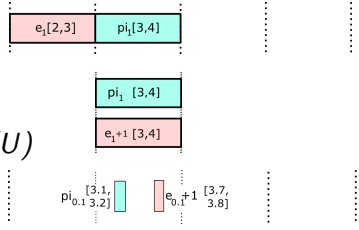


Example: Compare π and e, soundly.
Solution: Conservative interval approximation

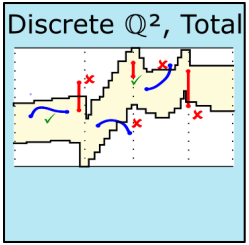
Example

Let $\nu_I = \{pi_1 \mapsto [3,4], \quad e_1 \mapsto [2,3],$
$pi_{0.1} \mapsto [3.1, 3.2], e_{0.1} \mapsto [2.7, 2.8]\}$, then

- $\nu_I[\![(pi_1 \geq e_1)]\!]$ is true ($\top$)
- $\nu_I[\![(pi_1 \geq e_1 + 1)]\!]$ is *a known unknown (U)*
- $\nu_I[\![(pi_{0.1} \geq e_{0.1} + 1)]\!]$ is false ($\bot$)



Intervals Make Real Numbers Rational

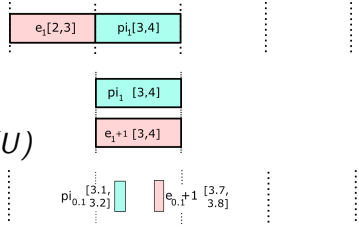


Example: Compare π and e, soundly.
Solution: Conservative interval approximation

Example

Let $\nu_I = \{pi_1 \mapsto [3,4], \quad e_1 \mapsto [2,3],$
$pi_{0.1} \mapsto [3.1, 3.2], e_{0.1} \mapsto [2.7, 2.8]\}$, then

- $\nu_I[\![(pi_1 \geq e_1)]\!]$ is true ($\top$)
- $\nu_I[\![(pi_1 \geq e_1 + 1)]\!]$ is *a known unknown (U)*
- $\nu_I[\![(pi_{0.1} \geq e_{0.1} + 1)]\!]$ is false ($\bot$)



When truth values can be unknown, formulas are *3-valued*

d$\mathcal{L}$ Has Interval Semantics

$$\omega_I[\![\theta_1 + \theta_2]\!] \;=\; [l_1 + l_2, u_1 + u_2] \text{ where } \omega_I[\![\theta_i]\!] = [l_i, u_i]$$

$\wedge$	$\top$	U	$\bot$
$\top$	$\top$	U	$\bot$
U	U	U	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

$\vee$	$\top$	U	$\bot$
$\top$	$\top$	$\top$	$\top$
U	$\top$	U	U
$\bot$	$\top$	U	$\bot$

$$\omega_I[\![\theta_1 < \theta_2]\!] \;=\; \begin{cases} \top & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } u_1 < l_2 \\ \bot & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } l_1 \geq u_2 \\ U & \text{otherwise} \end{cases}$$

$$(\omega_I, \omega_I) \in [\![?\phi]\!] \text{ iff } \omega_I[\![\alpha]\!] = \top$$
$$(\omega_I, \nu_I) \in [\![\alpha \cup \beta]\!] \text{ iff } (\omega_I, \nu_I) \in [\![\alpha]\!] \text{ or } (\omega_I, \nu_I) \in [\![\beta]\!]$$
$$(\omega_I, \nu_I) \in [\![x := \theta]\!] \text{ iff } \nu_I = \omega_I[x \mapsto \omega_I[\![\theta]\!]]$$

d$\mathcal{L}$ Has Interval Semantics

$$\omega_I[\![\theta_1 + \theta_2]\!] \;=\; [l_1 + l_2, u_1 + u_2] \text{ where } \omega_I[\![\theta_i]\!] = [l_i, u_i]$$

Value of term θ is an interval

$\wedge$	$\top$	U	$\bot$
$\top$	$\top$	U	$\bot$
U	U	U	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

$\vee$	$\top$	U	$\bot$
$\top$	$\top$	$\top$	$\top$
U	$\top$	U	U
$\bot$	$\top$	U	$\bot$

$$\omega_I[\![\theta_1 < \theta_2]\!] \;=\; \begin{cases} \top & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } u_1 < l_2 \\ \bot & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } l_1 \geq u_2 \\ U & \text{otherwise} \end{cases}$$

$$(\omega_I, \omega_I) \in [\![?\phi]\!] \text{ iff } \omega_I[\![\alpha]\!] = \top$$

$$(\omega_I, \nu_I) \in [\![\alpha \cup \beta]\!] \text{ iff } (\omega_I, \nu_I) \in [\![\alpha]\!] \text{ or } (\omega_I, \nu_I) \in [\![\beta]\!]$$

$$(\omega_I, \nu_I) \in [\![x := \theta]\!] \text{ iff } \nu_I = \omega_I[x \mapsto \omega_I[\![\theta]\!]]$$

d$\mathcal{L}$ Has Interval Semantics

$$\omega_I[\![\theta_1 + \theta_2]\!] \;=\; [l_1 + l_2, u_1 + u_2] \text{ where } \omega_I[\![\theta_i]\!] = [l_i, u_i]$$

Value of term θ is an interval

$\wedge$	$\top$	U	$\bot$
$\top$	$\top$	U	$\bot$
U	U	U	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

$\vee$	$\top$	U	$\bot$
$\top$	$\top$	$\top$	$\top$
U	$\top$	U	U
$\bot$	$\top$	U	$\bot$

3-valued truth tables for propositional ϕ

$$\omega_I[\![\theta_1 < \theta_2]\!] \;=\; \begin{cases} \top & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } u_1 < l_2 \\ \bot & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } l_1 \geq u_2 \\ U & \text{otherwise} \end{cases}$$

$$(\omega_I, \omega_I) \in [\![?\phi]\!] \text{ iff } \omega_I[\![\alpha]\!] = \top$$

$$(\omega_I, \nu_I) \in [\![\alpha \cup \beta]\!] \text{ iff } (\omega_I, \nu_I) \in [\![\alpha]\!] \text{ or } (\omega_I, \nu_I) \in [\![\beta]\!]$$

$$(\omega_I, \nu_I) \in [\![x := \theta]\!] \text{ iff } \nu_I = \omega_I[x \mapsto \omega_I[\![\theta]\!]]$$

d$\mathcal{L}$ Has Interval Semantics

$$\omega_I[\![\theta_1 + \theta_2]\!] \;=\; [l_1 + l_2, u_1 + u_2] \text{ where } \omega_I[\![\theta_i]\!] = [l_i, u_i]$$

Value of term θ is an interval

$\wedge$	$\top$	U	$\bot$
$\top$	$\top$	U	$\bot$
U	U	U	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

$\vee$	$\top$	U	$\bot$
$\top$	$\top$	$\top$	$\top$
U	$\top$	U	U
$\bot$	$\top$	U	$\bot$

3-valued truth tables for propositional ϕ

$$\omega_I[\![\theta_1 < \theta_2]\!] \;=\; \begin{cases} \top & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } u_1 < l_2 \\ \bot & \text{if } \omega_I[\![\theta_i]\!] = (l_i, u_i) \text{ and } l_1 \geq u_2 \\ U & \text{otherwise} \end{cases}$$

Condition must be true $\top$

Initial and final state

$$(\omega_I, \omega_I) \in [\![?\phi]\!] \text{ iff } \omega_I[\![\alpha]\!] = \top$$

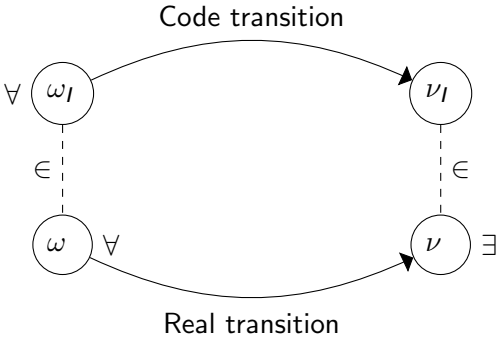
$$(\omega_I, \nu_I) \in [\![\alpha \cup \beta]\!] \text{ iff } (\omega_I, \nu_I) \in [\![\alpha]\!] \text{ or } (\omega_I, \nu_I) \in [\![\beta]\!]$$

$$(\omega_I, \nu_I) \in [\![x := \theta]\!] \text{ iff } \nu_I = \omega_I[x \mapsto \omega_I[\![\theta]\!]]$$

Interval Semantics Refines Real Semantics

Theorem (Interval Semantics Refines Real Semantics)

- *Assume* $\omega \in \omega_I$ *(Interval contains real state)*
- *Assume* $(\omega_I, \nu_I) \in [\![\alpha]\!]$ *(Interval program transitions)*
- *Then exists* $\nu \in \nu_I$ *such that* $(\omega, \nu) \in [\![\alpha]\!]$ *(New interval contains real state)*



Sandbox HP Already Verified

$$
\begin{aligned}
&\big(\big(\big(\; v := *; ?\mathsf{ctrlMon}(d, t, v, d^+, t^+, v^+);\big) \\
&\qquad \cup\, v := 0;\big) \\
&\quad t := 0; \\
&\quad d := *; \;\; t := *; ?\big(0 \leq t \leq \varepsilon \wedge d \geq v(\varepsilon - t)\big)\big);\big)^*
\end{aligned}
$$

Verified CakeML Source is Generated

CakeML source incorporates FFIs with control, actuation, sensing

```
fun cmlSandboxBody state =
   if not (stop ()) then
     state.ctrlNew:= extCtrl state;
     state.ctrl := if intervalSem ctrlMon state = ⊤
                   then state.ctrlNew
                   else fallback state;
     actuate state.ctrl;
     state.sensors:= sense ();
     if intervalSem plantMon state = ⊤ then
       Runtime.fullGC ();
       cmlSandboxBody state
     else violation "Plant Violation"
```

CakeML Sandbox is Sound

Theorem (Soundness for CakeML Sandbox, Main Case)

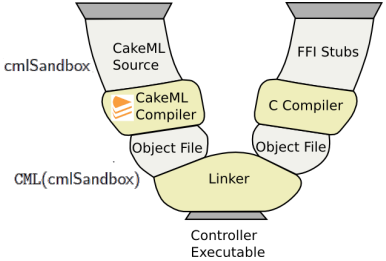
If $([\![\{\omega\}]\!], [\![\{\nu\}]\!]) \in [\![\{\mathit{cmlSandbox}\}]\!]$ *then* $([\![(\omega)]\!], [\![(\nu)]\!]) \in [\![\mathsf{sandbox}]\!]$

$$(\omega_l, \nu_l) \in \underbrace{[\![(\mathtt{total}(\mathsf{ctrl}); \mathtt{mon}(\mathsf{phys}))^*]\!]}_{\mathrm{d}\mathcal{L}\ (\mathbb{Q}^2)}$$

$$\Uparrow$$

$$(\omega_l, \nu_l) \in \underbrace{\{\!|\mathtt{EXE}((\mathtt{total}(\mathsf{ctrl}), \mathtt{mon}(\mathsf{phys}))^*)|\!\}}_{\text{ARM or x64}}$$

CakeML Compiler Preserves Guarantees



End-to-end Proof Meets in Middle

$$\omega \in \underbrace{[\![[(\mathsf{ctrl};\mathsf{physics})^*]\psi]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\mathtt{total}(\mathsf{ctrl});\mathsf{physics})^*]\psi]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Downarrow$$

$$\omega \in \underbrace{[\![[(\mathtt{total}(\mathsf{ctrl});\mathtt{discrete}(\mathsf{physics}))^*]\psi]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$(\omega,\nu) \in \underbrace{[\![(\mathtt{total}(\mathsf{ctrl});\mathtt{discrete}(\mathsf{physics}))^*]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{R})}$$

$$\Uparrow$$

$$(\omega_I,\nu_I) \in \underbrace{[\![(\mathtt{total}(\mathsf{ctrl});\mathtt{discrete}(\mathsf{physics}))^*]\!]}_{\mathsf{d}\mathcal{L}\ (\mathbb{Q}^2)}$$

$$\Uparrow$$

$$(\omega_I,\nu_I) \in \underbrace{\{\!|\mathtt{Compile}((\mathtt{total}(\mathsf{ctrl}),\mathtt{discrete}(\mathsf{physics}))^*)|\!\}}_{\text{ARM or x64}}$$

$$\Rightarrow \quad \nu \in [\![\psi]\!]$$

Real arithmetic, hybrid, trusted control

Real arithmetic, hybrid, untrusted control

Real arithmetic, discrete, untrusted control

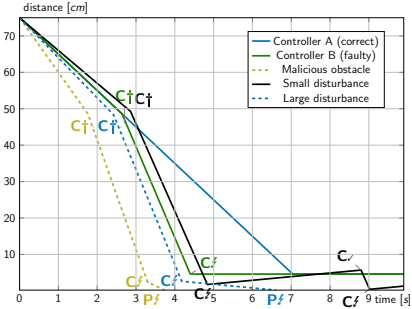
Real arithmetic, discrete, untrusted control

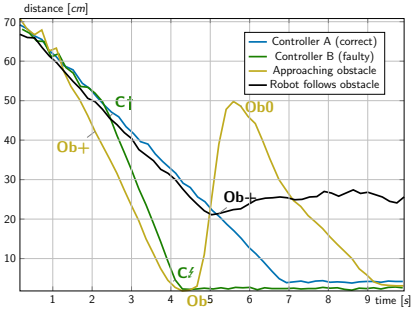
Interval arith., discrete, untrusted control

Interval word arithmetic, machine-executable

1D Evaluated in Hardware and Simulation

Sandbox Catches Bad Controller
Sandbox Catches Bad Obstacles





Control Fault **C↯**, Plant Fault **P↯**, Control Spike **C†**, Obstacle Motion **Ob**

Simulation Hardware

Let's look at 1D code

Reminder: Interface

Table: External functions and their intended meaning

External func.	Intended Meaning
`ffiConst`	Get the values of system constants
`ffiSense`	Get the current sensor readings
`ffiExtCtrl`	Get the next (untrusted) control decision
`ffiActuate`	Actuate a control decision
`ffiStop`	Check whether to run more control cycles
`ffiViolation`	Exit control loop due to a fatal violation

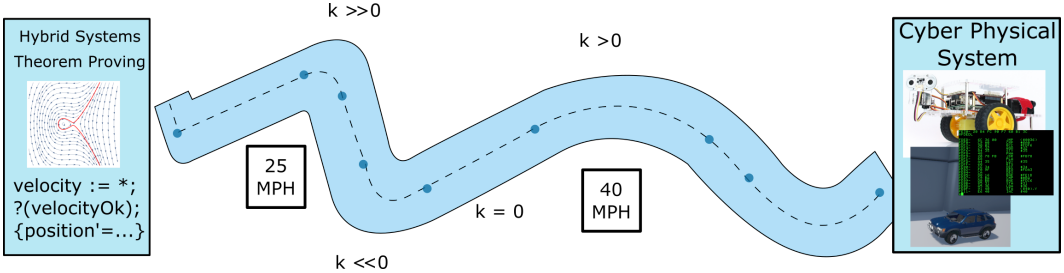
What about 2D?

Hybrid Systems
Theorem Proving

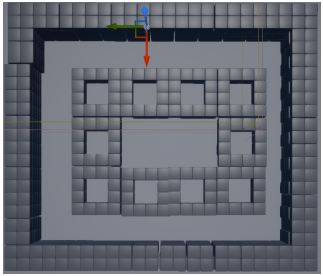
velocity := *;
?(velocityOk);
{position'=...}

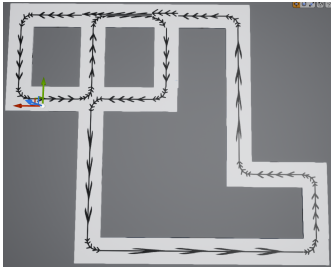
Cyber Physical System

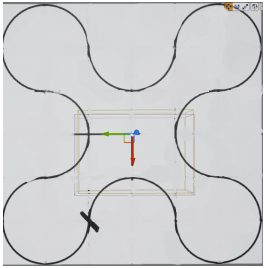
Waypoint Model Makes 2D Possible



AirSim Environments



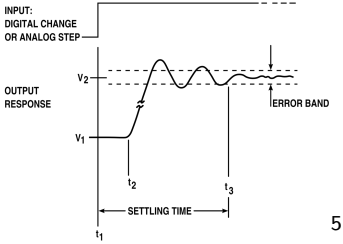




PD Controllers Control Car

- *Feedback control* chooses control value (steering) based on difference between current state and desired *velocity setpoint*
- *Proportional* term considers distance Δx to pathway with proportion c_x
- *Derivative* term considers derivative (orientation) *dir* with proportion c_{dir}

$$steer = \Delta x \cdot c_x + dir \cdot c_{dir}$$



[5]

[5] https://en.wikipedia.org/wiki/Settling_time

Evaluation

	Avg. Speed (m/s)				
World	BB	**PD1**	PD2	PD3	Human
Rect	4.3	**6.32**	7.16	12.6	9.92
Turns	3.78	**3.95**	4.43	4.69	9.66
Clover	X	**29.5**	29.5	29.5	28.9

	Ctrl Fail.				
World	BB	**PD1**	PD2	PD3	Human
Rect	0.5%	**0.1%**	0.1%	0.19%	1.14%
Turns	1.0%	**1.0%**	1.1%	4.7%	3.61%
Clover	X	**0.2%**	0.2%	0.19%	0.29%

	Plant Fail.				
World	BB	**PD1**	PD2	PD3	Human
Rect	36.8%	**8.23%**	8.5%	14%	41.3%
Turns	18.6%	**3.95%**	6.8%	11%	21.1%
Clover	X	**66%**	66%	66%	48%

Let's look at 2D code

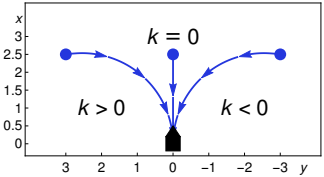
Conclusion

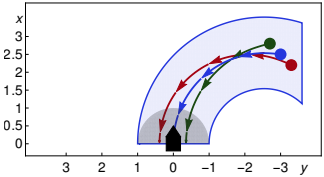
- We know to model idealized CPS, ready to go further
- Sandboxes + compilation bridge correct models to correct implementation
- Simulation + Experiments also validate model
- Simulations should be independent from model

References I

Benjamin Wilson, Judy Hoffman, and Jamie Morgenstern, *Predictive inequity in object detection*, CoRR **abs/1902.11097** (2019).

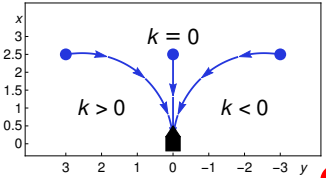
Game Models Driving

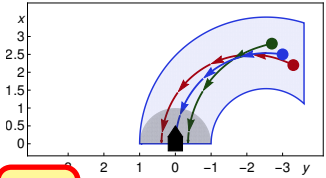




$$
\begin{aligned}
\alpha^* &\equiv (\text{input}; \text{ctrl}; \text{physics})^* \\
\text{input} &\equiv (x, y) := *;\ [vl, vh] := *;\ k := *;\ ?\text{Feas} \\
\text{ctrl} &\equiv (a := *; ?\text{Feas})^d \\
\text{physics} &\equiv \mathrm{t} := 0;\ \Big\{\mathrm{t}' = 1,\ v' = a,\ \mathrm{x}' = v\mathrm{k}\left(\mathrm{y} - \frac{1}{\mathrm{k}}\right),\ \mathrm{y}' = v\mathrm{k}\,(-\mathrm{x}), \\
&\qquad \&\ \mathrm{t} \leq T \ \wedge\ v \geq 0\Big\}
\end{aligned}
$$

Game Models Driving





Loop

$$\alpha^* \equiv (\text{input}; \text{ctrl}; \text{physics})^*$$

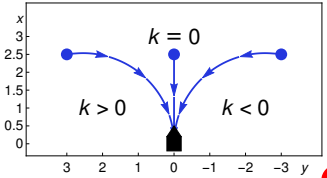
$$\text{input} \equiv (x, y) := *;\ [vl, vh] := *;\ k := *;\ ?\text{Feas}$$

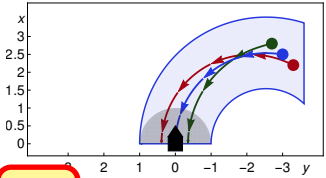
$$\text{ctrl} \equiv (a := *; ?\text{Feas})^d$$

$$\text{physics} \equiv \mathrm{t} := 0;\ \Big\{\mathrm{t}' = 1,\ v' = a,\ \mathrm{x}' = v\mathrm{k}\left(\mathrm{y} - \frac{1}{\mathrm{k}}\right),\ \mathrm{y}' = v\mathrm{k}\,(-\mathrm{x}),$$

$$\&\ \mathrm{t} \leq T \ \wedge\ v \geq 0\Big\}$$

Game Models Driving





Loop

Read value

Assume test

$$\alpha^* \equiv (\text{input}; \text{ctrl}; \text{physics})^*$$

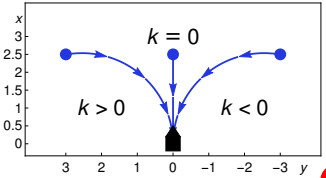
$$\text{input} \equiv (x, y) := *;\ [vl, vh] := *;\ k := *;\ ?\text{Feas}$$

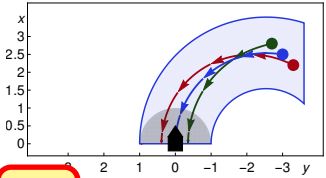
$$\text{ctrl} \equiv (a := *; ?\text{Feas})^d$$

$$\text{physics} \equiv \text{t} := 0;\ \Big\{\text{t}' = 1,\ v' = a,\ \text{x}' = v\text{k}\left(\text{y} - \frac{1}{\text{k}}\right),\ \text{y}' = v\text{k}\,(-\text{x}),$$

$$\&\ \text{t} \leq T \ \wedge\ v \geq 0\Big\}$$

Game Models Driving





Loop

Read value

Assume test

Switch players: Write value, assert test

$$\alpha^* \equiv (\text{input}; \text{ctrl}; \text{physics})^*$$

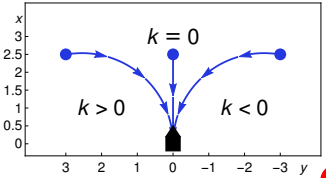
$$\text{input} \equiv (x, y) := *;\ [vl, vh]$$

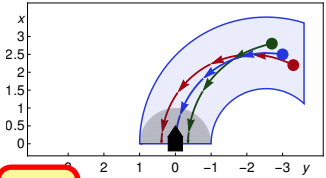
$$\text{ctrl} \equiv (a := *; ?\text{Feas})^d$$

$$\text{physics} \equiv \text{t} := 0;\ \Big\{\text{t}' = 1,\ v' = a,\ \text{x}' = vk\left(\text{y} - \frac{1}{\text{k}}\right),\ \text{y}' = vk\,(-\text{x}),$$

$$\&\ \text{t} \leq T \ \wedge\ v \geq 0\Big\}$$

Game Models Driving





Loop

Read value

Assume test

Switch players: Write value, assert test

Init timer

$$\alpha^* \equiv (\text{input}; \text{ctrl}; \text{physics})^*$$

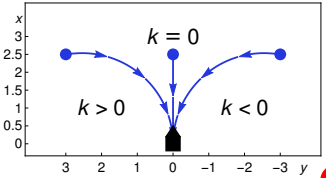
$$\text{input} \equiv (x, y) := *;\ [vl, vh]$$

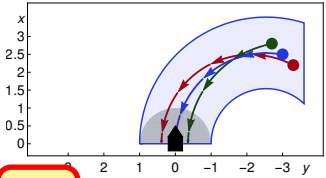
$$\text{ctrl} \equiv (a := *; ?\text{Feas})^d$$

$$\text{physics} \equiv \mathrm{t} := 0;\ \left\{\mathrm{t}' = 1,\ v' = a,\ \mathrm{x}' = v\mathrm{k}\left(\mathrm{y} - \frac{1}{\mathrm{k}}\right),\ \mathrm{y}' = v\mathrm{k}\,(-\mathrm{x}),\right.$$

$$\left.\&\ \mathrm{t} \leq T \ \wedge\ v \geq 0\right\}$$

Game Models Driving





Loop

Read value

Assume test

Switch players: Write value, assert test

Init timer

Evolve physics

$$\alpha^* \equiv (\text{input}; \text{ctrl}; \text{physics})^*$$

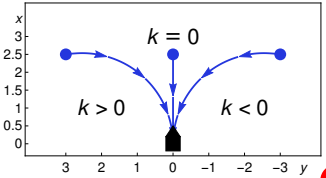
$$\text{input} \equiv (x, y) := *;\ [vl, vh]$$

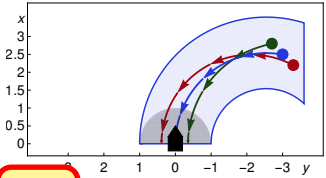
$$\text{ctrl} \equiv (a := *; ?\text{Feas})^d$$

$$\text{physics} \equiv \text{t} := 0;\ \left\{\text{t}' = 1,\ v' = a,\ \text{x}' = v\text{k}\left(\text{y} - \frac{1}{\text{k}}\right),\ \text{y}' = v\text{k}\,(-\text{x}),\right.$$

$$\left.\&\ \text{t} \leq T \ \wedge\ v \geq 0\right\}$$

Game Models Driving





Loop

Read value

Assume test

Switch players: Write value, assert test

$$\alpha^* \equiv (\text{input}; \text{ctrl}; \text{physics})^*$$

$$\text{input} \equiv (x, y) := *;\ [vl, vh]$$

$$\text{ctrl} \equiv (a := *; ?\text{Feas})^d$$

$$\text{physics} \equiv \text{t} := 0;\ \{\text{t}' = 1,\ v' = a,\ \text{x}' = vk\ \left(\text{y} - \frac{1}{\cdot}\right),\ \text{y}' = vk\ (-\text{x}),$$

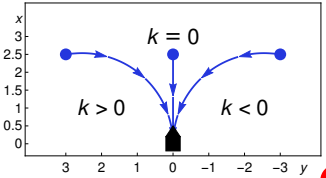
$$\&\ \text{t} \leq T\ \wedge\ v \geq 0\}$$

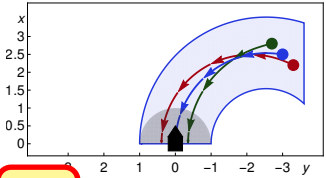
Init timer

Constraint

Evolve physics

Game Models Driving





Loop

Read value

Assume test

Switch players: Write value, assert test

Init timer

Constraint

Evolve physics

$$\alpha^* \equiv (\text{input}; \text{ctrl}; \text{physics})^*$$

$$\text{input} \equiv (x, y) := *;\ [vl, vh]\ :$$

$$\text{ctrl} \equiv (a := *; ?\text{Feas})^d$$

$$\text{physics} \equiv \text{t} := 0;\ \{\text{t}' = 1,\ v' = a,\ \text{x}' = v\text{k}\ \left(\text{y} - \frac{1}{\ }\right),\ \text{y}' = v\text{k}\ (-\text{x}),$$

$$\&\ \text{t} \leq T\ \wedge\ v \geq 0\}$$

$$\text{Ann} \equiv \text{Ann} \wedge \text{x}{>}0 \wedge 0{\leq}\text{vl}{<}\text{vh} \wedge \max(A, B)\ T \leq \text{vh} - \text{vl}$$

$$\text{Feas} \equiv -B \leq a \leq A$$

Goals are Safety and Liveness

$$\text{safe} \equiv \text{Inv} \wedge (\|(x,y)\| \leq \epsilon \rightarrow v \in [vl, vh])$$

$$\text{prog} \equiv \|(x,y)\| \leq \epsilon \wedge v \in [vl, vh]$$

$$\text{Safe} \equiv [(\text{input}; \text{ctrl}; \text{physics})^*]\text{safe}$$

$$\text{Live} \equiv [(\text{input}; \text{ctrl}; (\text{physics}^d))^\times]\text{prog}$$

Goals are Safety and Liveness

They move first

$$\text{safe} \equiv \text{Inv} \wedge (\|(x,y)\| \leq \epsilon \rightarrow v \in [vl, vh])$$

$$\text{prog} \equiv \|(x,y)\| \leq \epsilon \wedge v \in [vl, vh]$$

$$\text{Safe} \equiv [(\text{input}; \text{ctrl}; \text{physics})^*]\text{safe}$$

$$\text{Live} \equiv [(\text{input}; \text{ctrl}; (\text{physics}^d))^\times]\text{prog}$$

Goals are Safety and Liveness

$$\text{safe} \equiv \text{Inv} \wedge (\|(x,y)\| \leq \epsilon \rightarrow v \in [vl, vh])$$

$$\text{prog} \equiv \|(x,y)\| \leq \epsilon \wedge v \in [vl, vh]$$

$$\text{Safe} \equiv [(\text{input}; \text{ctrl}; \text{physics})^*]\text{safe}$$

$$\text{Live} \equiv [(\text{input}; \text{ctrl}; (\text{physics}^d))^\times]\text{prog}$$

They move first

They control loop

Goals are Safety and Liveness

$$\text{safe} \equiv \text{Inv} \wedge (\|(x,y)\| \leq \epsilon \rightarrow v \in [vl, vh])$$

$$\text{prog} \equiv \|(x,y)\| \leq \epsilon \wedge v \in [vl, vh]$$

$$\text{Safe} \equiv [(\text{input}; \text{ctrl}; \text{physics})^*]\text{safe}$$

$$\text{Live} \equiv [(\text{input}; \text{ctrl}; (\text{physics}^d))^\times]\text{prog}$$

They move first

They control loop

I control loop

Goals are Safety and Liveness

$$\text{safe} \equiv \text{Inv} \wedge (\|(x,y)\| \leq \epsilon \rightarrow v \in [vl, vh])$$

$$\text{prog} \equiv \|(x,y)\| \leq \epsilon \wedge v \in [vl, vh]$$

$$\text{Safe} \equiv [(\text{input}; \text{ctrl}; \text{physics})^*]\text{safe}$$

$$\text{Live} \equiv [(\text{input}; \text{ctrl}; (\text{physics}^d))^\times]\text{prog}$$

They move first

They control loop

I control loop

I control duration

Goals are Safety and Liveness

$$\text{safe} \equiv \text{Inv} \wedge (\|(x,y)\| \leq \epsilon \rightarrow v \in [vl, vh])$$

$$\text{prog} \equiv \|(x,y)\| \leq \epsilon \wedge v \in [vl, vh]$$

$$\text{Safe} \equiv [(\text{input}; \text{ctrl}; \text{physics})^*]\text{safe}$$

$$\text{Live} \equiv [(\text{input}; \text{ctrl}; (\text{physics}^d))^\times]\text{prog}$$

$$\text{Win} \equiv [(\text{input}; \text{ctrl}; (\text{physics}^d); ?\text{safe})^\times]\text{prog}$$

They move first

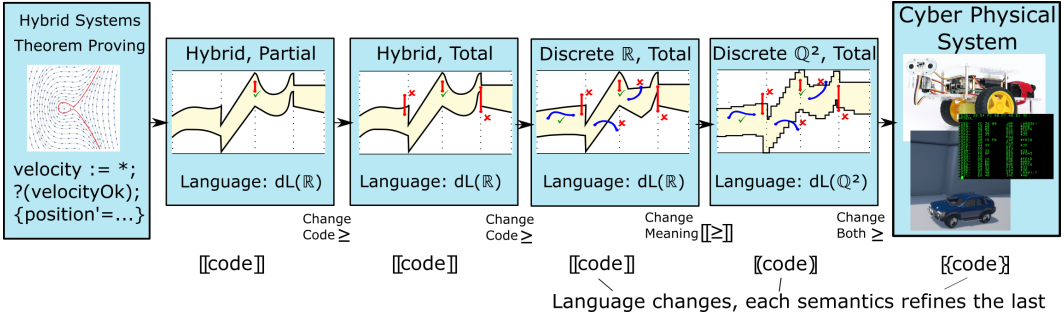
They control loop

I control loop

I control duration

Outline

Tooling Implements Verified Bridge



Each Step is a Refinement

$$\omega \in [\![[(\mathsf{ctrl}; \mathsf{physics})^*]\psi]\!]$$

Real arithmetic, hybrid, trusted control

$$\Downarrow$$

$$\omega \in [\![[(\mathtt{total}(\mathsf{ctrl}); \mathsf{physics})^*]\psi]\!]$$

Real arithmetic, hybrid, untrusted control

$$\Downarrow$$

$$\omega \in [\![[(\mathtt{total}(\mathsf{ctrl}); \mathtt{discrete}(\mathsf{physics}))^*]\psi]\!]$$

Real arithmetic, discrete, untrusted control

$$\Rightarrow \quad \nu \in [\![\psi]\!]$$

$$(\omega, \nu) \in [\![(\mathtt{total}(\mathsf{ctrl}); \mathtt{discrete}(\mathsf{physics}))^*]\!]$$

Real arithmetic, discrete, untrusted control

$$\Uparrow$$

$$(\omega_I, \nu_I) \in [\![((\mathtt{total}(\mathsf{ctrl}); \mathtt{discrete}(\mathsf{physics}))^*)]\!]$$

Interval arith., discrete, untrusted control

$$\Uparrow$$

$$(\omega_I, \nu_I) \in \{\!|\mathtt{Compile}((\mathtt{total}(\mathsf{ctrl}), \mathtt{discrete}(\mathsf{physics}))^*)|\!\}$$

Interval word arithmetic, machine-executable

Proof Consists of Refinement and Safety

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\cdots}{\mathsf{inv}(d), \mathsf{Feas} \to \mathsf{ctrl}_{sys} \leq_{[]} \mathsf{ctrl}}\ \leq I \text{ rules} \qquad \dfrac{\cdots}{\mathsf{inv}(d), \mathsf{Feas} \to [\mathsf{ctrl}_{sys}][\mathsf{physics}]\mathsf{inv}}\ [\cdot] \text{ rules}}{\mathsf{inv}(d), \mathsf{Feas} \to [\mathsf{ctrl}][(\mathsf{physics})^d]\mathsf{inv}(d - \Delta d)}\ \leq E}{\mathsf{inv}(d), \mathsf{Feas} \to [\mathsf{ctrl}; (\mathsf{physics})^d]\mathsf{inv}(d - \Delta d)}\ [;]}{\mathsf{inv}(d) \to [(\mathsf{input}; \mathsf{ctrl}; (\mathsf{physics})^d)]\mathsf{inv}(d - \Delta d)}\ [;], [:*], [?]}{[(\mathsf{input}; \mathsf{ctrl}; (\mathsf{physics})^d)^\times]\mathsf{goal}}\ [\times]
$$

Invariants Inform Controller Design

$$
\begin{aligned}
\mathsf{Inv} &\equiv v \geq 0 \wedge \mathsf{IsCircle} \wedge \mathsf{Ann} \wedge \mathsf{BoundV} \\
&\quad \wedge \mathsf{BoundXY}(v, vh, B) \wedge \mathsf{BoundXY}(vl, v, A) \\
\mathsf{IsCircle} &\equiv \varepsilon \leq \frac{1}{|\mathrm{k}|} \\
\cap_{circ} &\equiv \mathrm{k}(\mathrm{x}^2 + \mathrm{y}^2) - 2\mathrm{x} \\
\mathsf{Ann} &\equiv |\cap_{circ} - \mathrm{k}\varepsilon^2| \leq 2\varepsilon \\
\mathsf{BoundV} &\equiv 0 \leq \mathrm{vl} < \mathrm{vh} \wedge \max(A, B)T \leq \mathrm{vh} - \mathrm{vl} \\
\mathsf{BoundXY}(v_1, v_2, acc) &\equiv v_1 \leq v_2 \\
&\quad \vee (1 + |\mathrm{k}|\varepsilon)^2 \frac{v_1^2 - v_2^2}{2a} \leq \|(x, y)\|_\infty
\end{aligned}
$$

Proofs Propose Control Strategies

- Refine high-level control spec. to low-level spec: $\mathrm{ctrl}_{sys} \leq \mathrm{ctrl}$

$$
\begin{aligned}
\mathrm{input}; \mathrm{ctrl}_{sys} &\equiv (\mathrm{x}, \mathrm{y}) := *;\ [\mathrm{vl}, \mathrm{vh}] := *;\ \mathrm{k} := *;\ ?\mathrm{Feas};\ a := *;\ ?\mathrm{Go} \\
\mathrm{Go} &\equiv \mathrm{Feas} \wedge v + aT \geq 0 \\
&\wedge \Big(v \leq \mathrm{vh} \wedge v + aT \leq \mathrm{vh} \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{(v+aT)^2 - \mathrm{vh}^2}{2B} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big) \\
&\wedge \Big(\mathrm{vl} \leq v \wedge \mathrm{vl} \leq v + aT \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{\mathrm{vl}^2 - (v+aT)^2}{2A} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big)
\end{aligned}
$$

Proofs Propose Control Strategies

- Refine high-level control spec. to low-level spec: $\mathrm{ctrl}_{sys} \leq \mathrm{ctrl}$

$$
\begin{aligned}
\mathrm{input}; \mathrm{ctrl}_{sys} &\equiv (\mathrm{x}, \mathrm{y}) := *;\ [\mathrm{vl}, \mathrm{vh}] := *;\ \mathrm{k} \\
\mathrm{Go} &\equiv \mathrm{Feas} \wedge v + aT \geq 0 \\
&\wedge \Big(v \leq \mathrm{vh} \wedge v + aT \leq \mathrm{vh} \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{(v+aT)^2 - \mathrm{vh}^2}{2B} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big) \\
&\wedge \Big(\mathrm{vl} \leq v \wedge \mathrm{vl} \leq v + aT \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{\mathrm{vl}^2 - (v+aT)^2}{2A} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big)
\end{aligned}
$$

Don't go backward

Proofs Propose Control Strategies

- Refine high-level control spec. to low-level spec: $\mathrm{ctrl}_{sys} \leq \mathrm{ctrl}$

$$
\begin{aligned}
\mathrm{input}; \mathrm{ctrl}_{sys} &\equiv (\mathrm{x}, \mathrm{y}) := *;\ [\mathrm{vl}, \mathrm{vh}] := *;\ \mathrm{k} \ldots ?\mathrm{Go} \\
\mathrm{Go} &\equiv \mathrm{Feas} \wedge v + aT \geq 0 \\
&\wedge \Big(v \leq \mathrm{vh} \wedge v + aT \leq \mathrm{vh} \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{(v+aT)^2 - \mathrm{vh}^2}{2B} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big) \\
&\wedge \Big(\mathrm{vl} \leq v \wedge \mathrm{vl} \leq v + aT \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{\mathrm{vl}^2 - (v+aT)^2}{2A} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big)
\end{aligned}
$$

Don't go backward

High bound

Proofs Propose Control Strategies

- Refine high-level control spec. to low-level spec: $\mathrm{ctrl}_{sys} \leq \mathrm{ctrl}$

$$
\begin{aligned}
\mathrm{input}; \mathrm{ctrl}_{sys} &\equiv (\mathrm{x}, \mathrm{y}) := *;\ [\mathrm{vl}, \mathrm{vh}] := *;\ \mathrm{k} \ldots ?\mathrm{Go} \\
\mathrm{Go} &\equiv \mathrm{Feas} \wedge v + aT \geq 0 \\
&\wedge \Big(v \leq \mathrm{vh} \wedge v + aT \leq \mathrm{vh} \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{(v+aT)^2 - \mathrm{vh}^2}{2B} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big) \\
&\wedge \Big(\mathrm{vl} \leq v \wedge \mathrm{vl} \leq v + aT \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{\mathrm{vl}^2 - (v+aT)^2}{2A} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big)
\end{aligned}
$$

Don't go backward

High bound

Low bound

Proofs Propose Control Strategies

- Refine high-level control spec. to low-level spec: $\mathrm{ctrl}_{sys} \leq \mathrm{ctrl}$

$$
\begin{aligned}
\mathrm{input}; \mathrm{ctrl}_{sys} &\equiv (\mathrm{x}, \mathrm{y}) := *;\ [\mathrm{vl}, \mathrm{vh}] := *;\ \mathrm{k} \ldots \mathrm{Go} \\
\mathrm{Go} &\equiv \mathrm{Feas} \wedge v + aT \geq 0 \\
&\wedge \Big(v \leq \mathrm{vh} \wedge v + aT \leq \mathrm{vh} \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{(v+aT)^2 - \mathrm{vh}^2}{2B} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big) \\
&\wedge \Big(\mathrm{vl} \leq v \wedge \mathrm{vl} \leq v + aT \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{\mathrm{vl}^2 - (v+aT)^2}{2A} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big)
\end{aligned}
$$

Don't go backward

High bound

Limit already met

Low bound

Proofs Propose Control Strategies

- Refine high-level control spec. to low-level spec: $\mathrm{ctrl}_{sys} \leq \mathrm{ctrl}$

$$
\begin{aligned}
\mathrm{input}; \mathrm{ctrl}_{sys} &\equiv (\mathrm{x}, \mathrm{y}) := *;\ [\mathrm{vl}, \mathrm{vh}] := *;\ \mathrm{k} \ldots ?\mathrm{Go} \\
\mathrm{Go} &\equiv \mathrm{Feas} \wedge v + aT \geq 0 \\
&\wedge \Big(v \leq \mathrm{vh} \wedge v + aT \leq \mathrm{vh} \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{(v+aT) - \mathrm{vh}}{2B} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big) \\
&\wedge \Big(\mathrm{vl} \leq v \wedge \mathrm{vl} \leq v + aT \vee \\
&\quad (1 + |\mathrm{k}|\varepsilon)^2 \Big(vT + \frac{a}{2}T^2 + \frac{\mathrm{vl}^2 - (v+aT)^2}{2A} \Big) + \varepsilon \leq \|(\mathrm{x}, \mathrm{y})\|_\infty \Big)
\end{aligned}
$$

Don't go backward

High bound

Limit already met

Low bound

Endzone not reached

System Controller Refines Game Model

$$
\begin{array}{cl}
* & \\
\hline
\Gamma \to (\mathsf{Go}_a^{accTerm}) \wedge (\mathsf{Go} \to \mathsf{Feas})_a^{a'} & \mathbb{R} \\
\hline
\Gamma \to (\exists a\, \mathsf{Go}) \wedge (\forall a\, (\mathsf{Go} \to \mathsf{Feas})) & \exists l,\ \forall l \\
\hline
\Gamma \to (a := *;\ ?\mathsf{Go}) \leq_{[]} (a := *; ?\mathsf{Feas})^d & [:*^d] \\
\hline
\Gamma \to \mathsf{ctrl}_{sys} \leq_{[]} \mathsf{ctrl} & \text{def.}
\end{array}
$$

Refined System is Safe

$$
\dfrac{\dfrac{\dfrac{\dots}{\Gamma \to [\text{ctrl};]\mathit{lemma}}\,\vee E,\mathbb{R} \qquad \dfrac{\dots}{\mathit{lemma} \to [(\text{physics})^d]\text{inv}(d - \Delta d)}\,\text{ODE safety}}{\Gamma \to [\text{ctrl}_{sys}][(\text{physics})^d]\text{inv}(d - \Delta d)}\,M[\cdot]}{\Gamma \to [\text{ctrl}_{sys}; (\text{physics})^d]\text{inv}(d - \Delta d)}\,[;]
$$