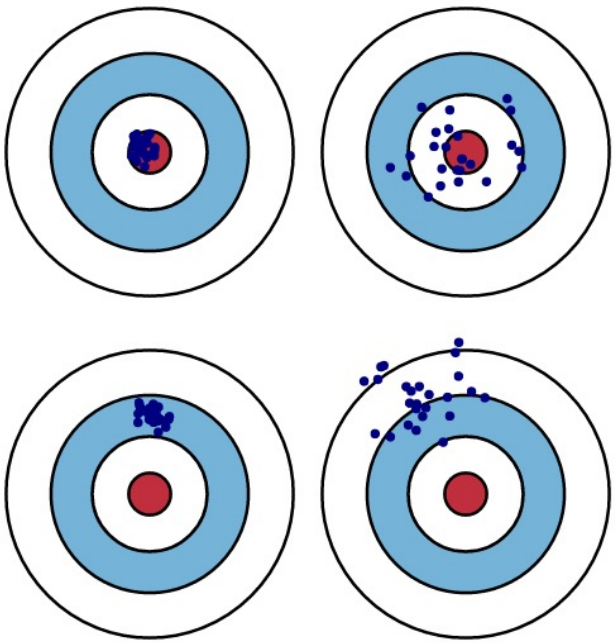
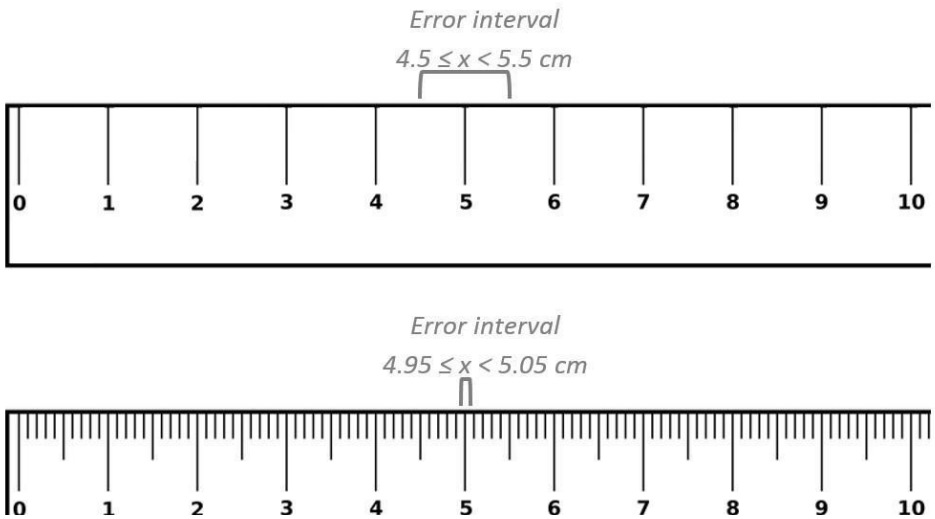
Controller Aware dL

Josh Clune (jclune@andrew.cmu.edu)





A Typical Story

The World

A Typical Story

The World

Cyber-Physical System

A Typical Story

The World

Goal

Cyber-Physical System

A Typical Story

Cyber-Physical Systems consider their environment

The World → Cyber-Physical System

Goal

A Typical Story

Cyber-Physical Systems consider their environment

The World

Goal

Cyber-Physical System

Cyber-Physical Systems affect the world

A Typical Story

Cyber-Physical Systems consider their environment

The World

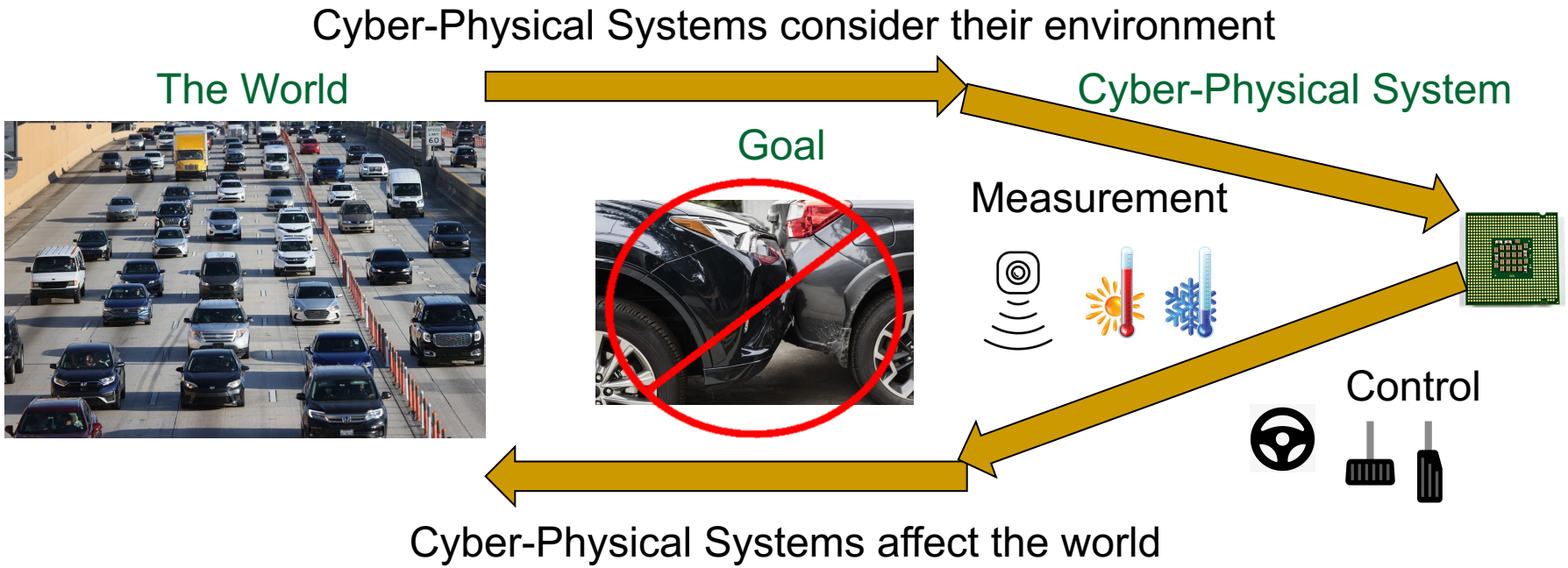
Cyber-Physical System

Goal

Cyber-Physical Systems affect the world

- Opportunities for Error:
  - Assumptions about the world
  - Implementing the cyber-physical system
  - Defining and proving the goal

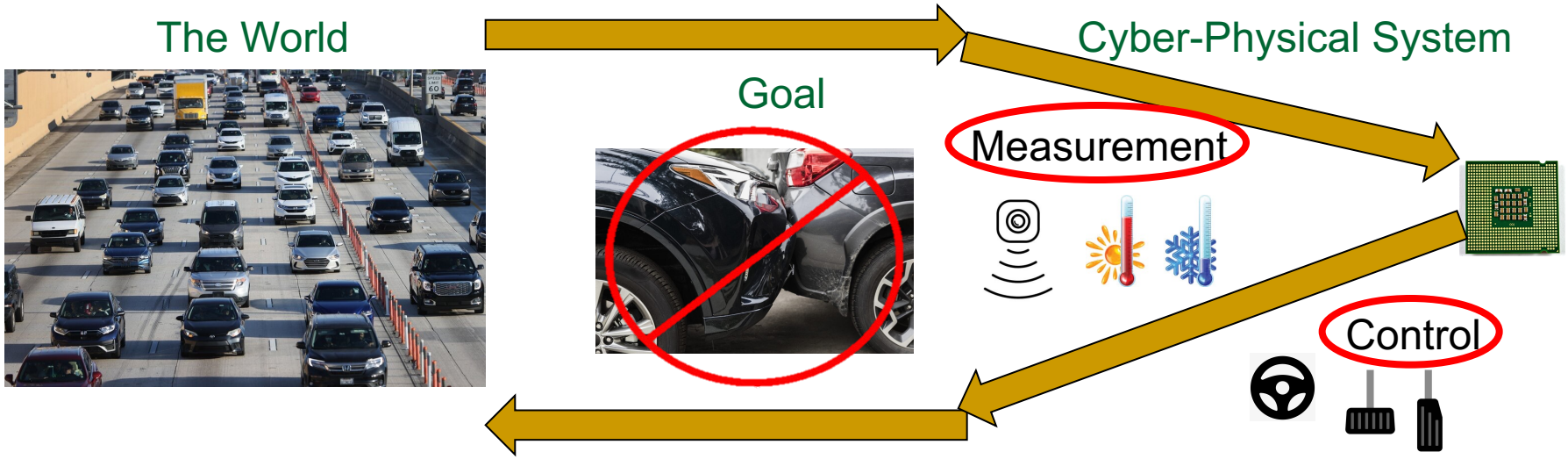
A Typical Story



- Opportunities for Error:
  - Assumptions about the world
  - Implementing the cyber-physical system
  - Defining and proving the goal

A Typical Story

Cyber-Physical Systems consider their environment



Cyber-Physical Systems affect the world

- Opportunities for Error:
  - Assumptions about the world
  - Implementing the cyber-physical system
  - Defining and proving the goal

Measurement and control phenomena are also opportunities for error

Motivation for Controller Aware dL

- Measurement and control phenomena exist in practically all cyber-physical systems
- All hardware is imperfect
- Modeling these imperfections is a fundamental problem
- Controller Aware dL is meant to make modeling hardware imperfections easier

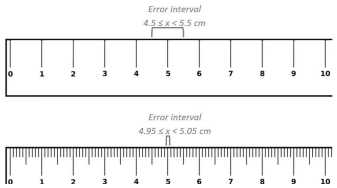
Goals for Controller Aware dL

- Assumptions about hardware imperfections should be explicit and easily extractable
- Reasoning about hardware imperfections should be separate from reasoning about the rest of the model
- Controller Aware dL should only reduce conceptual overhead

Measurable/Controllable Variables

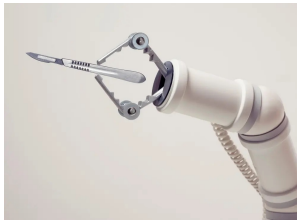
Measurable

Variables the CPS uses hardware to estimate



Controllable

Variables that the CPS uses hardware to approximately control



Syntax of Controller Aware dL

$$\text{term} \quad e \quad ::= \quad x \mid c \mid e_1 + e_2 \mid e_1 * e_2 \mid \sim x$$

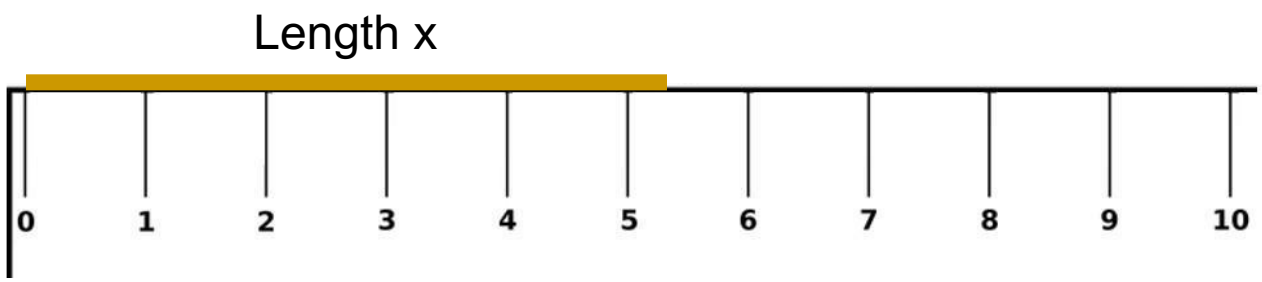
$$\text{formula} \quad P, Q \quad ::= \quad e_1 = e_2 \mid e_1 \leq e_2 \mid \neg P \mid P \wedge Q \mid$$
$$P \vee Q \mid P \rightarrow Q \mid \forall x P \mid \exists x P \mid \langle \alpha \rangle P \mid [\alpha] P$$

$$\text{hybrid program} \quad \alpha, \beta \quad ::= \quad x := e \mid x := * \mid ?P \mid x' = e \;\&\; P \mid$$
$$\alpha \cup \beta \mid \alpha; \beta \mid \alpha^* \mid \text{measure } x \mid \text{set } x \; e$$

Approximating Measurable Variables

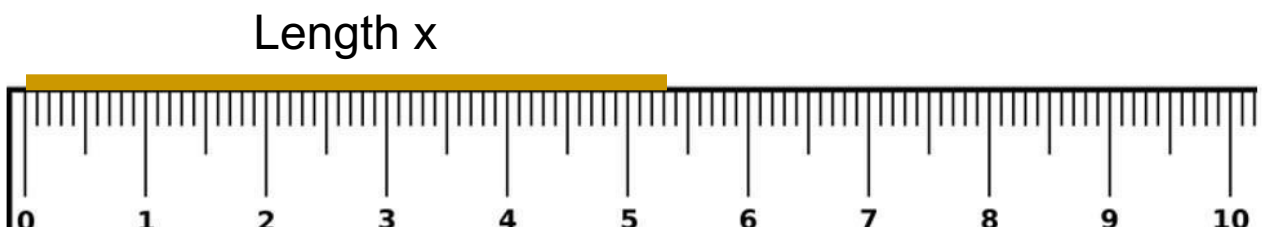
Length x

Approximating Measurable Variables



~x is between 5 and 6

Approximating Measurable Variables



~x is between 5.3 and 5.4

Approximating Measurable Variables

- ~x has some value in a range [a, b]
- The exact value of ~x is nondeterministically chosen

Approximating Measurable Variables

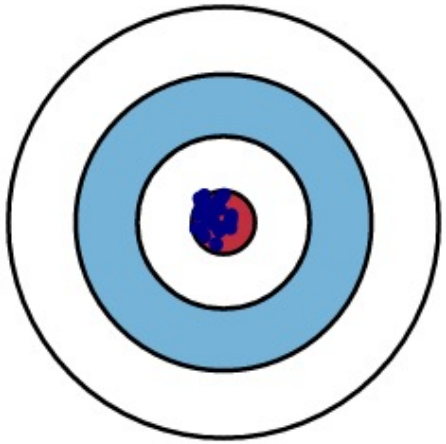
- ~x has some value in a range [a, b]
- The exact value of ~x is nondeterministically chosen
- $(\sim x)^2$ should always be positive
  - $(\sim x)^2$ should also always equal ~x*~x

Approximating Measurable Variables

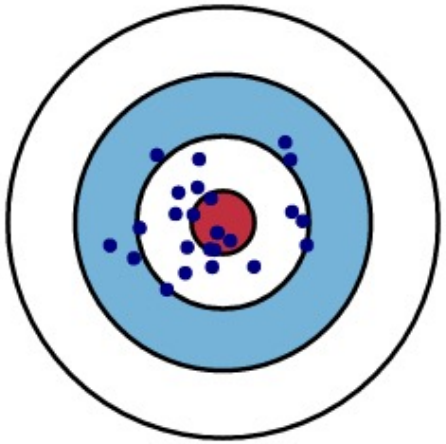
- ~x has some value in a range [a, b]
- The exact value of ~x is nondeterministically chosen
- $(\sim x)^2$ should always be positive
  - $(\sim x)^2$ should also always equal ~x*~x
- The exact value of ~x should be chosen when the programmer wants. This is what “measure x” is for

Setting Controllable Variables

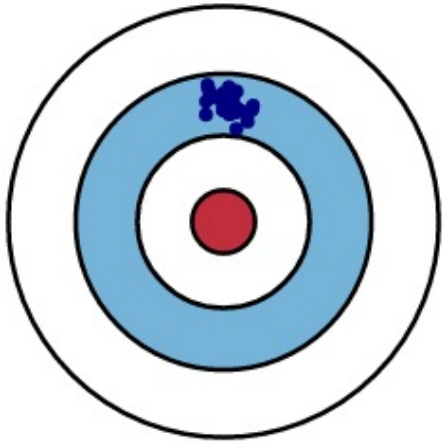
No wind



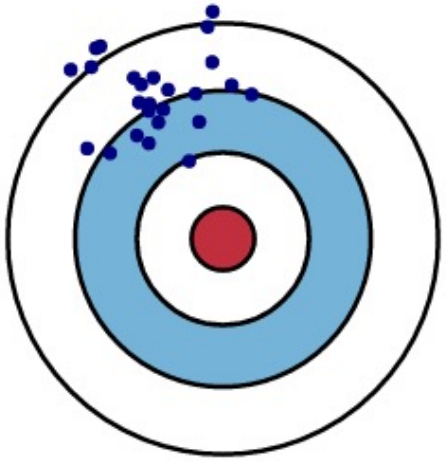
Weak, gusty wind



Consistent wind



Strong, gusty wind



Setting Controllable Variables

- x := e assigns x the value of e exactly
- “set x e” assigns x the approximate value of e
- After “set x e”, x has a value in a range [a, b]
- The exact value of x is nondeterministically chosen

Restrictions on Ranges

- How should we define these ranges of uncertainty?

Restrictions on Ranges

- How should we define these ranges of uncertainty?

- For each variable x, pick real values ε_{x1} and ε_{x2} and use the range $[x - \varepsilon_{x1}, x + \varepsilon_{x2}]$

Restrictions on Ranges

- How should we define these ranges of uncertainty?

- For each variable x, pick real values ε_{x1} and ε_{x2} and use the range $[x - \varepsilon_{x1}, x + \varepsilon_{x2}]$
  - We may want ε_{x1} and ε_{x2} to depend on x

Restrictions on Ranges

- How should we define these ranges of uncertainty?

- For each variable x, pick real values ε_{x1} and ε_{x2} and use the range $[x - \varepsilon_{x1}, x + \varepsilon_{x2}]$
  - We may want ε_{x1} and ε_{x2} to depend on x

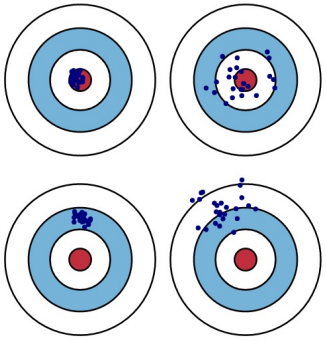
- For each variable x, pick expression e_1 and e_2 and use the range $[e_1, e_2]$

Restrictions on Ranges

- How should we define these ranges of uncertainty?

- For each variable x, pick real values ε_{x1} and ε_{x2} and use the range $[x - \varepsilon_{x1}, x + \varepsilon_{x2}]$
  - We may want ε_{x1} and ε_{x2} to depend on x

- For each variable x, pick expression e_1 and e_2 and use the range $[e_1, e_2]$
  - We may want the range to depend on the environment in a way that isn't expressible at the term level



Restrictions on Ranges

- For each variable x, define the range [a, b] in terms of dL hybrid programs α and β

- $[e_1, e_2]$ represented as:
  - $\alpha = (\sim x := e_1)$, $\beta = (\sim x := e_2)$

- $[e_1, e_2]$ if it's raining hard, $[e_3, e_4]$ otherwise
  - $\alpha = (?is\_raining; (\sim x := e_1)) \cup (?(\neg is\_raining); (\sim x := e_3))$
  - $\beta = (?is\_raining; (\sim x := e_2)) \cup (?(\neg is\_raining); (\sim x := e_4))$

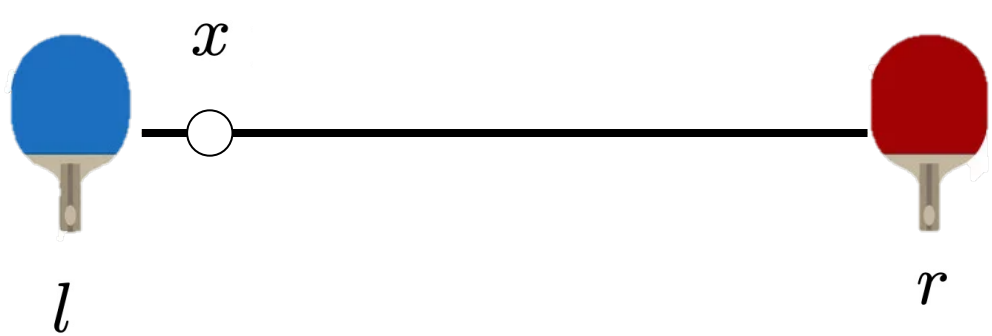
A Simple Example: Ping Pong in 1D

$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

$$[(\textbf{if}(x + vT < l \wedge v \leq 0 \vee x + vT > r \wedge v \geq 0)\ \textbf{then}\ v := -v;$$

$$t := 0; \{x' = v, t' = 1\ \&\ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



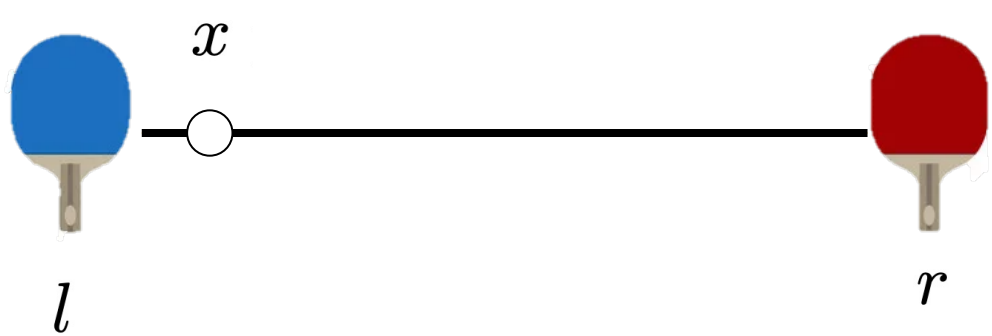
A Simple Example: Ping Pong in 1D

$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

$$[(\textbf{if}(x + vT < l \wedge v \leq 0 \vee x + vT > r \wedge v \geq 0)\ \textbf{then}\ \underline{v := -v};$$

$$t := 0; \{x' = v, t' = 1\ \&\ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



A Simple Example: Ping Pong in 1D

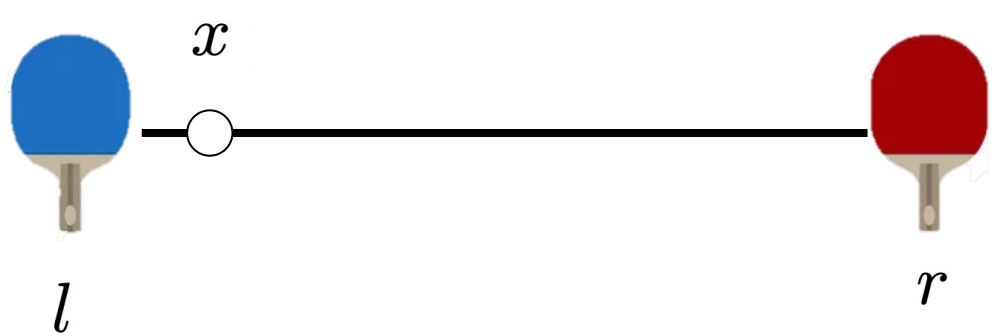
$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

$$[(\mathbf{if}(x + vT < l \wedge v \leq 0 \vee x + vT > r \wedge v \geq 0)$$

$$\mathbf{then}\ (v_{old} := v; v := *; ?(-v_{old} - \varepsilon_1 \leq v \wedge v \leq -v_{old} + \varepsilon_2));$$

$$t := 0; \{x' = v, t' = 1\ \&\ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



A Simple Example: Ping Pong in 1D

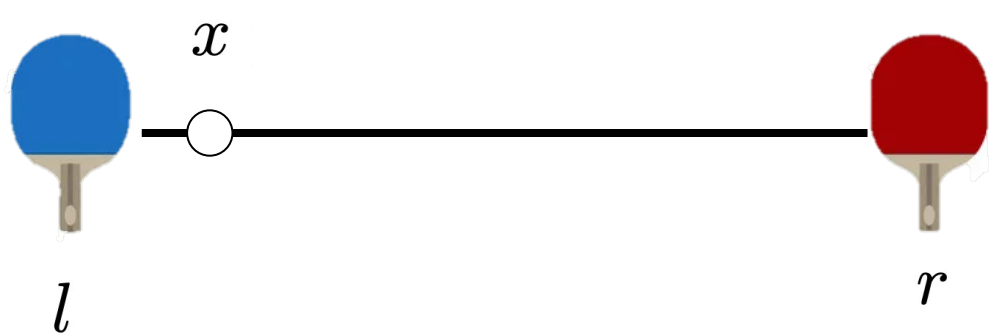
$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

$$[(\textbf{if}(x + \underline{v}T < l \wedge \underline{v} \leq 0 \vee x + \underline{v}T > r \wedge \underline{v} \geq 0)$$

$$\textbf{then}\ (v_{old} := v; v := *; ?(-v_{old} - \varepsilon_1 \leq v \wedge v \leq -v_{old} + \varepsilon_2));$$

$$t := 0; \{x' = v, t' = 1\ \&\ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



A Simple Example: Ping Pong in 1D

$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

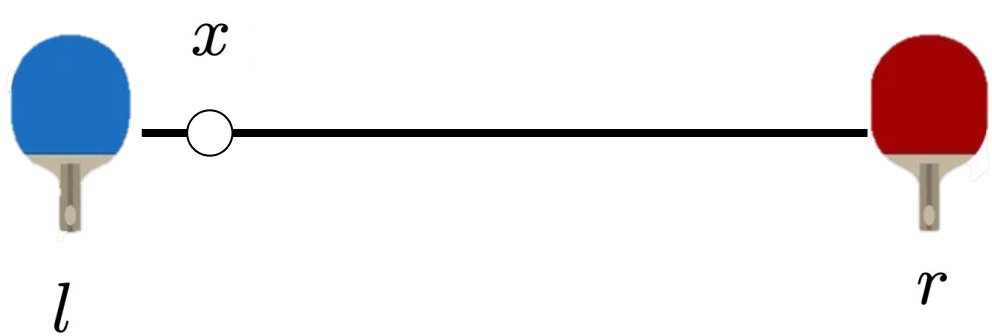
$$[(v_{approx} := *; ?(v - \varepsilon_3 \leq v_{approx} \wedge v + \varepsilon_4);$$

$$\textbf{if}(x + v_{approx}T < l \wedge v_{approx} \leq 0 \vee x + v_{approx}T > r \wedge v_{approx} \geq 0)$$

$$\textbf{then}\ (v_{old} := v_{approx}; v := *; ?(-v_{old} - \varepsilon_1 \leq v \wedge v \leq -v_{old} + \varepsilon_2));$$

$$t := 0; \{x' = v, t' = 1\ \&\ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



A Simple Example: Ping Pong in 1D

$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

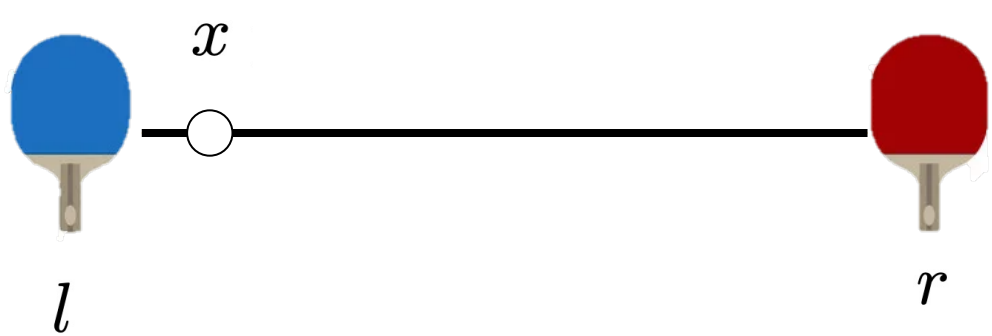
$$[(v_{approx} := *; ?(v - \varepsilon_3 \leq v_{approx} \wedge v + \varepsilon_4);$$

$$\textbf{if}(\underline{x} + v_{approx}T < l \wedge v_{approx} \leq 0 \vee \underline{x} + v_{approx}T > r \wedge v_{approx} \geq 0)$$

$$\textbf{then}\ (v_{old} := v_{approx}; v := *; ?(-v_{old} - \varepsilon_1 \leq v \wedge v \leq -v_{old} + \varepsilon_2));$$

$$t := 0; \{x' = v, t' = 1\ \&\ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



A Simple Example: Ping Pong in 1D

$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

$$[(v_{approx} := *; ?(v - \varepsilon_3 \leq v_{approx} \wedge v + \varepsilon_4);$$

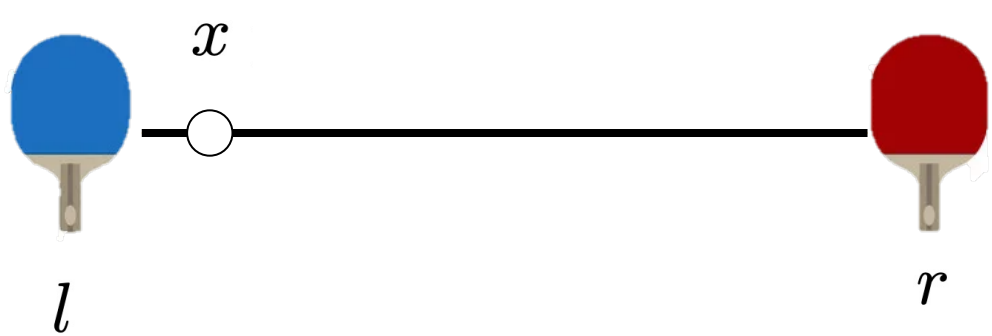
$$x_{approx} := *; ?(x - \varepsilon_5 \leq x_{approx} \wedge x + \varepsilon_6);$$

$$\textbf{if}(x_{approx} + v_{approx}T < l \wedge v_{approx} \leq 0 \vee x_{approx} + v_{approx}T > r \wedge v_{approx} \geq 0)$$

$$\textbf{then}\ (v_{old} := v_{approx}; v := *; ?(-v_{old} - \varepsilon_1 \leq v \wedge v \leq -v_{old} + \varepsilon_2));$$

$$t := 0; \{x' = v, t' = 1\ \&\ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



A Simple Example: Ping Pong in 1D

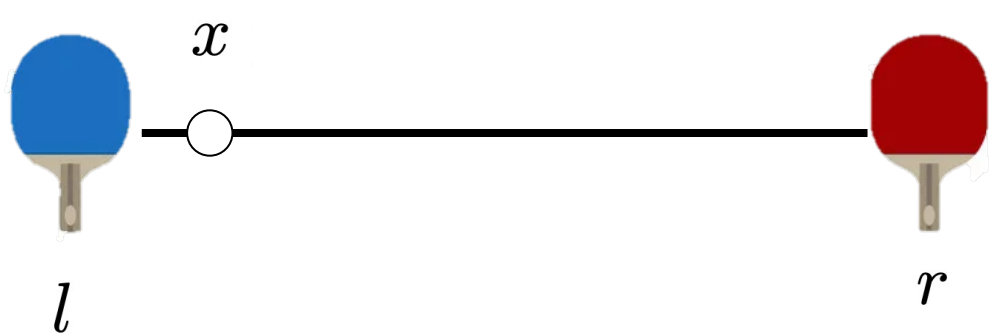
$$l \leq x \wedge x \leq r \wedge v \geq 0 \wedge T > 0 \wedge l + 2vT \leq r \rightarrow$$

$$[(\text{measure } x; \text{measure } v;$$

$$\textbf{if}(\sim x + \sim vT < l \wedge \sim v \leq 0 \vee \sim x + \sim vT > r \wedge \sim v \geq 0) \textbf{ then } \text{set } v \ \ (-\sim v);$$

$$t := 0; \{x' = v, t' = 1 \ \& \ 0 \leq t \leq T\})^*]$$

$$l \leq x \wedge x \leq r$$



Formalization

- I've given the high-level vision and motivation for Controller Aware dL

- There are a lot of technical details that go into actually making Controller Aware dL feasible
  - Giving a formal semantics
  - Formalizing the restrictions on ranges
  - Defining a translation to dL
  - Proving said translation sound