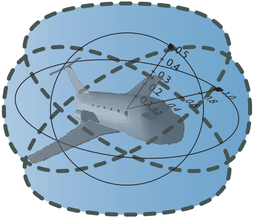
08: Events & Responses

15-424: Foundations of Cyber-Physical Systems

André Platzer

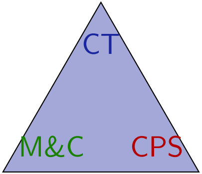
aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA



Outline

Outline

using loop invariants
design event-triggered control

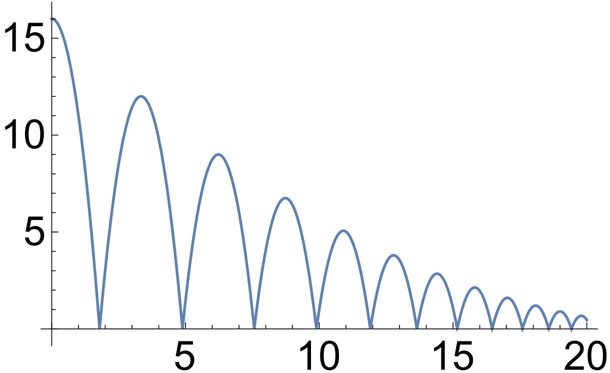


modeling CPS
event-triggered control
continuous sensing
feedback mechanisms
control vs. physics
Cartesian Demons

semantics of event-triggered control
operational effects
model-predictive control

Outline

Quantum the Safely Bored Bouncing Ball

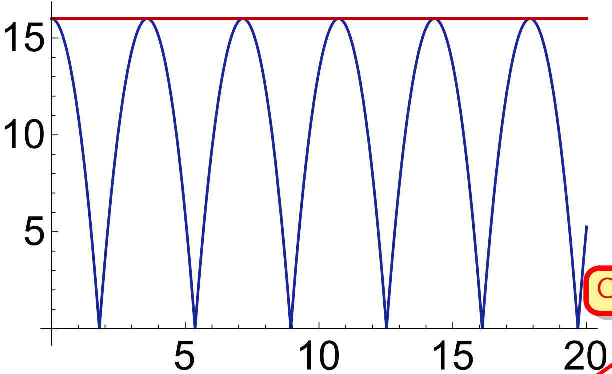


Proposition (Quantum can bounce around safely)

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow$$
$$[\big(x' = v, v' = -g \,\&\, x \ge 0; (?x{=}0; v := -cv \cup ?x{\ne}0)\big)^*](0 \le x \land x \le H)$$

Proof `@invariant`$(2gx = 2gH - v^2 \land x \ge 0)$

Quantum the Safely Bored Bouncing Ball



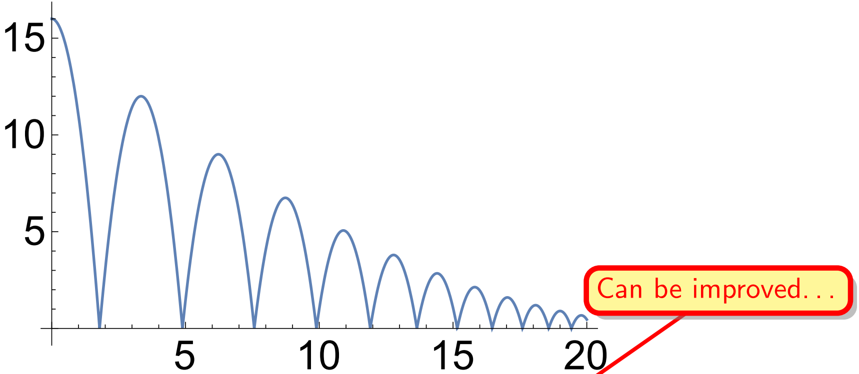
Can be improved...

Proposition (Quantum can bounce around safely)

$$0 \leq x \land x = H \land v = 0 \land g > 0 \land 1 = c \rightarrow$$
$$[(x' = v, v' = -g \,\&\, x \geq 0; (?x{=}0; v := -cv \cup ?x{\neq}0))^*](0 \leq x \land x \leq H)$$

Proof `@invariant`$(2gx = 2gH - v^2 \land x \geq 0)$

Quantum the Safely Bored Bouncing Ball

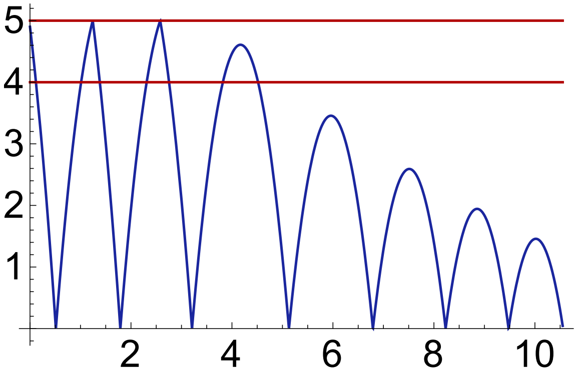


Proposition (Quantum can bounce around safely)

$$0 \le x \land x = H \land v = 0 \land g > 0 \land 1 \ge c \ge 0 \rightarrow$$
$$[(x' = v, v' = -g \,\&\, x \ge 0; (?x{=}0; v := -cv \cup ?x{\ne}0))^*](0 \le x \land x \le H)$$

Proof `@invariant`$(2gx = 2gH - v^2 \land x \ge 0)$

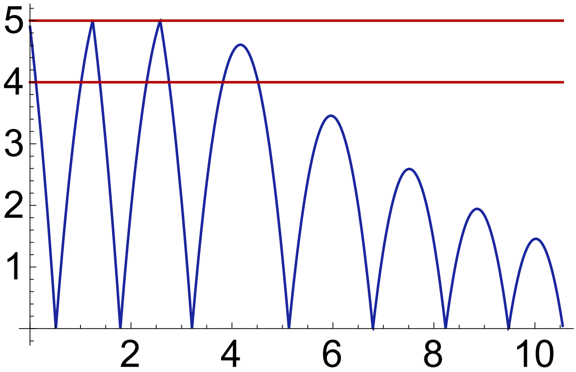
Quantum the Daring Ping Pong Ball



Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \to$$
$$\big[\big(x' = v, v' = -g \,\&\, x \ge 0;$$
$$(?x{=}0; v := -cv \cup ?x{\ne}0)\big)^*\big](0{\le}x{\le}5)$$

Quantum the Daring Ping Pong Ball



Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\big(x' = v, v' = -g \,\&\, x \ge 0;$$
$$(?x{=}0; v := -cv \cup ?4{\le}x{\le}5; v := -fv \cup ?x{\ne}0)\big)^*\Big](0{\le}x{\le}5)$$

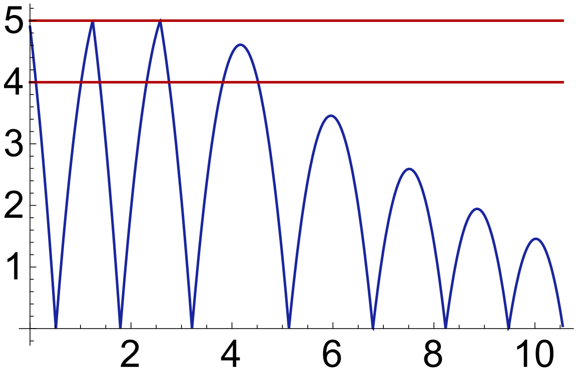
Proof? Ask René Descartes

Cartesian Doubt: René Descartes's Cartesian Demon 1641

Outwit the Cartesian Demon

Skeptical about the truth of all beliefs until justification has been found.

Quantum the Daring Ping Pong Ball

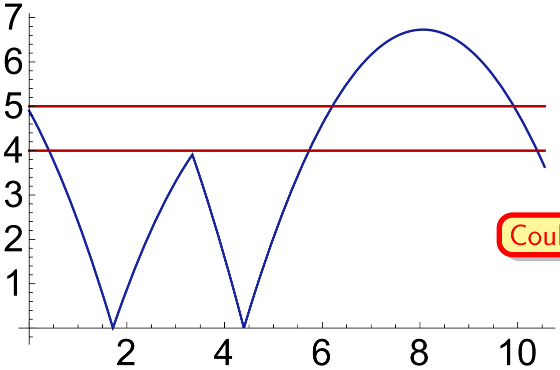


Conjecture (Quantum can play ping pong safely)

$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow$$
$$\big[\big(x' = v, v' = -g \,\&\, x \geq 0;$$
$$(?x{=}0;\, v := -cv \cup ?4{\leq}x{\leq}5;\, v := -fv \cup ?x{\neq}0)\big)^*\big](0{\leq}x{\leq}5)$$

Proof? Ask René Descartes

Quantum the Daring Ping Pong Ball



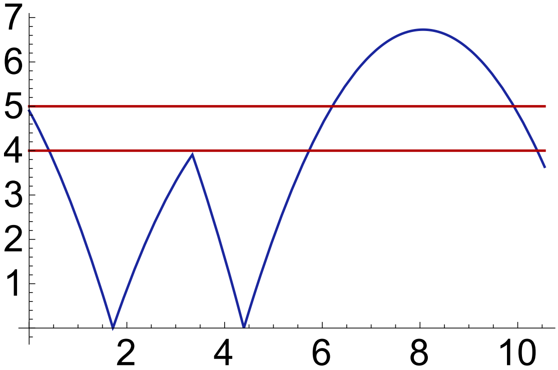
Could run instead of control

Conjecture (Quantum can play ping pong safely)

$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow$$
$$\big[\big(x' = v, v' = -g \,\&\, x \geq 0;$$
$$(?x{=}0; v := -cv \cup ?4{\leq}x{\leq}5; v := -fv \cup ?x{\neq}0)\big)^*\big](0{\leq}x{\leq}5)$$

Proof? Ask René Descartes who says no!

Quantum the Daring Ping Pong Ball



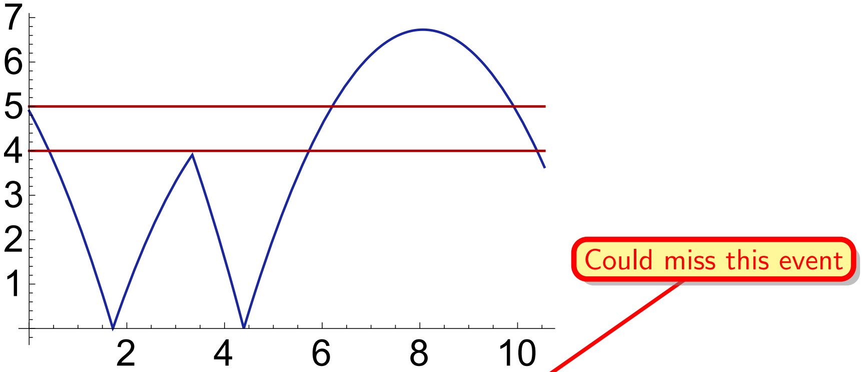
No bounce at event

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(x' = v, v' = -g \,\&\, x \ge 0;$$
$$(?x{=}0; v := -cv \cup ?4{\le}x{\le}5; v := -fv \cup ?x{\ne}0 \land x{<}4 \lor x{>}5)\big)^*\big](0{\le}x{\le}5)$$

Proof? Ask René Descartes who says no!

Quantum the Daring Ping Pong Ball

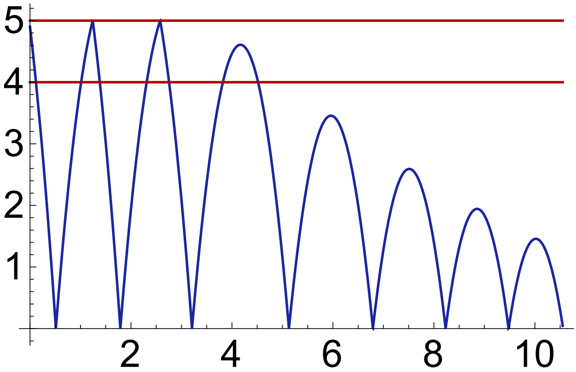


Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\big(x' = v, v' = -g \,\&\, x \ge 0;$$
$$(?x{=}0; v := -cv \cup ?4{\le}x{\le}5; v := -fv \cup ?x{\ne}0{\land}x{<}4{\lor}x{>}5)\big)^*\Big](0{\le}x{\le}5)$$

Proof? Ask René Descartes who says no!

Quantum the Deterministically Daring Ping Pong Ball

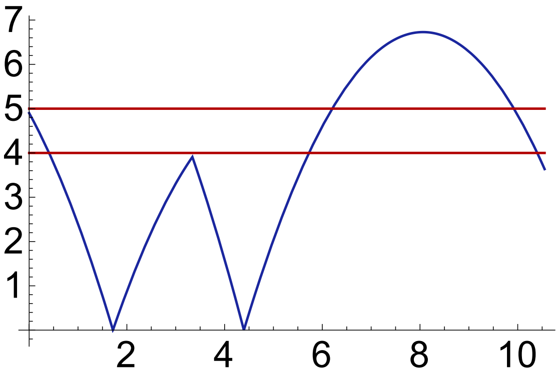


Conjecture (Quantum can play ping pong safely)

$$0 \leq x \wedge x \leq 5 \wedge v \leq 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \wedge f \geq 0 \rightarrow \\ \left[\left(\{x' = v, v' = -g \,\&\, x \geq 0\}; \\ \texttt{if}(x{=}0)\, v := -cv \;\texttt{else}\; \texttt{if}(4{\leq}x{\leq}5)\, v := -fv\right)^*\right](0{\leq}x{\leq}5)$$

Proof? Ask René Descartes

Quantum the Deterministically Daring Ping Pong Ball

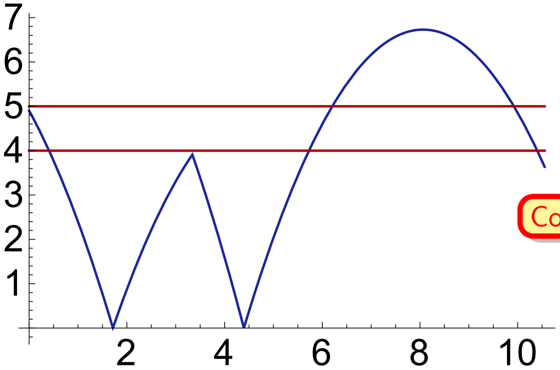


Conjecture (Quantum can play ping pong safely)

$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow \Big[\big(\{x' = v, v' = -g \,\&\, x \geq 0\}; \; \texttt{if}(x{=}0)\, v := -cv \;\texttt{else}\; \texttt{if}(4{\leq}x{\leq}5)\, v := -fv\big)^*\Big](0{\leq}x{\leq}5)$$

Proof? Ask René Descartes who says no!

Quantum the Deterministically Daring Ping Pong Ball



Could also miss if-then event

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0\};$$
$$\texttt{if}(x{=}0)\ v := -cv\ \texttt{else if}(4{\le}x{\le}5)\ v := -fv\big)^*\big](0{\le}x{\le}5)$$

Proof? Ask René Descartes who says no!

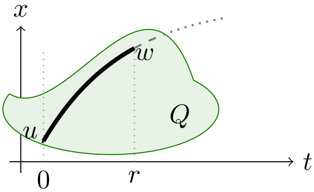
Outline

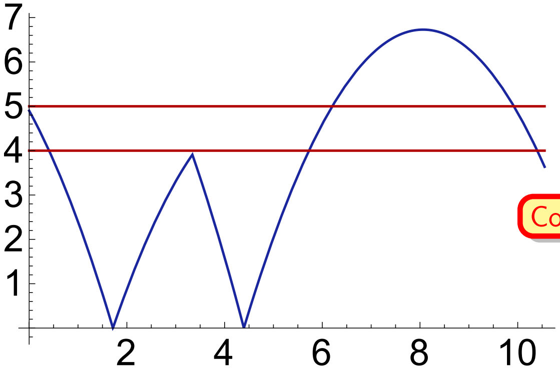
Evolution Domains Detect Events

Evolution domains detect events

$$x' = f(x) \,\&\, Q$$

Evolution domain Q of a differential equation is responsible for detecting events. Q can stop physics whenever an event happens on which the control wants to take action.



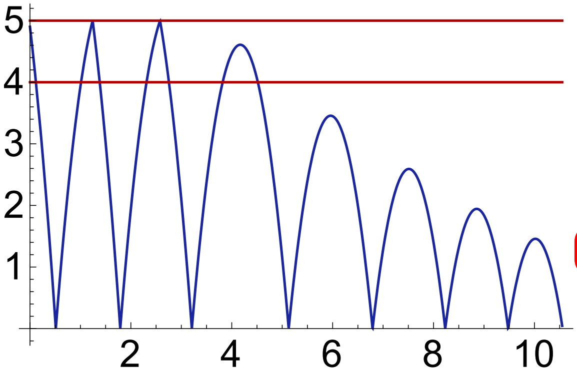


Could also miss if-then event

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow \\ \big[\big(\{x' = v, v' = -g \,\&\, x \ge 0\}; \\ \texttt{if}(x{=}0)\, v := -cv \;\texttt{else}\; \texttt{if}(4{\le}x{\le}5)\, v := -fv\big)^*\big](0{\le}x{\le}5)$$

Proof? Ask René Descartes who says no!

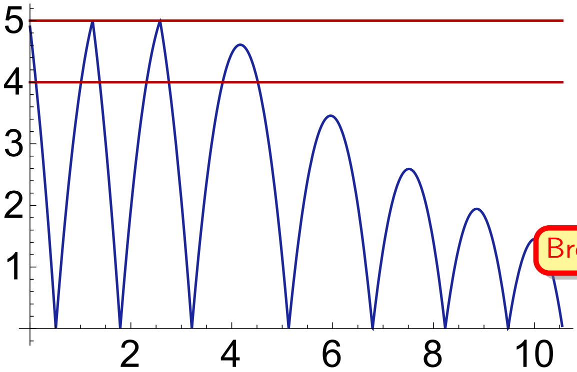


Domain as event trap?

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land 4 \le x \le 5\};$$
$$\mathtt{if}(x=0)\, v := -cv \;\mathtt{else}\;\mathtt{if}(4 \le x \le 5)\, v := -fv\big)^*\Big](0 \le x \le 5)$$

Proof? Ask René Descartes who says no!

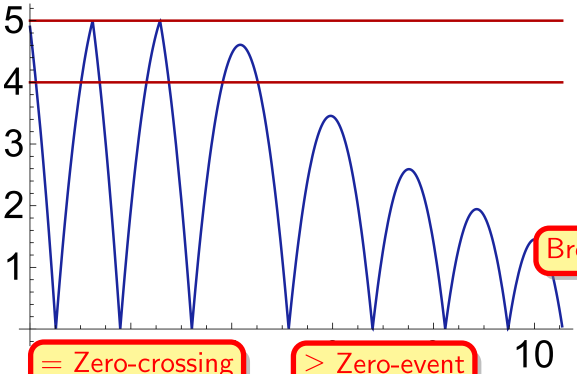


Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land 4 \le x \le 5\};$$
$$\text{if}(x=0)\, v := -cv \,\text{else if}(4 \le x \le 5)\, v := -fv\big)^*\big](0 \le x \le 5)$$

Proof? Ask René Descartes who says no!

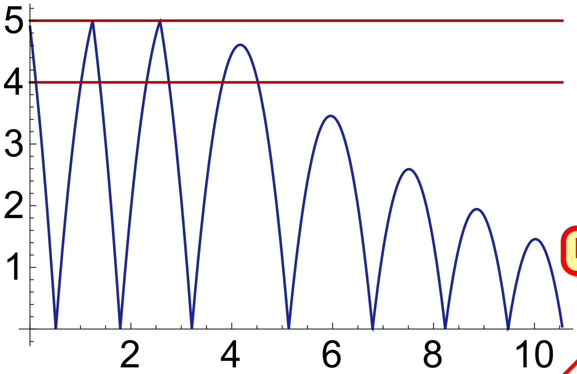
Quantum the Deterministically Daring Ping Pong Ball



Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land 4 \le x \le 5\};$$
$$\texttt{if}(x{=}0)\; v := -cv \;\texttt{else}\;\texttt{if}(4 \le x \le 5)\; v := -fv\big)^*\big](0 \le x \le 5)$$

Proof? Ask René Descartes who says no!

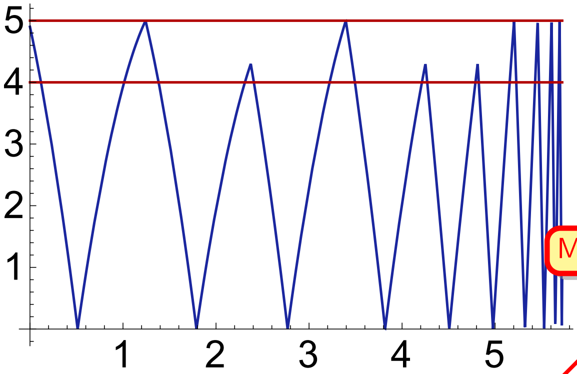


Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5\};$$
$$\texttt{if}(x=0)\, v := -cv \,\texttt{else}\,\texttt{if}(4 \le x \le 5)\, v := -fv\big)^*\Big](0 \le x \le 5)$$

Proof? Ask René Descartes who says yes!

Quantum the Deterministically Daring Ping Pong Ball

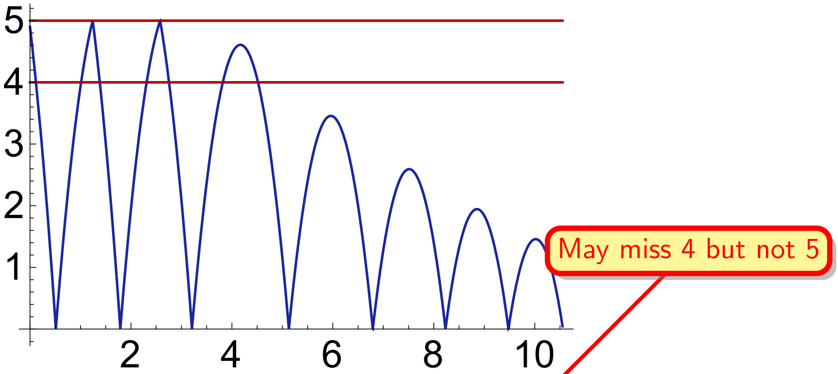


Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5\};$$
$$\mathtt{if}(x=0)\, v := -cv \,\mathtt{else}\,\mathtt{if}(4 \le x \le 5)\, v := -fv\big)^*\big](0 \le x \le 5)$$

Proof? Ask René Descartes who says yes!

Quantum the Deterministically Daring Ping Pong Ball

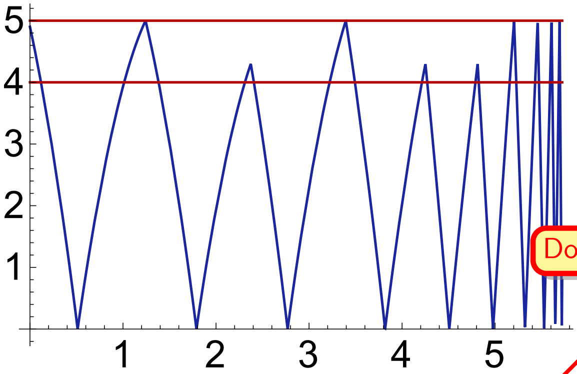


Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5\};$$
$$\texttt{if}(x=0)\, v := -cv\, \texttt{else}\, \texttt{if}(4 \le x \le 5)\, v := -fv\big)^*\big](0 \le x \le 5)$$

Proof? Ask René Descartes who says yes!

Quantum the Deterministically Daring Ping Pong Ball

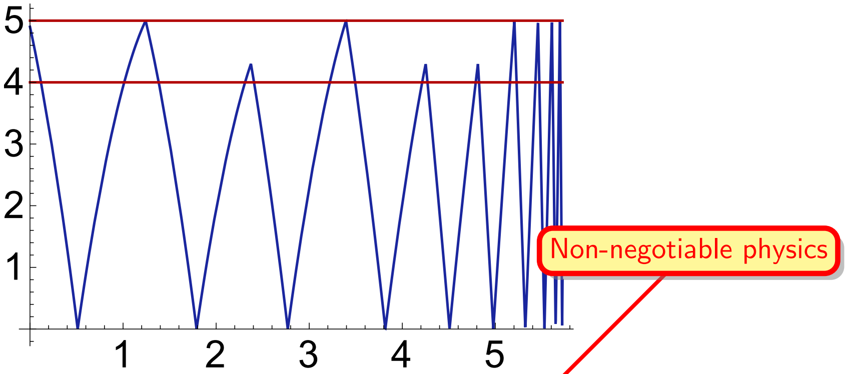


Domain by construction

Conjecture (Quantum can play ping pong safely)

$$0 \leq x \wedge x \leq 5 \wedge v \leq 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \wedge f \geq 0 \rightarrow \Big[\big(\{x' = v, v' = -g \,\&\, x \geq 0 \wedge x \leq 5\}; \; \mathtt{if}(x=0)\, v := -cv \,\mathtt{else}\, \mathtt{if}(4 \leq x \leq 5)\, v := -fv\big)^*\Big](0 \leq x \leq 5)$$

Proof? Ask René Descartes who says yes! But meant to say no!



Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \to \Big[\Big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5\};\ \mathtt{if}(x{=}0)\, v := -cv \,\mathtt{else\,if}(4{\le}x{\le}5)\, v := -fv\Big)^*\Big](0{\le}x{\le}5)$$

Proof? Ask René Descartes who says yes! But meant to say no!

On the Nuisance of Nuances of Physics

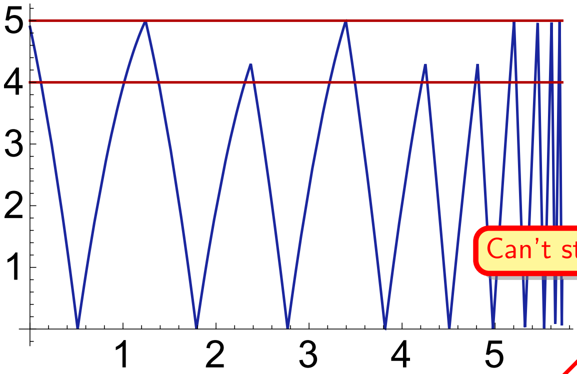
Non-negotiability of Physics

1. Making systems safe by construction is a great idea. For control!
2. Not by changing the laws of physics around.
3. Physics is unpleasantly non-negotiable.
4. If models are safe because we forgot to include all behavior of physical reality, then correctness statements only hold in that other universe.

Despite control — We don't get to boss physics around

We don't make this world any safer by writing CPS programs for another universe.

Quantum the Deterministically Daring Ping Pong Ball

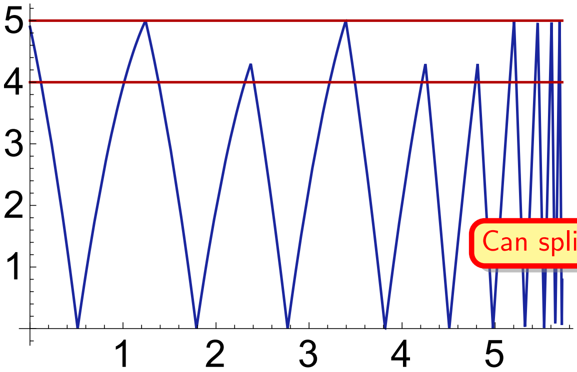


Can't stop the world for an event

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5\};$$
$$\mathtt{if}(x{=}0)\, v := -cv \,\mathtt{else}\,\mathtt{if}(4{\le}x{\le}5)\, v := -fv\big)^*\big](0{\le}x{\le}5)$$

Proof? Ask René Descartes who says yes! But meant to say no!

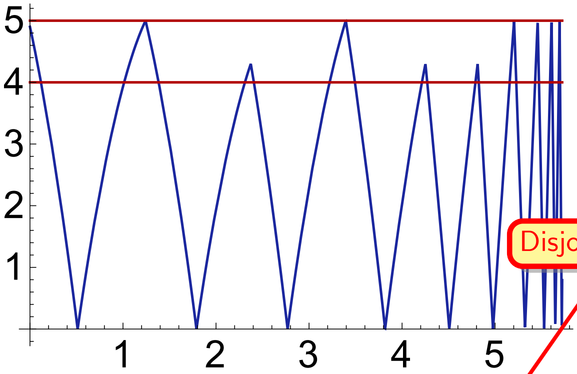


Can split the world for an event

Conjecture (Quantum can play ping pong safely)

$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \geq 0 \land x \leq 5 \;\cup\; x' = v, v' = -g \,\&\, x > 5\};$$
$$\texttt{if}(x=0)\, v := -cv \;\texttt{else}\;\texttt{if}(4 \leq x \leq 5)\, v := -fv\big)^*\big](0 \leq x \leq 5)$$

Proof? Ask René Descartes



Disjoint domains

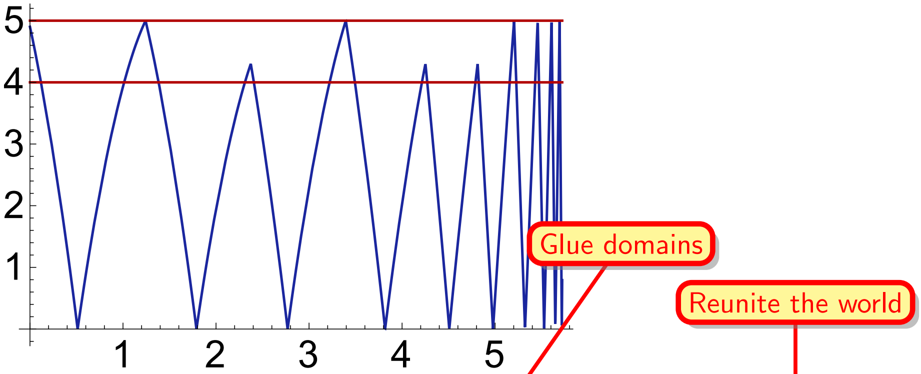
Shattered the world

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5 \;\cup\; x' = v, v' = -g \,\&\, x > 5\};$$
$$\texttt{if}(x=0)\, v := -cv \,\texttt{else}\,\texttt{if}(4 \le x \le 5)\, v := -fv\big)^*\big](0 \le x \le 5)$$

Proof? Ask René Descartes

Quantum the Deterministically Daring Ping Pong Ball



Conjecture (Quantum can play ping pong safely)

$$0 \le x \wedge x \le 5 \wedge v \le 0 \wedge g > 0 \wedge 1 \ge c \ge 0 \wedge f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \wedge x \le 5 \;\cup\; x' = v, v' = -g \,\&\, x \ge 5\};$$
$$\mathtt{if}(x=0)\, v := -cv \;\mathtt{else}\;\mathtt{if}(4 \le x \le 5)\, v := -fv\big)^*\big](0 \le x \le 5)$$

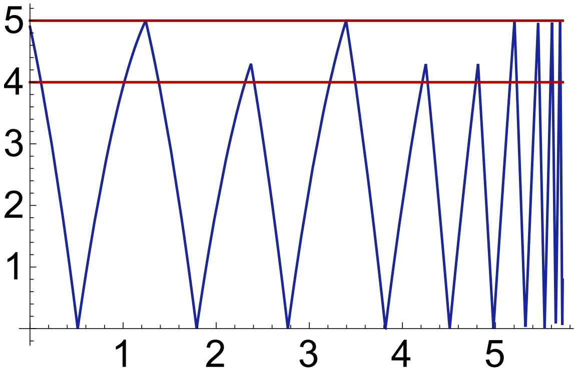
Proof? Ask René Descartes

Connected evolution domains

1. Evolution domain constraints need care.
2. Determine regions within which the system can evolve.
3. Disconnected/disjoint disallows continuous transitions.

1. Splitting the state space into different regions to detect events is fine.
2. Destroying the world is not.
3. Not even by poking infinitesimal holes into the time-space continuum.

Quantum the Deterministically Daring Ping Pong Ball

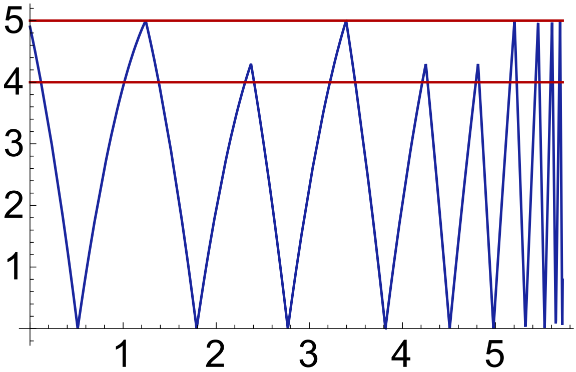


Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\Big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5 \;\cup\; x' = v, v' = -g \,\&\, x \ge 5\};$$
$$\texttt{if}(x{=}0)\, v := -cv \,\texttt{else}\,\texttt{if}(4 \le x \le 5)\, v := -fv\Big)^*\Big](0 \le x \le 5)$$

Proof? Ask René Descartes

Quantum the Deterministically Daring Ping Pong Ball



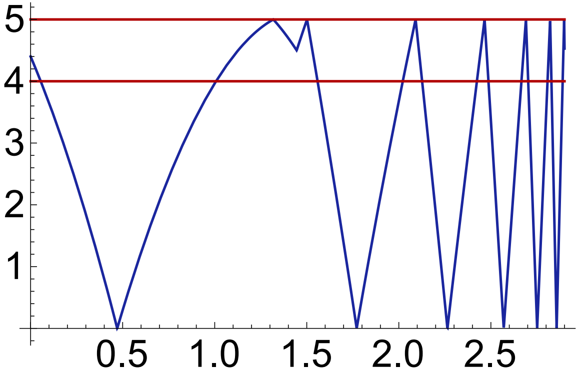
Multi-fire

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5 \cup x' = v, v' = -g \,\&\, x \ge 5\};$$
$$\texttt{if}(x=0)\, v := -cv \,\texttt{else}\,\texttt{if}(4 \le x \le 5)\, v := -fv\big)^*\big](0 \le x \le 5)$$

Proof? Ask René Descartes

Quantum the Deterministically Daring Ping Pong Ball



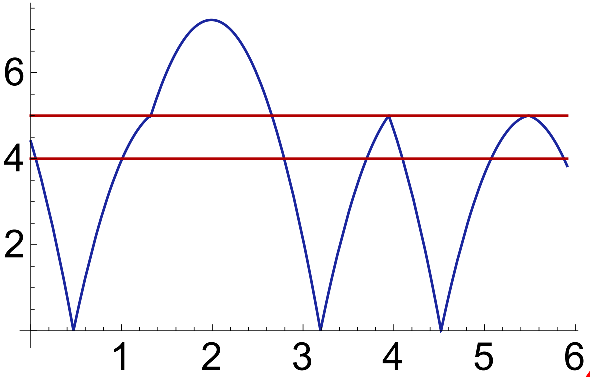
Multi-fire

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow \big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5 \cup x' = v, v' = -g \,\&\, x \ge 5\};\ \mathtt{if}(x=0)\, v := -cv\ \mathtt{else}\ \mathtt{if}(4 \le x \le 5)\, v := -fv\big)^*\big](0 \le x \le 5)$$

Proof? Ask René Descartes

Quantum the Deterministically Daring Ping Pong Ball



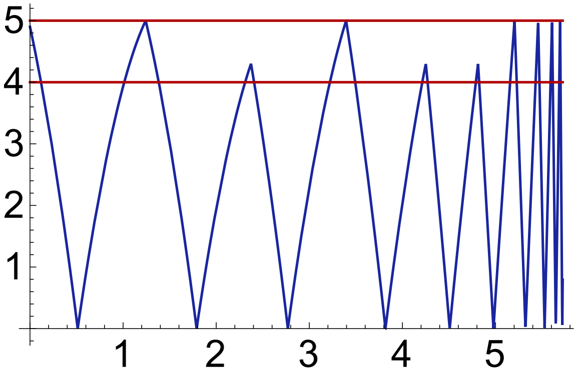
Multi-fire

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \to$$
$$\Big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5 \cup x' = v, v' = -g \,\&\, x \ge 5\};$$
$$\mathtt{if}(x{=}0)\, v := -cv \;\mathtt{else\ if}(4 \le x \le 5)\, v := -fv\big)^*\Big](0 \le x \le 5)$$

Proof? Ask René Descartes who definitely says no!

Quantum the Deterministically Daring Ping Pong Ball



Only upsense event

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5 \;\cup\; x' = v, v' = -g \,\&\, x \ge 5\};$$
$$\texttt{if}(x{=}0)\; v := -cv \;\texttt{else}\;\texttt{if}(4 \le x \le 5 \land v \ge 0)\; v := -fv\big)^*\Big](0 \le x \le 5)$$

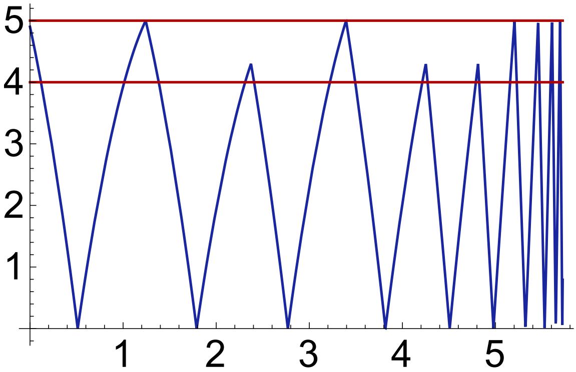
Proof? Ask René Descartes

Multi-firing Events

Multi-firing of events

1. If the same event is detected multiple times:
2. Are multiple responses acceptable?
3. Or is a single response crucial?

Physics vs. Control: Classification



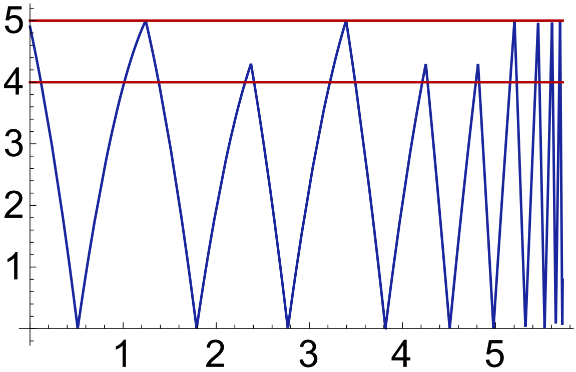
control: robust, all cases

physics: precise

Conjecture (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\Big(\big((x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5) \cup (x' = v, v' = -g \,\&\, x \ge 5)\big);$$
$$\texttt{if}(x=0)\, v := -cv \;\texttt{else}\;\texttt{if}(4 \le x \le 5 \land v \ge 0)\, v := -fv\Big)^*\Big](0 \le x \le 5)$$

Physics vs. Control: Classification



control: robust, all cases

physics: precise

Conjecture (Quantum can play ping pong safely)

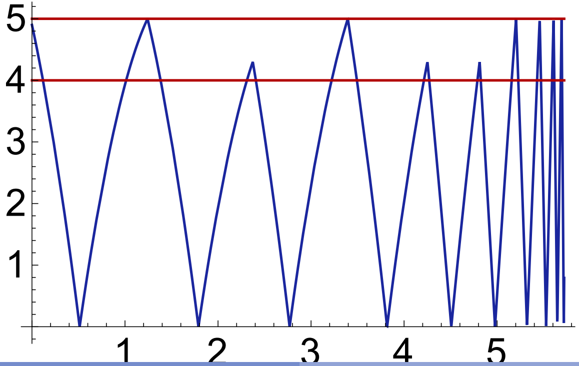
$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow$$
$$\Big[\big(((x' = v, v' = -g \,\&\, x \geq 0 \land x \leq 5) \cup (x' = v, v' = -g \,\&\, x \geq 5));$$
$$\texttt{if}(x{=}0)\, v := -cv \;\texttt{else}\; \texttt{if}(4 \leq x \leq 5 \land v \geq 0)\, v := -fv\big)^*\Big](0 \leq x \leq 5)$$

Outline

Quantum's Ping Pong Proof Invariants

Proposition (Quantum can play ping pong safely)

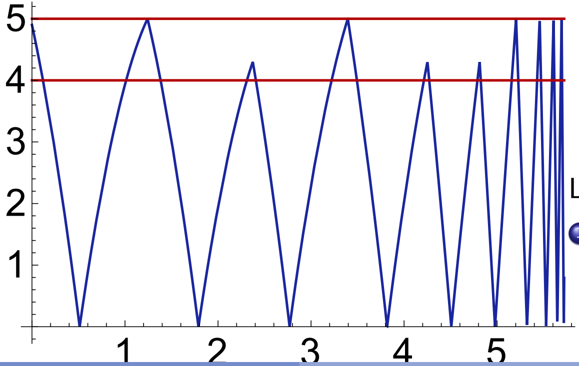
$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\Big[\Big(\big((x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5) \cup (x' = v, v' = -g \,\&\, x \ge 5)\big);$$
$$\texttt{if}(x=0)\; v := -cv \;\texttt{else}\;\texttt{if}(4 \le x \le 5 \land v \ge 0)\; v := -fv\Big)^*\Big](0 \le x \le 5)$$



Quantum's Ping Pong Proof Invariants

Proposition (Quantum can play ping pong safely)

$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow$$
$$\big[\big(((x' = v, v' = -g \,\&\, x \geq 0 \land x \leq 5) \cup (x' = v, v' = -g \,\&\, x \geq 5));$$
$$\texttt{if}(x=0)\, v := -cv\, \texttt{else}\, \texttt{if}(4 \leq x \leq 5 \land v \geq 0)\, v := -fv\big)^*\big](0 \leq x \leq 5)$$



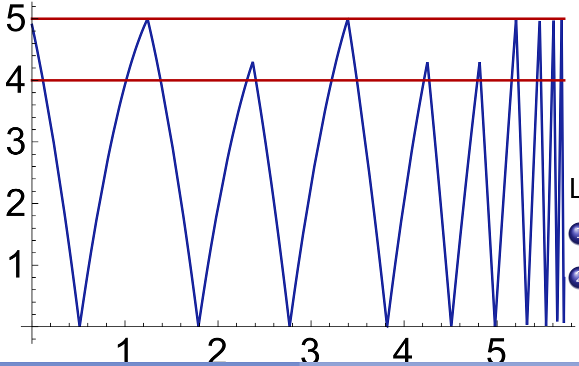
Loop invariant $j(x, v)$:

1. $0 \leq x \leq 5$ not inductive

Quantum's Ping Pong Proof Invariants

Proposition (Quantum can play ping pong safely)

$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(((x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5) \cup (x' = v, v' = -g \,\&\, x \ge 5));$$
$$\texttt{if}(x=0)\, v := -cv \;\texttt{else}\; \texttt{if}(4 \le x \le 5 \land v \ge 0)\, v := -fv\big)^*\big](0 \le x \le 5)$$



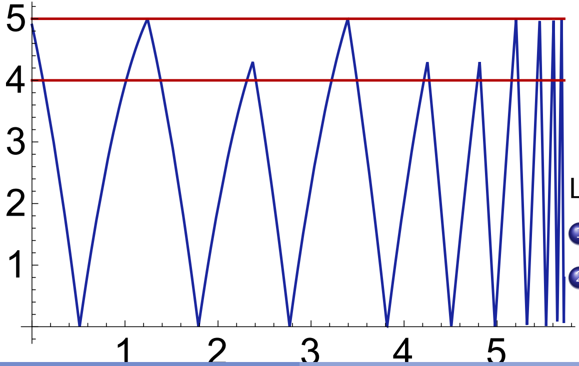
Loop invariant $j(x, v)$:

1. $0 \le x \le 5$ not inductive
2. $0 \le x \le 5 \land v \le 0$

Quantum's Ping Pong Proof Invariants

Proposition (Quantum can play ping pong safely)

$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow$$
$$\big[\big(((x' = v, v' = -g \,\&\, x \geq 0 \land x{\leq}5) \cup (x' = v, v' = -g \,\&\, x{\geq}5));$$
$$\texttt{if}(x{=}0)\, v := -cv \,\texttt{else}\,\texttt{if}(4{\leq}x{\leq}5{\land}v{\geq}0)\, v := -fv\big)^*\big](0{\leq}x{\leq}5)$$



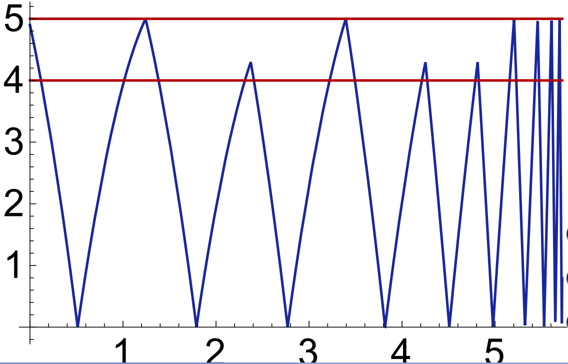
Loop invariant $j(x, v)$:

1. $0{\leq}x{\leq}5$ not inductive
2. $0{\leq}x{\leq}5{\land}v{\leq}0$ not inductive

Quantum's Ping Pong Proof Invariants

Proposition (Quantum can play ping pong safely)

$$0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \rightarrow$$
$$\big[\big(((x' = v, v' = -g \,\&\, x \geq 0 \land x{\leq}5) \cup (x' = v, v' = -g \,\&\, x{\geq}5));$$
$$\texttt{if}(x{=}0)\, v := -cv \,\texttt{else}\, \texttt{if}(4{\leq}x{\leq}5{\land}v{\geq}0)\, v := -fv\big)^*\big](0{\leq}x{\leq}5)$$



Loop invariant $j(x, v)$:

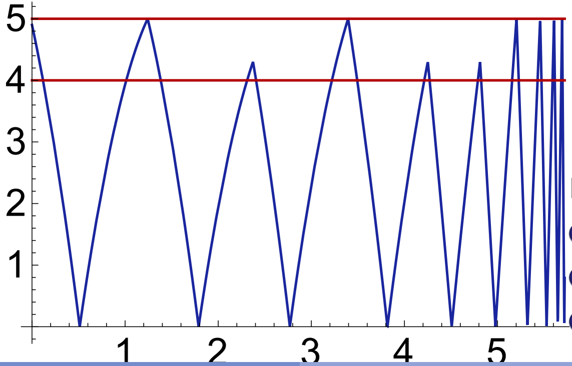
1. $0{\leq}x{\leq}5$ not inductive
2. $0{\leq}x{\leq}5{\land}v{\leq}0$ not inductive
3. $0{\leq}x{\leq}5{\land}(x{=}5{\rightarrow}v{\leq}0)$

Quantum's Ping Pong Proof Invariants

Proposition (Quantum can play ping pong safely)

$$0 \leq x \wedge x \leq 5 \wedge v \leq 0 \wedge g > 0 \wedge 1 \geq c \geq 0 \wedge f \geq 0 \rightarrow$$
$$\big[\big(((x' = v, v' = -g \,\&\, x \geq 0 \wedge x \leq 5) \cup (x' = v, v' = -g \,\&\, x \geq 5));$$
$$\texttt{if}(x=0)\, v := -cv \;\texttt{else}\; \texttt{if}(4 \leq x \leq 5 \wedge v \geq 0)\, v := -fv\big)^*\big](0 \leq x \leq 5)$$

Proof $\texttt{@invariant}(0 \leq x \leq 5 \wedge (x = 5 \rightarrow v \leq 0))$



Loop invariant $j(x, v)$:

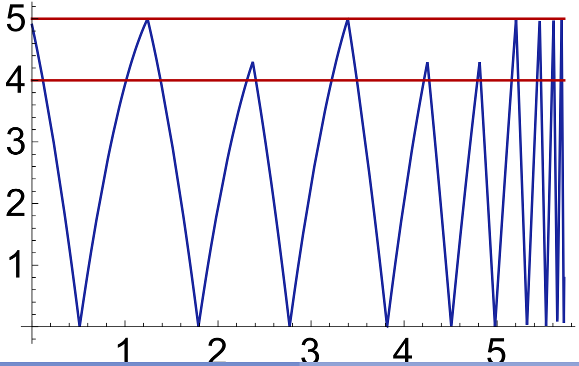
1. $0 \leq x \leq 5$ not inductive
2. $0 \leq x \leq 5 \wedge v \leq 0$ not inductive
3. $0 \leq x \leq 5 \wedge (x=5 \rightarrow v \leq 0)$ yes!

Quantum's Ping Pong Proof Invariants

Proposition (Quantum can play ping pong safely)

$$0 \le x \wedge x \le 5 \wedge v \le 0 \wedge g > 0 \wedge 1 \ge c \ge 0 \wedge f \ge 0 \rightarrow$$
$$\big[\big(\big((x' = v, v' = -g \,\&\, x \ge 0 \wedge x \le 5) \cup (x' = v, v' = -g \,\&\, x \ge 5)\big);$$
$$\texttt{if}(x=0)\; v := -cv \;\texttt{else}\;\texttt{if}(4 \le x \le 5 \wedge v \ge 0)\; v := -fv\big)^*\big](0 \le x \le 5)$$

Proof `@invariant`$(0 \le x \le 5 \wedge (x = 5 \rightarrow v \le 0))$



Outline

Summary: Event-triggered Control

1. Common conceptually simple paradigm for designing controllers
2. Assumes all events are surely detected
3. Implementation: Requires continuous sensing
   Tell me if you found a good implementation platform ...
4. Robust events, not just $\texttt{if}(x = 9.8696)$ ...
5. Events have subtle models, but make design and verification easier!

Non-negotiability of Physics | Connected domains | Multi-firing

6. Verify event-triggered model as first step, then refine toward realistic implementation based on safe event-triggered design
7. Physics $\neq$ Control

On the Nuisance of Nuances of Physics

Non-negotiability of Physics

1. Making systems safe by construction is a great idea. For control!
2. Not by changing the laws of physics around.
3. Physics is unpleasantly non-negotiable.
4. If models are safe because we forgot to include all behavior of physical reality, then correctness statements only hold in that other universe.

Despite control | We don't get to boss physics around

We don't make this world any safer by writing CPS programs for another universe.

André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2016.
URL: http://www.cs.cmu.edu/~aplatzer/course/fcps16.html.

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.