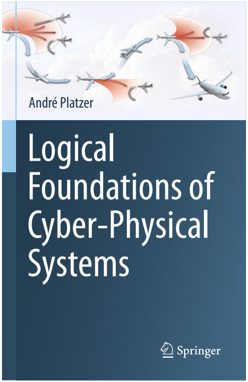
08: Events & Responses

Logical Foundations of Cyber-Physical Systems



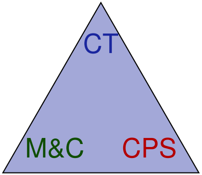
André Platzer

Carnegie Mellon University
Computer Science Department

Outline

Learning Objectives

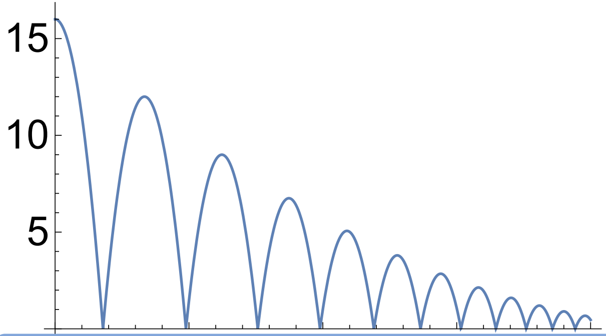
using loop invariants
design event-triggered control



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

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

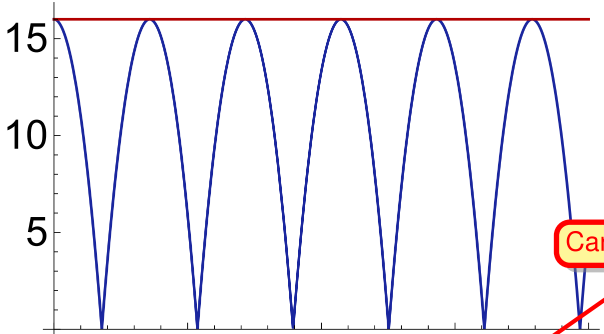
Outline



Proposition (Quantum can bounce around safely)

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

Quantum the Safely Bored Bouncing Ball



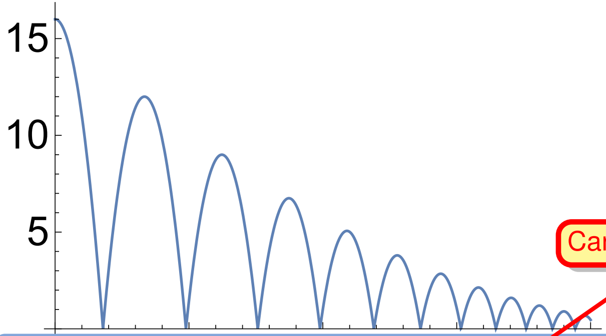
Can be improved...

Proposition (Quantum can bounce around safely)

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

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

Quantum the Safely Bored Bouncing Ball

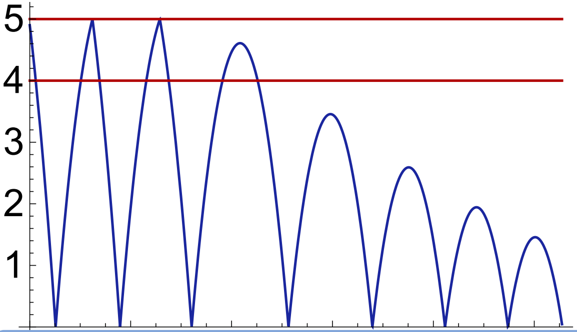


Can be improved...

Proposition (Quantum can bounce around safely)

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

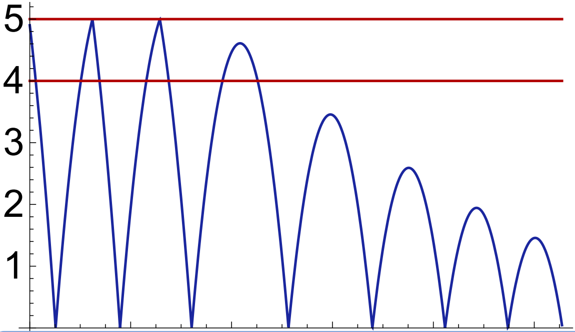
Quantum the Daring Ping-Pong Ball



Conjecture (Quantum can play ping-pong safely)

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

Quantum the Daring Ping-Pong Ball



Conjecture (Quantum can play ping-pong safely)

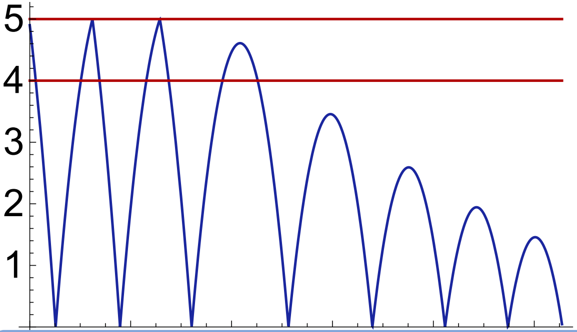
$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow \Big[\Big(\{x' = v, v' = -g \,\&\, x \ge 0\}; \; (?x{=}0; v := -cv \cup ?4{\le}x{\le}5; v := -fv \cup ?x{\ne}0)\Big)^*\Big](0{\le}x{\le}5)$$

Proof? Ask René Descartes

Outwit the Cartesian Demon

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

Quantum the Daring Ping-Pong Ball

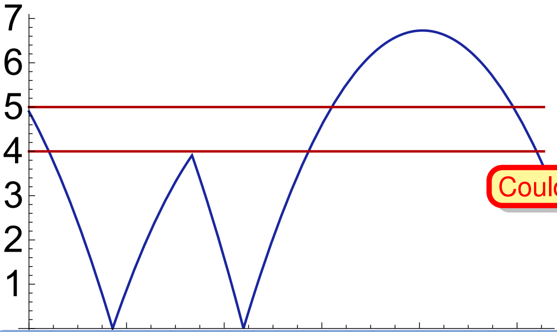


Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes

Quantum the Daring Ping-Pong Ball



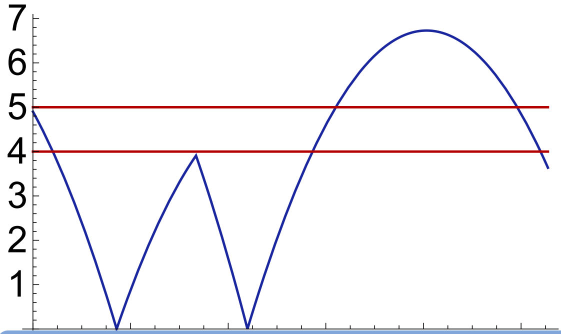
Could run instead of control

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

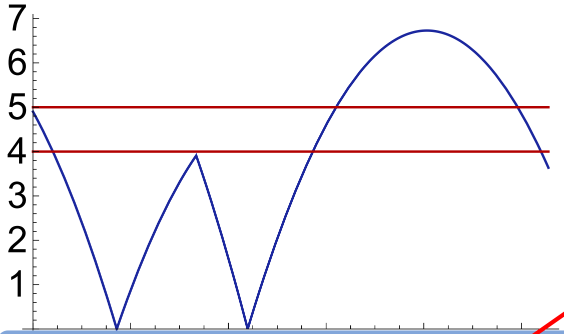


No bounce nor event

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes who says no!



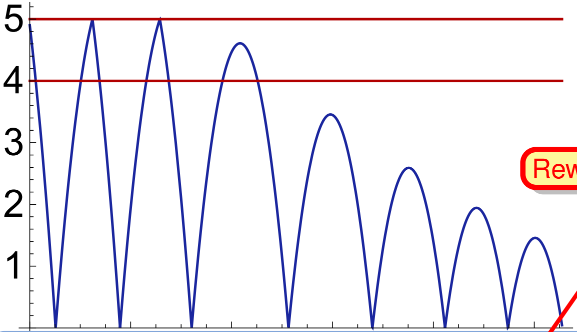
Could miss this event

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 Deterministically Daring Ping-Pong Ball

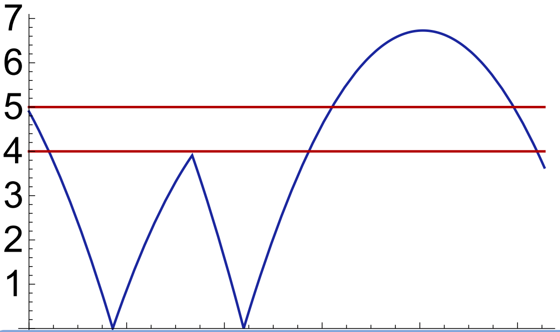


Rewrite as if-then-else

Conjecture (Quantum can play ping-pong safely)

$$
\begin{aligned}
&0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \to \\
&\quad \big[\big(\big(\{x' = v, v' = -g \,\&\, x \geq 0\}\big); \\
&\qquad \mathrm{if}(x{=}0)\, v := -cv \,\mathrm{else\,if}(4{\leq}x{\leq}5)\, v := -fv\big)^*\big](0{\leq}x{\leq}5)
\end{aligned}
$$

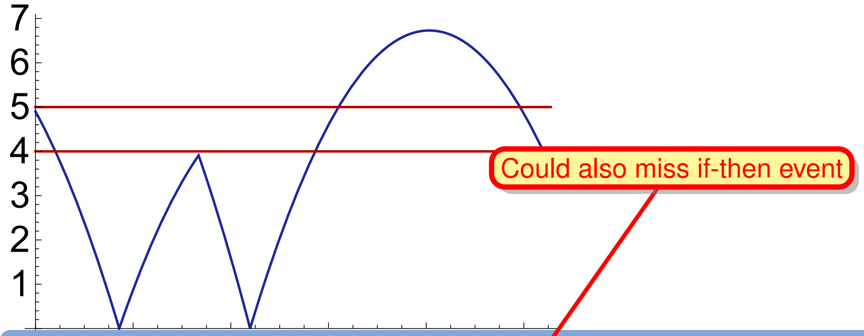
Proof? Ask René Descartes



Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes who says no!



Conjecture (Quantum can play ping-pong safely)

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

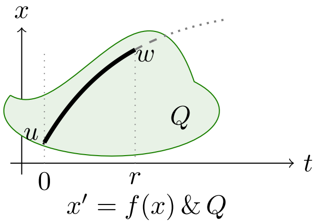
Proof? Ask René Descartes who says no!

Outline

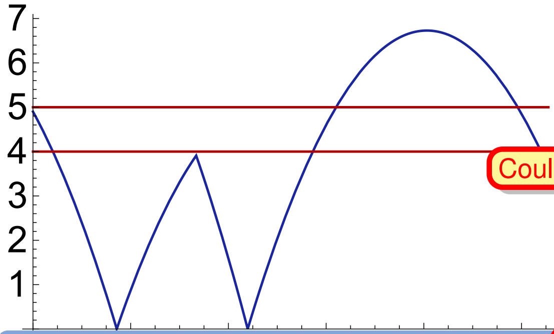
Evolution domains detect events

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

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.



Quantum the Deterministically Daring Ping-Pong Ball

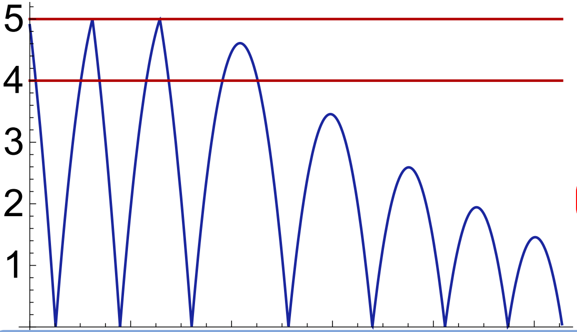


Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes who says no!

Quantum the Deterministically Daring Ping-Pong Ball



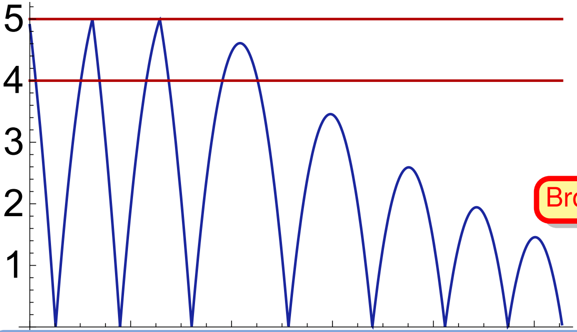
Domain as event trap?

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes who says no!

Quantum the Deterministically Daring Ping-Pong Ball

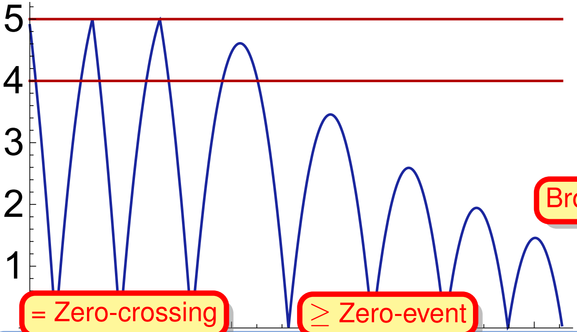


Broken physics: Always event

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes who says no!



= Zero-crossing

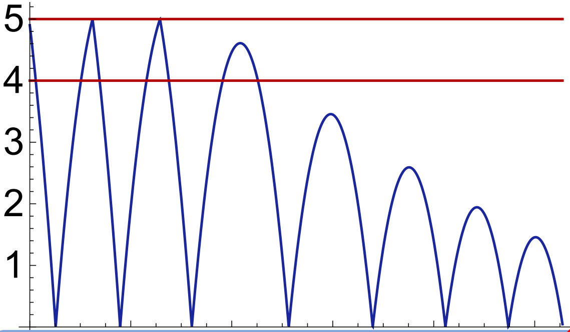
$\geq$ Zero-event

Broken physics: Always event

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes who says no!

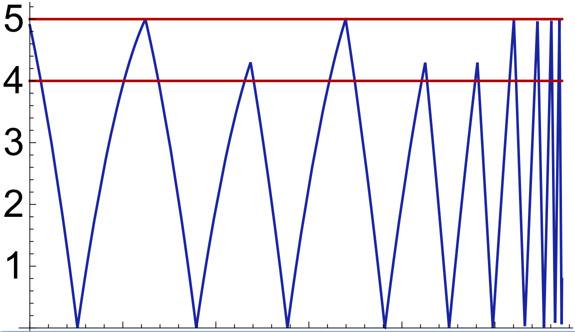


Limiting constraint

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes

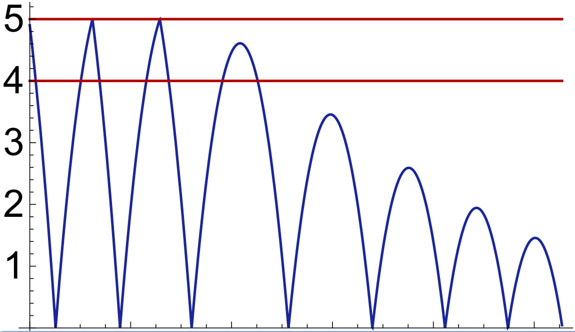


May miss 4 but not 5

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes

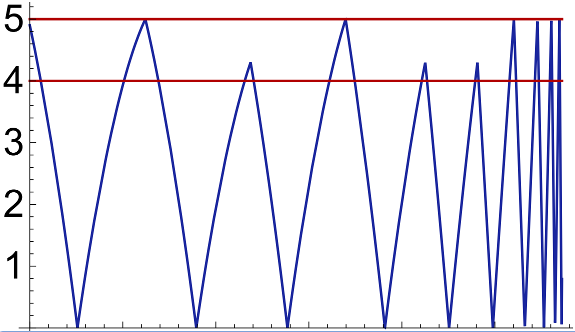


May miss 4 but not 5

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes who says yes!



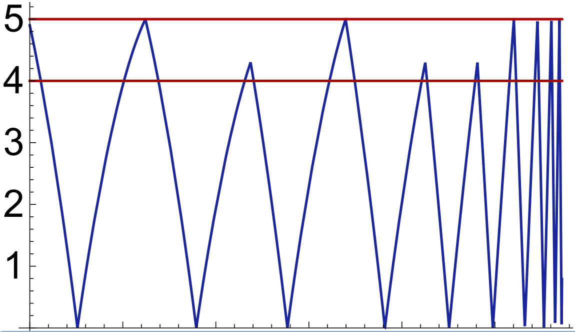
Domain by construction

Conjecture (Quantum can play ping-pong safely)

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

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

Quantum the Deterministically Daring Ping-Pong Ball



Non-negotiable physics

Conjecture (Quantum can play ping-pong safely)

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

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

On the Nuisance of Nuances of Physics

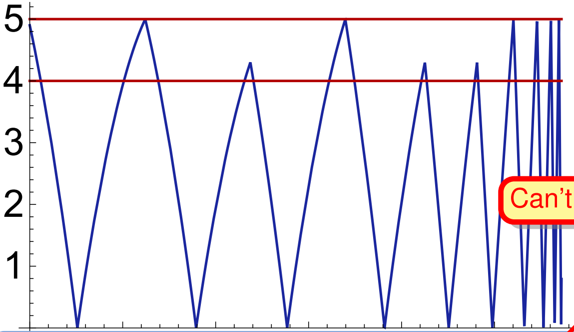
Non-negotiability of Physics

1. Making systems safe by construction is a great idea. For control!
2. But not by changing the laws of physics.
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



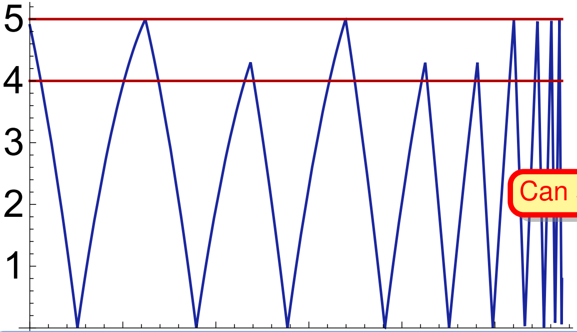
Can't stop the world for an event

Conjecture (Quantum can play ping-pong safely)

$$\begin{aligned}&0 \leq x \land x \leq 5 \land v \leq 0 \land g > 0 \land 1 \geq c \geq 0 \land f \geq 0 \to \\ &\quad \big[\big((\{x' = v, v' = -g \,\&\, x \geq 0 \land x \leq 5\}); \\ &\qquad \text{if}(x{=}0)\, v := -cv \,\text{else}\,\text{if}(4{\leq}x{\leq}5)\, v := -fv\big)^*\big](0{\leq}x{\leq}5)\end{aligned}$$

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

Quantum the Deterministically Daring Ping-Pong Ball

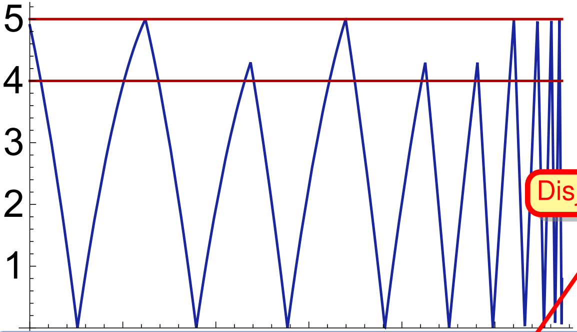


Can split the world for an event

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes



Disjoint domains

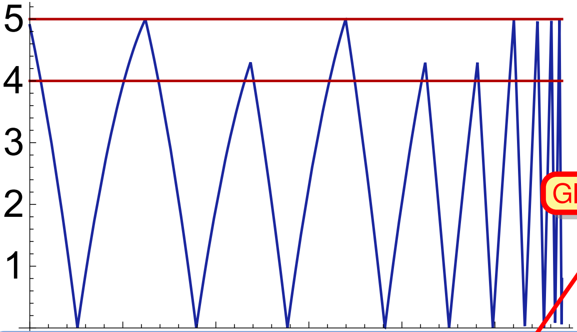
Shattered the world

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes

Quantum the Deterministically Daring Ping-Pong Ball



Glue domains

Reunite the world

Conjecture (Quantum can play ping-pong safely)

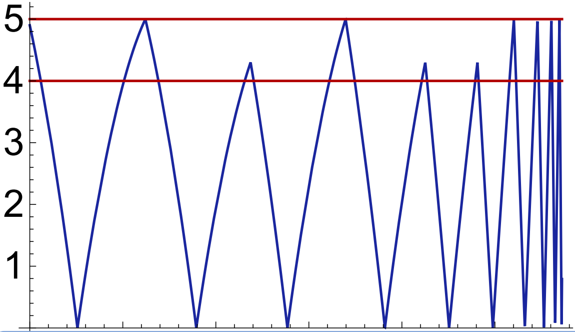
$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \to \\ \Big[\big((\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5\} \cup \{x' = v, v' = -g \,\&\, x \ge 5\}); \\ \text{if}(x=0)\, v := -cv \,\text{else if}(4 \le x \le 5)\, v := -fv\big)^*\Big](0 \le x \le 5)$$

Proof? Ask René Descartes

Connected evolution domains

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

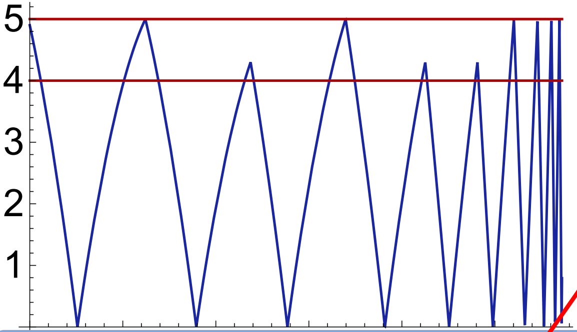
1. Splitting the state space into different regions to detect events is fine.
2. Destroying the world is not.
3. Not even by poking infinitesimal holes into the time-space continuum.



Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes

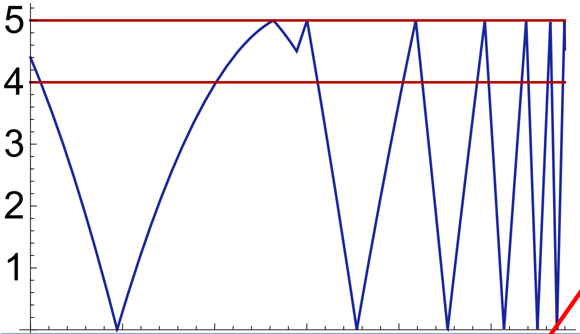


Multi-fire

Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes

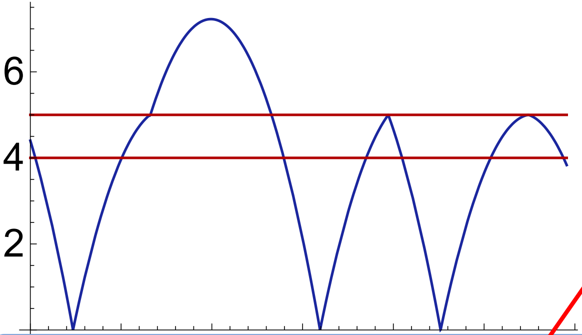


Conjecture (Quantum can play ping-pong safely)

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

Proof? Ask René Descartes

Quantum the Deterministically Daring Ping-Pong Ball



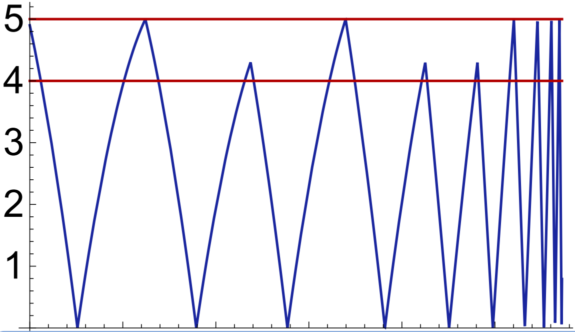
Multi-fire

Conjecture (Quantum can play ping-pong safely)

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

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)

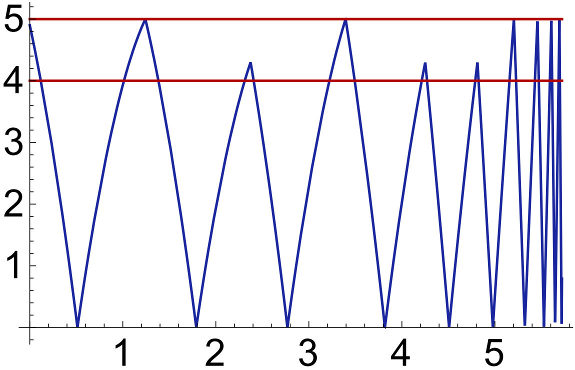
$$0 \le x \land x \le 5 \land v \le 0 \land g > 0 \land 1 \ge c \ge 0 \land f \ge 0 \rightarrow$$
$$\big[\big(\big(\{x' = v, v' = -g \,\&\, x \ge 0 \land x \le 5\} \cup \{x' = v, v' = -g \,\&\, x \ge 5\}\big);$$
$$\text{if}(x=0)\, v := -cv \,\text{else if}(4 \le x \le 5 \land v \ge 0)\, v := -fv\big)^*\big](0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

Proof? Ask René Descartes

Multi-firing 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

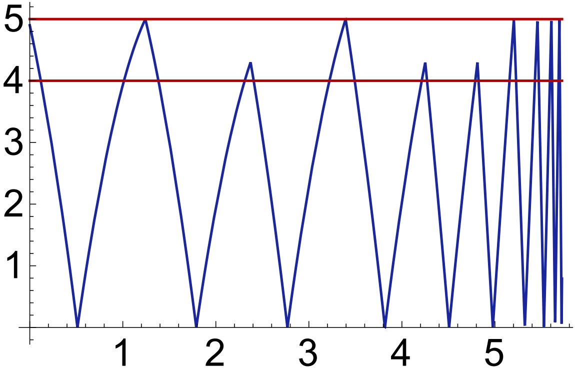


control: robust, all cases
physics: precise

Conjecture (Quantum can play ping-pong safely)

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

Physics vs. Control: Classification



control: robust, all cases

physics: precise

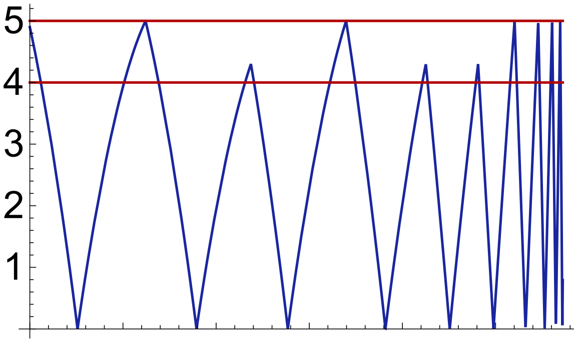
Conjecture (Quantum can play ping-pong safely)

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

Quantum's Ping-Pong Proof Invariants

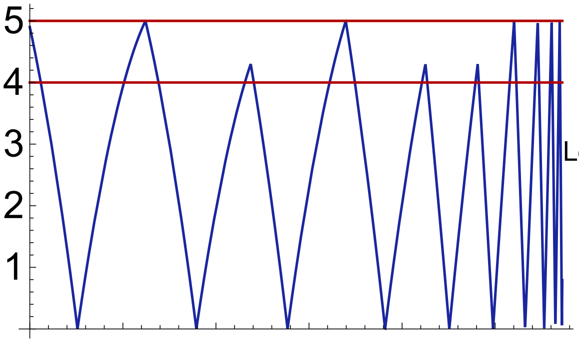
Proposition (Quantum can play ping-pong safely)

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



Proposition (Quantum can play ping-pong safely)

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

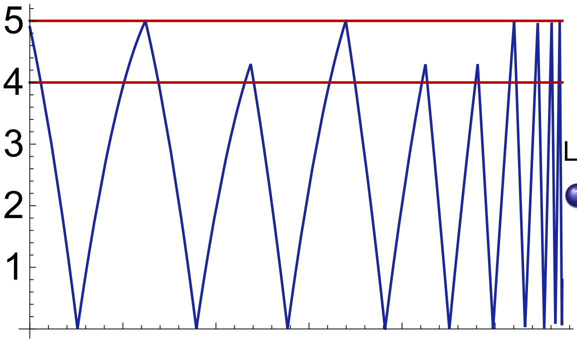


Loop invariant $j(x, v)$:

Quantum's Ping-Pong Proof Invariants

Proposition (Quantum can play ping-pong safely)

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



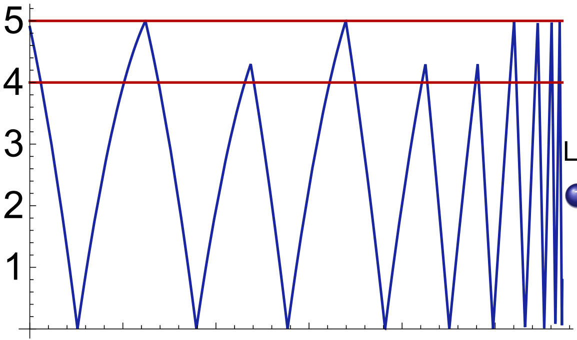
Loop invariant $j(x, v)$:

1. $0 \leq x \leq 5$

Quantum's Ping-Pong Proof Invariants

Proposition (Quantum can play ping-pong safely)

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



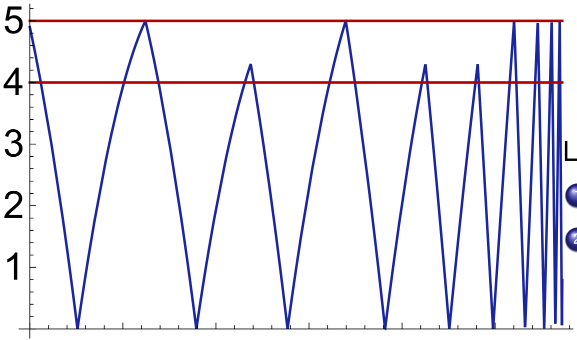
Loop invariant $j(x,v)$:

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

Quantum's Ping-Pong Proof Invariants

Proposition (Quantum can play ping-pong safely)

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



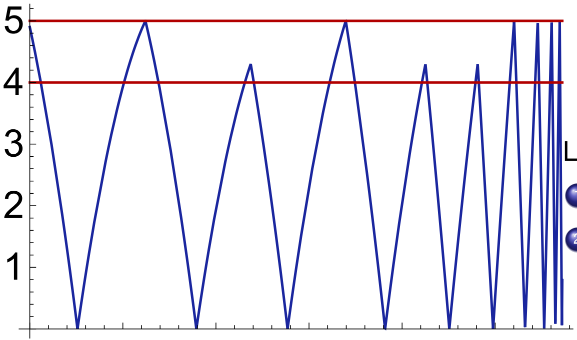
Loop invariant $j(x, v)$:

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)

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



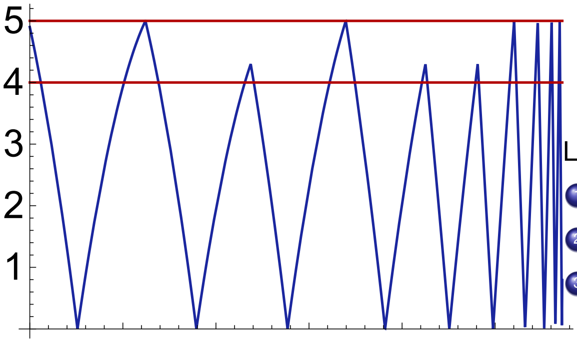
Loop invariant $j(x, v)$:

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

Quantum's Ping-Pong Proof Invariants

Proposition (Quantum can play ping-pong safely)

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



Loop invariant $j(x, v)$:

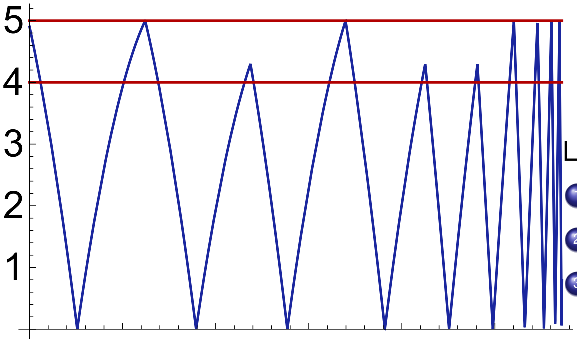
1. $0 \leq x \leq 5$ not inductive
2. $0 \leq x \leq 5 \land v \leq 0$ not inductive
3. $0 \leq x \leq 5 \land (x=5 \rightarrow v \leq 0)$

Quantum's Ping-Pong Proof Invariants

Proposition (Quantum can play ping-pong safely)

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

Proof **@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!

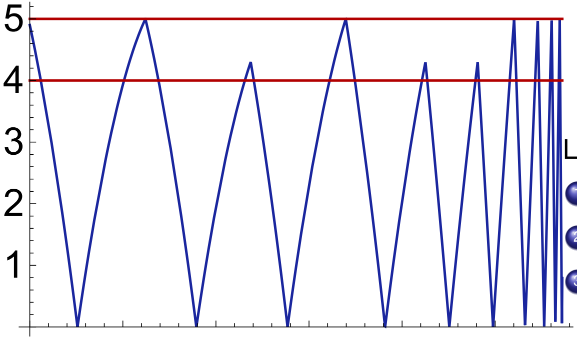
Quantum's Ping-Pong Proof Invariants

Proposition (Quantum can play ping-pong safely)

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

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

Just can't implement ...



Loop invariant $j(x, v)$:

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

Outline

Summary: Event-triggered Control

1. One important principle for designing feedback mechanisms
2. Conceptually simple: detect all relevant events and respond correctly
3. Assumes all events are surely detected
4. Implementation: Requires continuous sensing
   Tell me if you ever find a faithful implementation platform ...
5. Robust events, not just: if$(x = 9.8696)$ ...
6. Events have subtle models, but make design and verification easier!
   Non-negotiability of Physics | Connected domains | Multi-firing
7. Useful abstraction when system evolves slowly but senses quickly
8. Verify event-triggered model as first step
9. Then refine toward realistic implementation based on safe event-triggered design
10. Physics $\neq$ Control

Non-negotiability of Physics

1. Making systems safe by construction is a great idea. For control!
2. But not by changing the laws of physics.
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.
Logical Foundations of Cyber-Physical Systems.
Springer, Switzerland, 2018.
URL: http://www.springer.com/978-3-319-63587-3,
doi:10.1007/978-3-319-63588-0.

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

Sarah M. Loos and André Platzer.
Differential refinement logic.
In Martin Grohe, Eric Koskinen, and Natarajan Shankar, editors, *LICS*, pages 505–514, New York, 2016. ACM.
doi:10.1145/2933575.2934555.