

04: Safety & Contracts

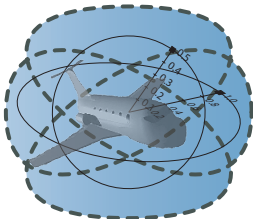
15-424: Foundations of Cyber-Physical Systems

André Platzer

aplatzer@cs.cmu.edu

Computer Science Department

Carnegie Mellon University, Pittsburgh, PA

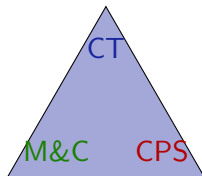


- 1 Learning Objectives
- 2 Quantum the Acrophobic Bouncing Ball
- 3 Contracts for CPS
 - Safety of Robots
 - Safety of Bouncing Balls

- 1 Learning Objectives
- 2 Quantum the Acrophobic Bouncing Ball
- 3 Contracts for CPS
 - Safety of Robots
 - Safety of Bouncing Balls

Learning Objectives: Safety & Contracts

rigorous specification
contracts
preconditions
postconditions
differential dynamic logic

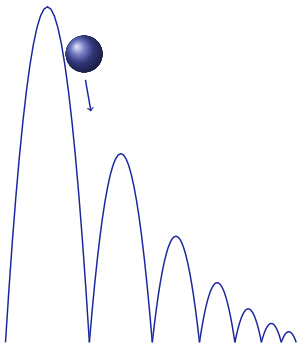


discrete+continuous
analytic reasoning

model semantics
reasoning principles

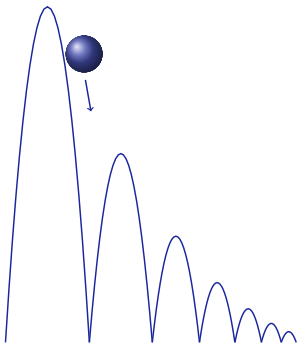
- 1 Learning Objectives
- 2 Quantum the Acrophobic Bouncing Ball
- 3 Contracts for CPS
 - Safety of Robots
 - Safety of Bouncing Balls

Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

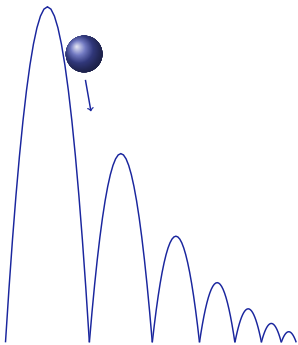
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$x' = v, v' = -g \ \& \ x \geq 0$$

Quantum the Acrophobic Bouncing Ball

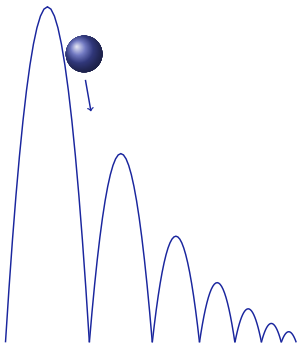


Example (Quantum the Bouncing Ball)

$$x' = v, v' = -g \ \& \ x \geq 0;$$

$$\text{if}(x = 0) \ v := -cv$$

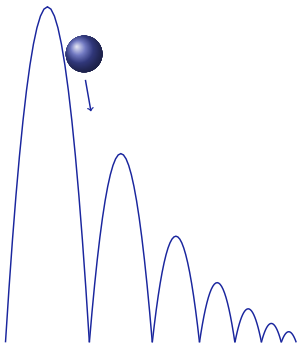
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$\begin{aligned} &(x' = v, v' = -g \ \& \ x \geq 0; \\ &\text{if}(x = 0) \ v := -cv)^* \end{aligned}$$

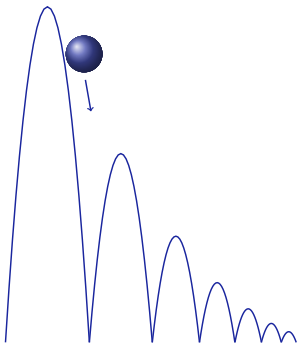
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$\begin{aligned} &(x' = v, v' = -g \ \& \ x \geq 0; \\ &\text{if}(x = 0) \ v := -cv)^* \end{aligned}$$

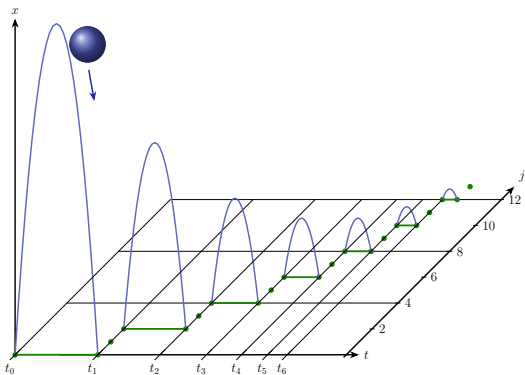
Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

$$(x' = v, v' = -g \ \& \ x \geq 0;$$
$$\text{if}(x = 0) \ v := -cv)^*$$

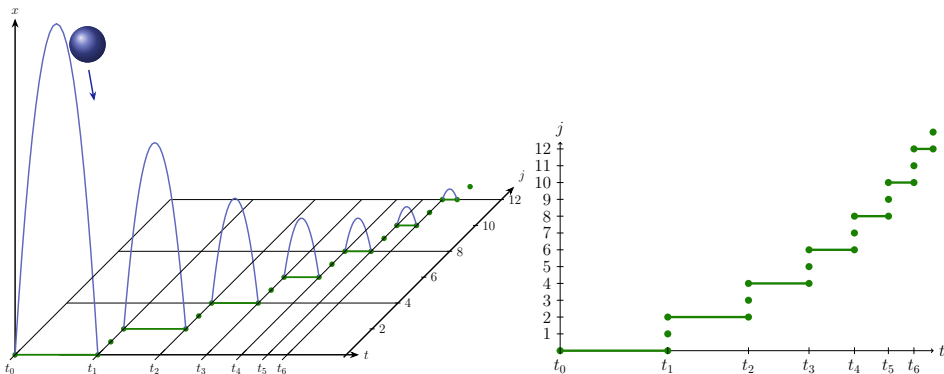
Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

$$(x' = v, v' = -g \ \& \ x \geq 0; \\ \text{if}(x = 0) \ v := -cv)^*$$

Quantum Discovered a Crack in the Fabric of Time



Example (Quantum the Bouncing Ball)

$$\begin{aligned} (x' = v, v' = -g \ \& \ x \geq 0; \\ \text{if}(x = 0) \ v := -cv)^* \end{aligned}$$

- 1 Learning Objectives
- 2 Quantum the Acrophobic Bouncing Ball
- 3 **Contracts for CPS**
 - Safety of Robots
 - Safety of Bouncing Balls

Three Laws of Robotics

Isaac Asimov

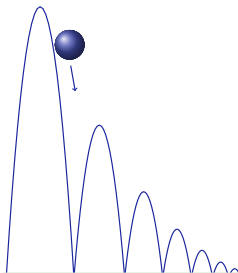
- 1 A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- 2 A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
- 3 A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Three Laws of Robotics

Isaac Asimov

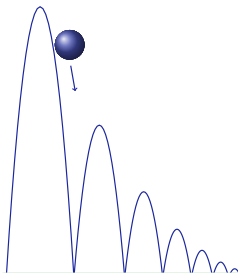
- 1 A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- 2 A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
- 3 A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

Three Laws of Robotics are not the answer.
They are the inspiration!



Example (Quantum the Bouncing Ball)

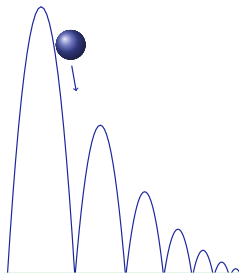
$$(x' = v, v' = -g \ \& \ x \geq 0; \\ \text{if}(x = 0) \ v := -cv)^*$$



Example (Quantum the Bouncing Ball)

@ensures($0 \leq x$)

$(x' = v, v' = -g \ \& \ x \geq 0;$
 $\text{if}(x = 0) \ v := -cv)^*$



Example (Quantum the Bouncing Ball)

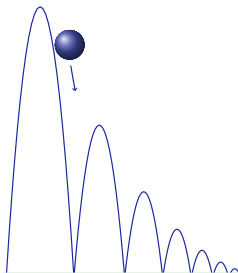
@ensures($0 \leq x$)

@ensures($x \leq H$)

($x' = v, v' = -g \ \& \ x \geq 0;$

if($x = 0$) $v := -cv$)*

Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

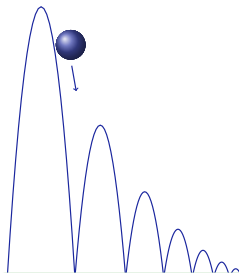
@requires($x = H$)

@ensures($0 \leq x$)

@ensures($x \leq H$)

($x' = v, v' = -g \ \& \ x \geq 0;$

if($x = 0$) $v := -cv$)*



Example (Quantum the Bouncing Ball)

@requires($x = H$)

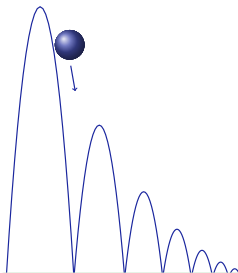
@requires($0 \leq H$)

@ensures($0 \leq x$)

@ensures($x \leq H$)

($x' = v, v' = -g \ \& \ x \geq 0;$

if($x = 0$) $v := -cv$)*



Example (Quantum the Bouncing Ball)

@requires($x = H$)

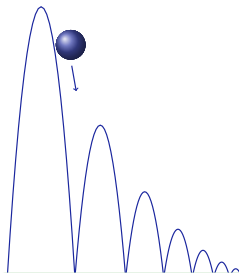
@requires($0 \leq H$)

@ensures($0 \leq x$)

@ensures($x \leq H$)

($x' = v, v' = -g \ \& \ x \geq 0;$

if($x = 0$) $v := -cv$)^{*} @invariant($x \geq 0$)



Example (Quantum the Bouncing Ball)

@requires($x = H$)

@requires($0 \leq H$)

@ensures($0 \leq x$)

@ensures($x \leq H$)

($x' = v, v' = -g \ \& \ x \geq 0;$

$\text{if}(x = 0) \ v := -cv)^* \text{@invariant}(x \geq 0)$

Developed on the board:

- 1 Differential dynamic logic $d\mathcal{L}$ as a precise specification language for CPS
- 2 Translation of contracts for bouncing ball to logical formula in $d\mathcal{L}$
- 3 Syntax and semantics of $d\mathcal{L}$

See lecture notes for details [1].



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.