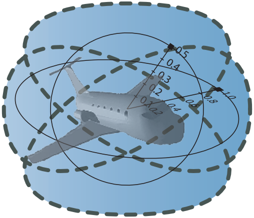
04: Safety & Contracts

15-424: Foundations of Cyber-Physical Systems

André Platzer

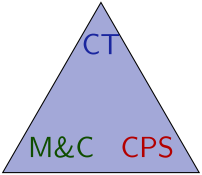
aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA



Outline

Outline

rigorous specification
contracts
preconditions
postconditions
differential dynamic logic

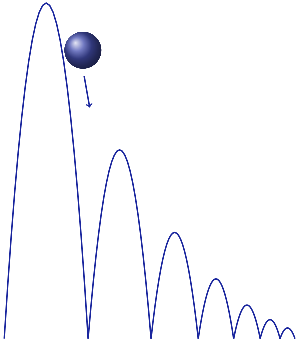


discrete+continuous
analytic specification

model semantics
reasoning principles

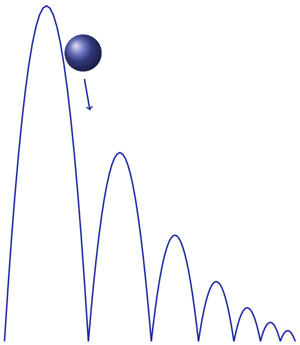
Outline

Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

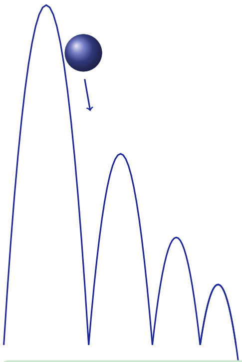
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$x' = v, v' = -g$$

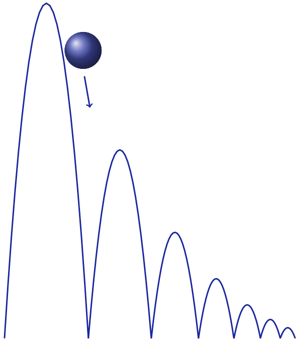
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$x' = v, v' = -g$$

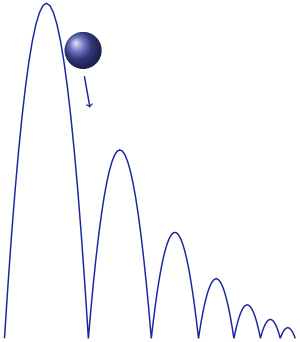
Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

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

Quantum the Acrophobic Bouncing Ball

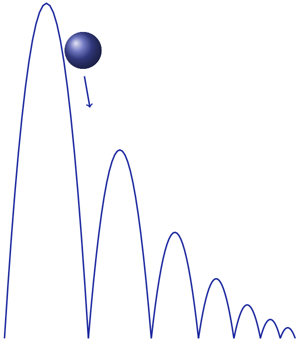


Example (Quantum the Bouncing Ball)

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

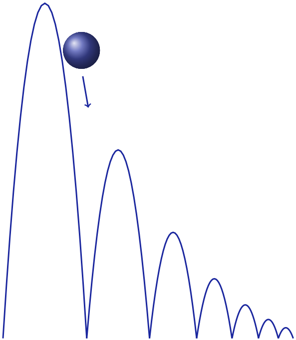
$$\text{if}(x = 0)\; v := -cv$$

Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

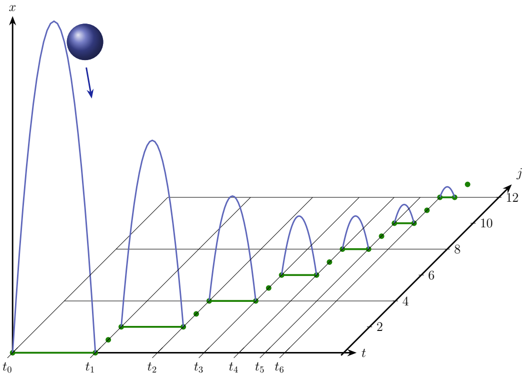
$$\left(x' = v, v' = -g \,\&\, x \geq 0;\right.$$
$$\left.\text{if}(x = 0)\; v := -cv\right)^*$$



Example (Quantum the Bouncing Ball)

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

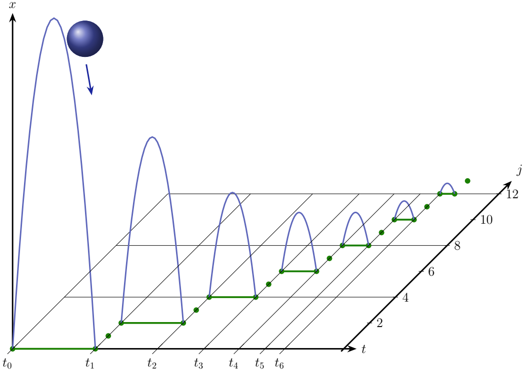
Quantum Discovered a Crack in the Fabric of Time

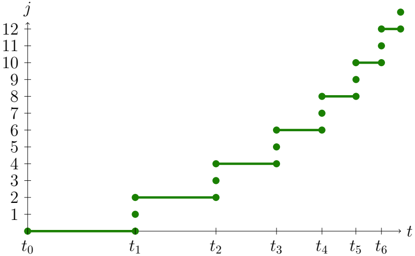


Example (Quantum the Bouncing Ball)

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

Quantum Discovered a Crack in the Fabric of Time





Example (Quantum the Bouncing Ball)

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

Outline

Safety of Robots

Safety of Robots

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.

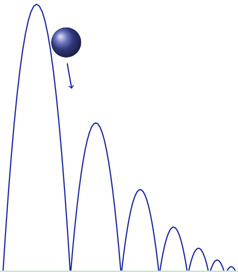
Safety of Robots

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!

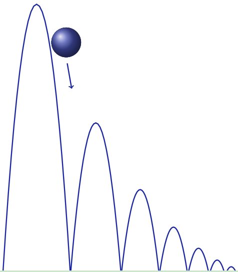
Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

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

Contracts for Quantum the Acrophobic Bouncing Ball

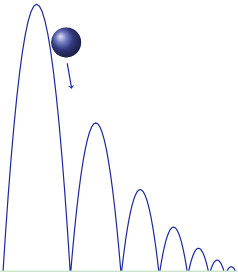


Example (Quantum the Bouncing Ball)

$$@\text{ensures}(0 \le x)$$

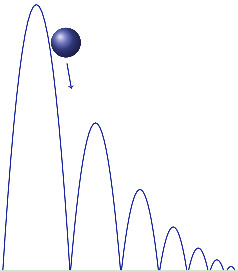
$$\big(x' = v, v' = -g \,\&\, x \ge 0;$$
$$\text{if}(x = 0)\, v := -cv\big)^*$$

Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$
\begin{aligned}
&@\text{ensures}(0 \le x)\\
&\color{red}{@\text{ensures}(x \le H)}\\
&\big(x' = v, v' = -g \,\&\, x \ge 0;\\
&\quad \text{if}(x = 0)\, v := -cv\big)^*
\end{aligned}
$$



Example (Quantum the Bouncing Ball)

$$@\mathrm{requires}(x = H)$$

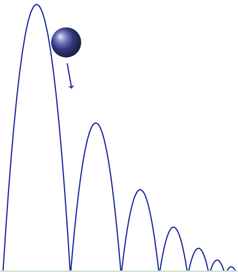
$$@\mathrm{ensures}(0 \le x)$$

$$@\mathrm{ensures}(x \le H)$$

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

$$\mathrm{if}(x = 0)\, v := -cv\big)^*$$

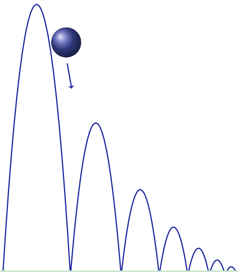
Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$
\begin{aligned}
&@\mathrm{requires}(x = H)\\
&@\mathrm{requires}(0 \le H)\\
&@\mathrm{ensures}(0 \le x)\\
&@\mathrm{ensures}(x \le H)\\
&\big(x' = v, v' = -g \,\&\, x \ge 0;\\
&\quad \mathrm{if}(x = 0)\, v := -cv\big)^*
\end{aligned}
$$

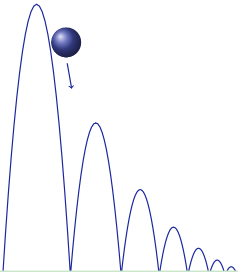
Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$@\mathrm{requires}(x = H)$$
$$@\mathrm{requires}(0 \le H)$$
$$@\mathrm{ensures}(0 \le x)$$
$$@\mathrm{ensures}(x \le H)$$
$$\big(x' = v, v' = -g \,\&\, x \ge 0;$$
$$\mathrm{if}(x = 0)\, v := -cv\big)^* @\mathrm{invariant}(x \ge 0)$$

Contracts for Quantum the Acrophobic Bouncing Ball



Example (Quantum the Bouncing Ball)

$$
\begin{aligned}
&@\mathrm{requires}(x = H)\\
&@\mathrm{requires}(0 \le H)\\
&@\mathrm{ensures}(0 \le x)\\
&@\mathrm{ensures}(x \le H)\\
&\big(x' = v, v' = -g \,\&\, x \ge 0;\\
&\quad \mathrm{if}(x = 0)\, v := -cv\big)^{*} @\mathrm{invariant}(x \ge 0)
\end{aligned}
$$

Developed on the board:

1. Differential dynamic logic dL as a precise specification language for CPS
2. Translation of contracts for bouncing ball to logical formula in dL
3. Syntax and semantics of dL

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.