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

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

CT

M&C

CPS

discrete+continuous
analytic reasoning

model semantics
reasoning principles

Andrée Platzer (CMU)
Outline

1. Learning Objectives

2. Quantum the Acrophobic Bouncing Ball

3. Contracts for CPS
   - Safety of Robots
   - Safety of Bouncing Balls
Example (Quantum the Bouncing Ball)
Example (Quantum the Bouncing Ball)

\[ x' = v, \quad v' = -g \quad \& \quad x \geq 0 \]
Example (Quantum the Bouncing Ball)

\[ x' = v, \quad v' = -g \quad \& \quad x \geq 0; \]
\[ \text{if}(x = 0) \quad v := -cv \]
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)

\[(x' = v, v' = -g \land x \geq 0;\]
\[\text{if}(x = 0) v := -cv)\]

*Andre Platzer (CMU)*
Quantum Discovered a Crack in the Fabric of Time

Example (Quantum the Bouncing Ball)

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

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

\(\text{if}(x = 0) v := -cv)\)
1. Learning Objectives

2. Quantum the Acrophobic Bouncing Ball

3. Contracts for CPS
   - Safety of Robots
   - Safety of Bouncing Balls
Safety of Robots

A robot may not injure a human being or, through inaction, allow a human being to come to harm.

A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.

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!

André Platzer (CMU)
## Safety of Robots

### Three Laws of Robotics

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.

---

 Andrés Platzer (CMU)  
 FCPS / 04: Safety & Contracts
### Three Laws of Robotics

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

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

---

André Platzer  (CMU)  
FCPS / 04: Safety & Contracts
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 ≤ x)

\[ (x' = v, v' = -g & x ≥ 0; \text{if}(x = 0) v := -cv)^* \]
@requires \( x = H \)
@requires \( 0 \leq H \)
@ensures \( 0 \leq x \)
@ensures \( x \leq H \)
\( (x' = v, v' = -g \& x \geq 0; \)
\( \text{if}(x = 0) v := -cv) \)
Example (Quantum the Bouncing Ball)

```plaintext
@requires(x = H)
@ensures(0 ≤ x)
@ensures(x ≤ H)
(x' = v, v' = -g & x ≥ 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 ≤ H)
@ensures(0 ≤ x)
@ensures(x ≤ H)
(x' = v, v' = −g & x ≥ 0; if(x = 0) v := −cv)\* @invariant(x ≥ 0)
Example (Quantum the Bouncing Ball)

@requires(x = H)
@requires(0 ≤ H)
@ensures(0 ≤ x)
@ensures(x ≤ H)
\(x' = v, v' = -g \& x \geq 0;\)
\[\text{if}(x = 0) v := -cv\]  
@invariant(x ≥ 0)
Developed on the board:

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

See lecture notes for details [1].
André Platzer.
Foundations of cyber-physical systems.

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