15-819/18-879: Logical Analysis of Hybrid Systems
01: Hybrid Systems Applications

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA
1 Hybrid Systems Applications

- Air Traffic Control
- Hybrid Systems / Cyber-Physical Systems
- Train Control
- Car Control
- UAV
- Chemical/Physical Process Control
- Biomedical Applications
- Advanced Chip Design
How can we build computerized controllers for physical systems that are guaranteed to meet their design goals?
Hybrid systems
Logical analysis
Symbolic / numerical techniques
Automatic theorem proving
Model checking
Verification
Balance theory, practice & applications
30% Homework, 15% Midterm, 55% Project
Project: Theory and/or implementation and/or application
Whitepaper (4p), proposal (10p), report
Course Outline

1. Safety-critical complex physical systems
2. Dynamical systems: discrete, continuous, hybrid
3. Controllability, safety & stability
4. First-order logic and first-order real arithmetic
5. Symbolic reachability analysis
6. Hybrid programs and hybrid automata
7. Dynamic logic & dynamical systems, differential dynamic logic
8. Differential variance and invariance
9. Differential-algebraic equations and differential algebra
10. Differential transformations and differential reductions
11. Railway control applications
12. Air traffic control applications
13. Distributed car control applications
Differential equations
Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
Differential equations (Peano, Picard-Lindelöf, Cauchy-Lipschitz)
First-order logic
• Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
• First-order logic
• Hybrid systems
Differential equations (Peano, Picard-Lindelöf, Cauchy-Lipschitz)
First-order logic
Hybrid systems
Deduction & formal proofs
Differential equations (Peano, Picard-Lindelöf, Cauchy-Lipschitz)
First-order logic
Hybrid systems
Deduction & formal proofs
Model checking
- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs
- Model checking
- Quantifier elimination
Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
First-order logic
Hybrid systems
Deduction & formal proofs
Model checking
Quantifier elimination
Algebraic geometry
Differential equations (Peano, Picard-Lindelöf, Cauchy-Lipschitz)
First-order logic
Hybrid systems
Deduction & formal proofs
Model checking
Quantifier elimination
Algebraic geometry
Differential algebra
- Differential equations (Peano, Picard-Lindelöff, Cauchy-Lipschitz)
- First-order logic
- Hybrid systems
- Deduction & formal proofs
- Model checking
- Quantifier elimination
- Algebraic geometry
- Differential algebra
- Computer algebra
Logical Analysis of Hybrid Systems

- Logic
- Model Checking
- Proof Calculus
- Theorem Proving
- Computer Algebra
- Algebraic Geometry
- Algebra
- Differential Algebra
- Differential Equations
- Dynamical Systems
- Analysis
- Differentiation
- Algorithms
- Decision Procedures
- Proof Strategies
- Fixedpoint Loops

André Platzer (CMU)
André Platzer. 
http://symbolaris.com/lahs/
Hybrid Systems Applications

- Air Traffic Control
- Hybrid Systems / Cyber-Physical Systems
- Train Control
- Car Control
- UAV
- Chemical/Physical Process Control
- Biomedical Applications
- Advanced Chip Design
Air Traffic Control

Hybrid Systems

interacting discrete and continuous dynamics
Hybrid Systems

interacting discrete and continuous dynamics
André Platzer (CMU)  LAHS/01: Hybrid Systems Applications  8 / 21

\[
\begin{bmatrix}
    x_1' = v \cos \vartheta \\
    y_1' = u \cos \varsigma \\
    x_2' = v \sin \vartheta \\
    y_2' = u \sin \varsigma
\end{bmatrix}
\]
Verification?
looks correct
Verification?
looks correct NO!
\[
\begin{align*}
\mathbf{x}_1' &= -v + u \cos \vartheta + \omega x_2 \\
\mathbf{x}_2' &= u \sin \vartheta - \omega x_1 \\
\vartheta' &= \omega - \omega
\end{align*}
\]

Verification?

looks correct **NO!**
Example ("Solving" differential equations)

\[
\begin{align*}
\dot{x}_1(t) &= \frac{1}{\omega \varpi} \left( x_1 \omega \varpi \cos \varpi \omega - u \omega \cos \varpi \omega \sin \vartheta + u \omega \cos \varpi \omega \cos \varpi \omega \sin \vartheta - v \varpi \sin \varpi \omega \right) \\
&\quad + x_2 \omega \varpi \sin \varpi \omega - u \omega \cos \vartheta \cos \varpi \omega \sin \varpi \omega - u \omega \sqrt{1 - \sin \vartheta^2} \sin \varpi \omega \\
&\quad + u \omega \cos \vartheta \cos \varpi \omega \sin \varpi \omega + u \omega \sin \vartheta \sin \varpi \omega \sin \varpi \omega \sin \varpi \omega \right) \ldots
\end{align*}
\]
Air Traffic Control

Example ("Solving" differential equations)

\[ \forall t \geq 0 \quad \frac{1}{\omega \varpi} \left( x_1 \omega \varpi \cos t \omega - u \omega \cos t \omega \sin \vartheta + u \omega \cos t \omega \cos t \varpi \sin \vartheta - v \varpi \sin t \omega \ight. \\
+ x_2 \omega \varpi \sin t \omega - u \omega \cos \vartheta \cos t \varpi \sin t \omega - u \omega \sqrt{1 - \sin \vartheta^2} \sin t \omega \\
+ u \omega \cos \vartheta \cos t \varpi \sin t \varpi + u \omega \sin \vartheta \sin t \omega \sin t \varpi \right) \ldots \]
Human at ATC detected conflict
Human instructed Tupolev to descend
TCAS instructed Tupolev to climb and Boeing to descend
Boeing couldn’t notify human (busy)
Pilots on both aircraft descended
Mid-air collision (less than a minute after conflict detected)
Mid-air Collision at Überlingen, Germany 2002
Mathematical model for complex physical systems:

**Definition (Hybrid Systems)**

systems with interacting discrete and continuous dynamics

Technical characteristics:

**Definition (Cyber-Physical Systems)**

(Distributed network of) computerized control for physical system
ETCS objectives:

1. Collision free
2. Maximise throughput & velocity (320 km/h = 200 mph)
3. $2.1 \times 10^6$ passengers/day
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

André Platzer (CMU)
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers:
   no NullPointerException ⇛ safe
Train Control

Challenge

Hybrid systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no NullPointerException ⇓ safe
2. More than physics: braking control $v^2 \leq 2b(MA - z) ⇓ safe$
Train Control

**Challenge**

Hybrid systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no NullPointerException ⇒ safe
2. More than physics: braking control \( v^2 \leq 2b(MA - z) \) ⇒ safe
3. Joint dynamics requires:

\[
SB \geq \frac{v^2}{2b} + \frac{a^2 \varepsilon^2}{2b} + \frac{a}{b} \varepsilon v + \frac{a}{2} \varepsilon^2 + \varepsilon v \ldots
\]
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

André Platzer (CMU)

LAHS/01: Hybrid Systems Applications
Train Control

Challenge

Hybrid systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

\[ SB \geq \frac{v^2}{2b} + \frac{a^2 \varepsilon^2}{2b} + \frac{a}{b} \varepsilon v + \frac{a}{2} \varepsilon^2 + \varepsilon v \]
Train Control

Challenge

Hybrid systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

∀ MA ⊃ SB “train always safe”
European Train Control System

Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

∀MA ∃SB “train always safe”
Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

∀MA ∃SB “train always safe”
Parametric Hybrid Systems

continuous evolution along differential equations + discrete change
Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

- Challenge: verification
- Which constraints for parameter $SB$?

$$\forall MA \exists SB \text{ "train always safe"}$$
- Train engineer disobeyed stop signal at single track section
- No warning issued to train dispatcher
- First sight 4 seconds before impact
- Freight train triggers emergency brakes 2 seconds before impact
Head-on Train Collision at Chatsworth, CA 2008
Adaptive cruise control keeps safe distance?
Lane change assistant
Safe control with wireless interactions in CAR2CAR and USCAR
Virtual car platooning
UAV - Unmanned Aerial Vehicle Control
Safe and stable UAV flight control
Mixing UAV swarms into pilot flight control areas
Refueling of UAV: mixed human operation and micro turbulences
Many other robotic applications
Computerized Chemical/Physical Process Control

Control objective: Stabilize neutron multiplication factor.

André Platzer (CMU)
André Platzer (CMU)

LAHS/01: Hybrid Systems Applications

18 / 21

Computerized Chemical/Physical Process Control

Stabilize neutron multiplication factor

$e^{(k-1) \frac{t}{\lambda}}$

$k < 1$

$X$
Control objective

Stabilize neutron multiplication factor

\[ e^{(k-1) \frac{t}{\lambda}} \]

\[ k > 1 \]

\[ k < 1 \]
Biomedical Applications: Glucose/Insulin Regulation

Control objective
Maintain glucose in bounded range
Hybrid Effects in Chip Design

\[ I_C \]

\[ L \]

\[ C_1 \]

\[ C_2 \]
Hybrid Systems Analysis is Important for . . .