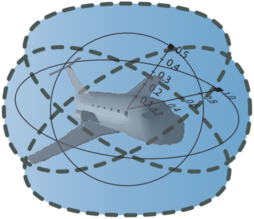
15-819/18-879: Hybrid Systems Analysis & Theorem Proving

01: Safety-critical Hybrid Systems

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon /University, Pittsburgh, PA



Outline

1. Applications
   - Air Traffic Control
   - Hybrid Systems / Cyber-Physical Systems
   - Train Control
   - Car Control
   - UAV
   - Chemical/Physical Process Control
   - Biomedical Applications
   - Advanced Chip Design
2. Hybrid Systems
   - Labeled Transition Systems
   - Finite Automata
   - Hybrid Automata
   - Hybrid Systems
3. Differential Equations

How can we build computerized controllers for physical systems that are guaranteed to meet their design goals?

About 15-819/18-879

- Hybrid systems
- Logic-based 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 Hybrid Systems
2. Propositional Logic
3. First-order Logic
4. Numerical Analysis versus Symbolic Verification
5. Propositional Tableau Procedures
6. First-order Tableau Procedures
7. Dynamic Logic Programs and Dynamical Systems
8. Hybrid Dynamical Systems & Hybrid Programs
9. Aircraft, Train, and Car Control
10. Dynamic Verification Calculi
11. Decision Procedures
12. Theorem Proving Modulo
13. Differential Equations, Differential Variance and Invariance
14. Disturbances in Hybrid Systems Control
15. *Proof Theory of Hybrid Systems*
16. *Fixedpoint Model Checking Engines*

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic
- First-order logic

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic
- First-order logic
- Automated theorem proving

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic
- First-order logic
- Automated theorem proving
- Model checking (discrete / hybrid)

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic
- First-order logic
- Automated theorem proving
- Model checking (discrete / hybrid)
- Quantifier elimination

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic
- First-order logic
- Automated theorem proving
- Model checking (discrete / hybrid)
- Quantifier elimination
- Algebraic geometry

Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic
- First-order logic
- Automated theorem proving
- Model checking (discrete / hybrid)
- Quantifier elimination
- Algebraic geometry
- Differential algebra

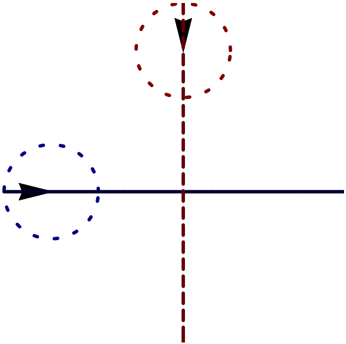
Questionnaire

- Differential equations (Peano, Picard, Lipschitz)
- Hybrid systems
- Propositional logic
- First-order logic
- Automated theorem proving
- Model checking (discrete / hybrid)
- Quantifier elimination
- Algebraic geometry
- Differential algebra
- Computer algebra

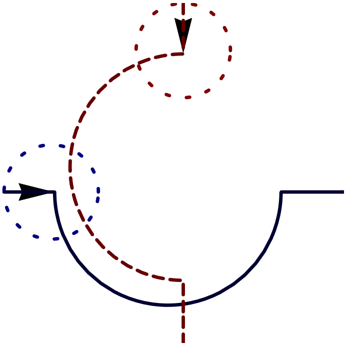
Outline

1. Applications
   - Air Traffic Control
   - Hybrid Systems / Cyber-Physical Systems
   - Train Control
   - Car Control
   - UAV
   - Chemical/Physical Process Control
   - Biomedical Applications
   - Advanced Chip Design
2. Hybrid Systems
   - Labeled Transition Systems
   - Finite Automata
   - Hybrid Automata
   - Hybrid Systems
3. Differential Equations

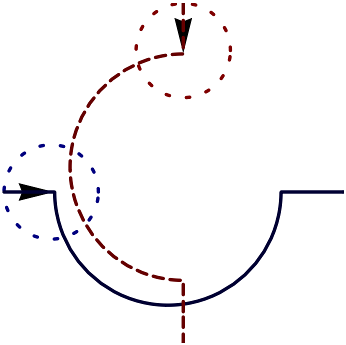
Air Traffic Control



Air Traffic Control

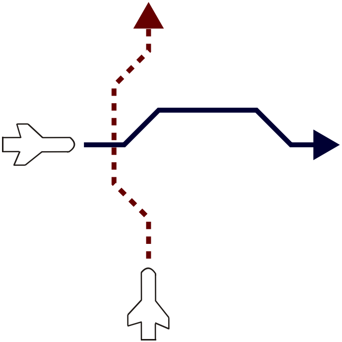


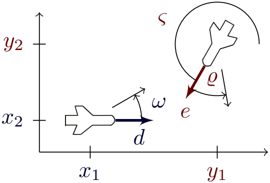
Air Traffic Control



Hybrid Systems

interacting discrete and continuous dynamics



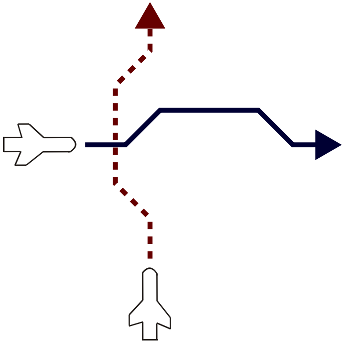


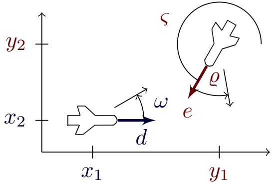
$$\begin{bmatrix} x_1' = v\cos\vartheta & y_1' = u\cos\varsigma \\ x_2' = v\sin\vartheta & y_2' = u\sin\varsigma \end{bmatrix}$$

Hybrid Systems

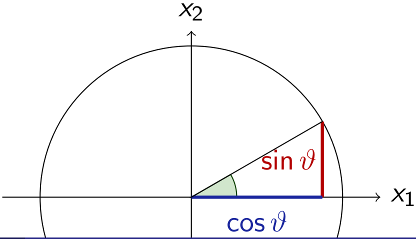
interacting discrete and continuous dynamics

Air Traffic Control

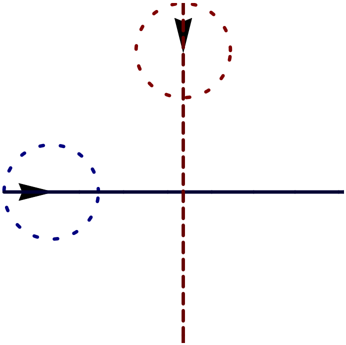




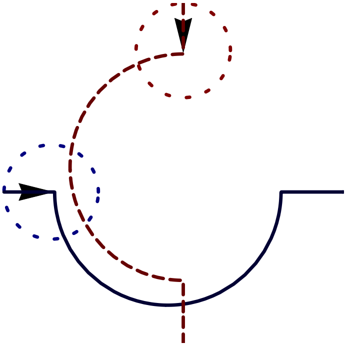
$$\begin{bmatrix} x_1' = v\cos\vartheta & y_1' = u\cos\varsigma \\ x_2' = v\sin\vartheta & y_2' = u\sin\varsigma \end{bmatrix}$$



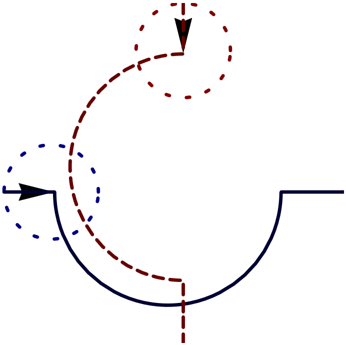
Air Traffic Control



Air Traffic Control



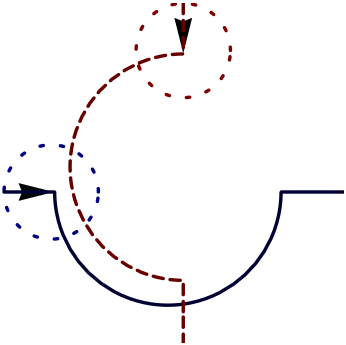
Air Traffic Control

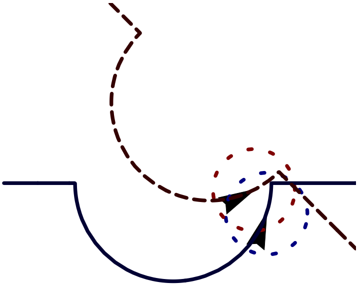


Verification?

looks correct

Air Traffic Control

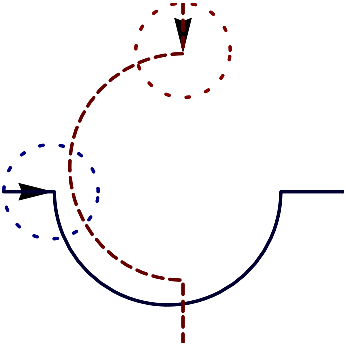


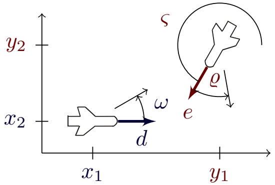


Verification?

looks correct NO!

Air Traffic Control



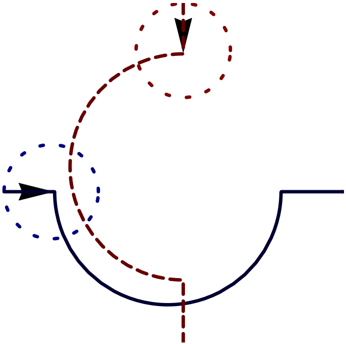


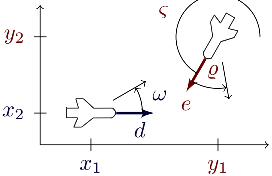
$$\begin{bmatrix} x_1' = -v + u\cos\vartheta + \omega x_2 \\ x_2' = u\sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Verification?

looks correct NO!

Air Traffic Control



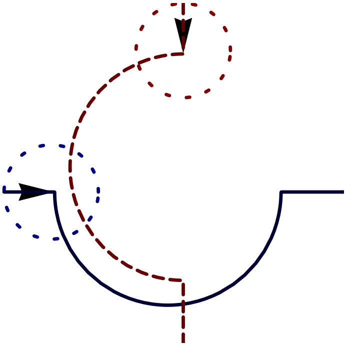


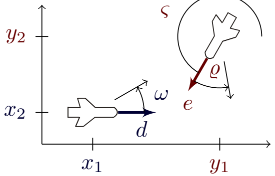
$$\begin{bmatrix} x_1' = -v + u\cos\vartheta + \omega x_2 \\ x_2' = u\sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

$$x_1(t) = \frac{1}{\omega\varpi}\big(x_1\omega\varpi\cos t\omega - u\omega\cos t\omega\sin\vartheta + u\omega\cos t\omega\cos t\varpi\sin\vartheta - v\varpi\sin t\omega$$
$$+ x_2\omega\varpi\sin t\omega - u\omega\cos\vartheta\cos t\varpi\sin t\omega - u\omega\sqrt{1-\sin\vartheta^2}\sin t\omega$$
$$+ u\omega\cos\vartheta\cos t\omega\sin t\varpi + u\omega\sin\vartheta\sin t\omega\sin t\varpi\big)\ldots$$

Air Traffic Control





$$\begin{bmatrix} x_1' = -v + u\cos\vartheta + \omega x_2 \\ x_2' = u\sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

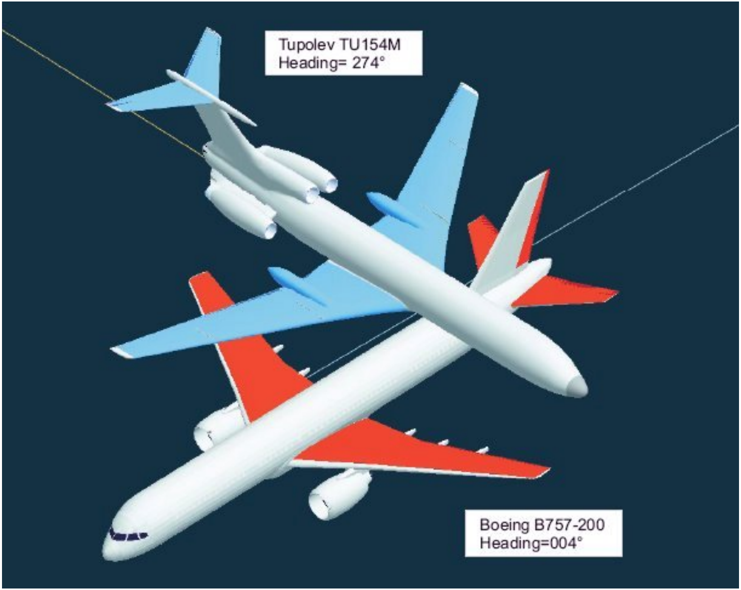
Example ("Solving" differential equations)

$$\forall t \geq 0 \quad \frac{1}{\omega\varpi}\Big(x_1\omega\varpi\cos t\omega - u\omega\cos t\omega\sin\vartheta + u\omega\cos t\omega\cos t\varpi\sin\vartheta - v\varpi\sin t\omega$$
$$+ x_2\omega\varpi\sin t\omega - u\omega\cos\vartheta\cos t\varpi\sin t\omega - u\omega\sqrt{1-\sin\vartheta^2}\sin t\omega$$
$$+ u\omega\cos\vartheta\cos t\omega\sin t\varpi + u\omega\sin\vartheta\sin t\omega\sin t\varpi\Big)\ldots$$

Mid-air Collision at Überlingen, Germany 2002

- 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



Hybrid Systems / Cyber-Physical Systems

Mathematical model for complex physical systems:

Definition (Hybrid Systems)

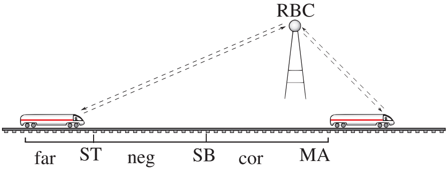
systems with interacting discrete and continuous dynamics

Technical characteristics:

Definition (Cyber-Physical Systems)

(Distributed network of) computerized control for physical system

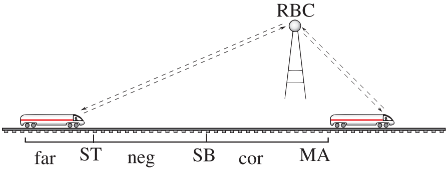
European Train Control System



ETCS objectives:

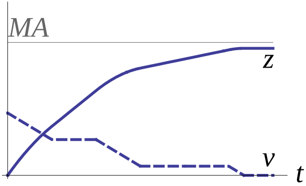
1. Collision free
2. Maximise throughput & velocity (320 km/h = 200 mph)
3. $2.1 * 10^6$ passengers/day

European Train Control System

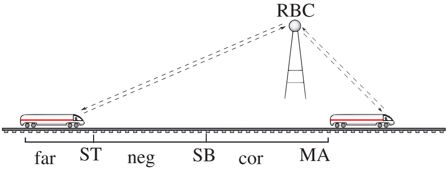


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

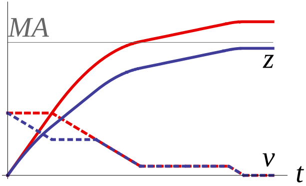


European Train Control System

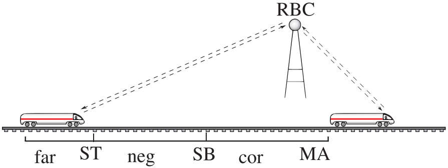


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

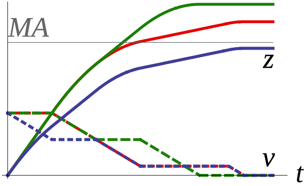


European Train Control System

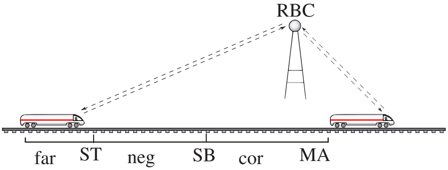


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change



European Train Control System

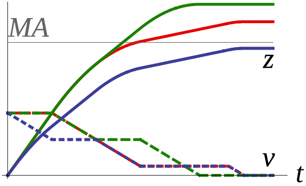


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

- Challenge: verification
- Which constraints for parameter SB?

$$\forall MA\, \exists SB \text{ “train always safe”}$$

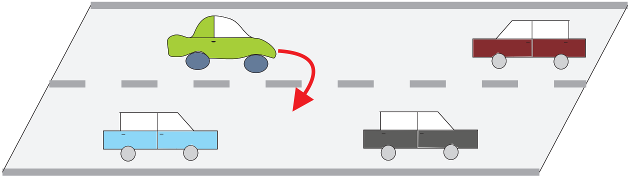


Head-on Train Collision at Chatsworth, CA 2008

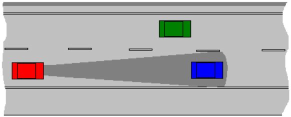
- Train engineer disobeyed stop signal at single track section
- No warning issued to train dispatcher
- First sight 4 seconds before impact
- Freight train triggers emergency brakes 2 seconds before impact

Head-on Train Collision at Chatsworth, CA 2008

Car Control



- Adaptive cruise control keeps safe distance?
- Lane change assistant
- Safe control with wireless interactions in CAR2CAR and USCAR
- Virtual car platooning

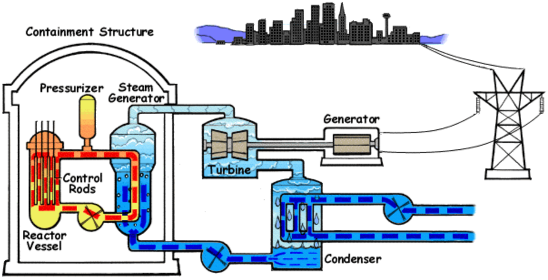


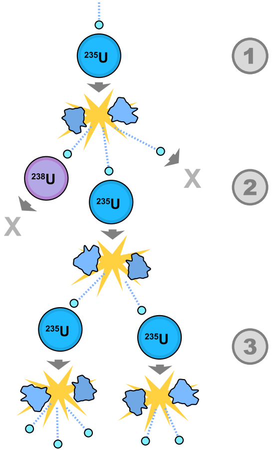
UAV - Unmanned Aerial Vehicle Control

UAV - Unmanned Aerial Vehicle Control

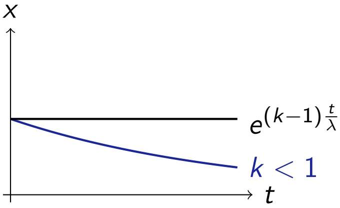
- Safe and stable UAV flight control
- Mixing UAV swarms into pilot flight control areas
- Refueling of UAV: mixed human operation and micro turbulences
- Many other robotic applications

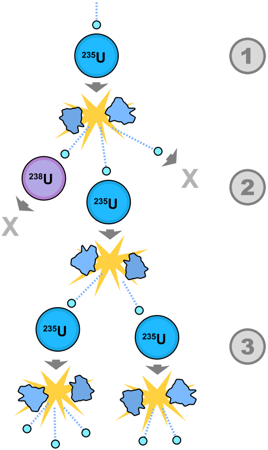
Computerized Chemical/Physical Process Control



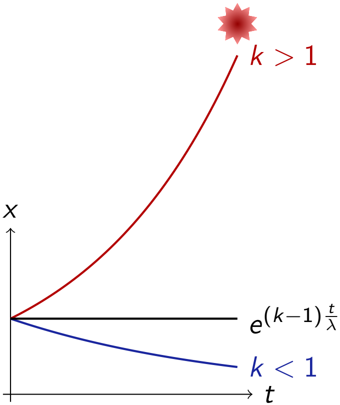


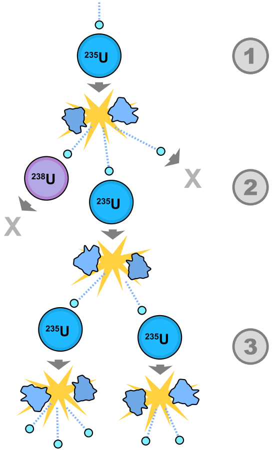
Computerized Chemical/Physical Process Control





Computerized Chemical/Physical Process Control

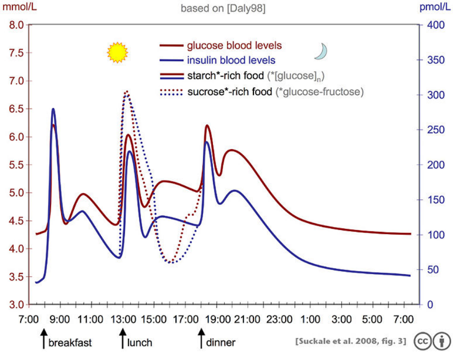




Control objective

Stabilize neutron multiplication factor

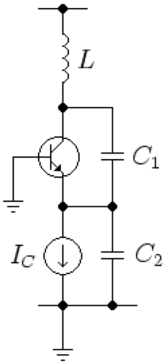
Biomedial Applications: Glucose/Insulin Regulation



Control objective

Maintain glucose in bounded range

Hybrid Effects in Chip Design



Outline

1. Applications
   - Air Traffic Control
   - Hybrid Systems / Cyber-Physical Systems
   - Train Control
   - Car Control
   - UAV
   - Chemical/Physical Process Control
   - Biomedical Applications
   - Advanced Chip Design
2. Hybrid Systems
   - Labeled Transition Systems
   - Finite Automata
   - Hybrid Automata
   - Hybrid Systems
3. Differential Equations

Labeled Transition Systems

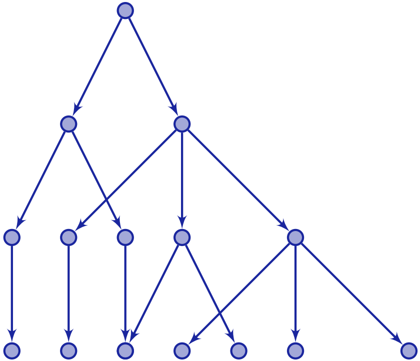
Definition (Labeled Transition System)

- Transition relation on $Q \times A \times Q$, denoted as $q \xrightarrow{a} q^+$, along with
- (possibly infinite) set A of transition actions,
- (possibly infinite) set Q of states.

Labeled Transition Systems

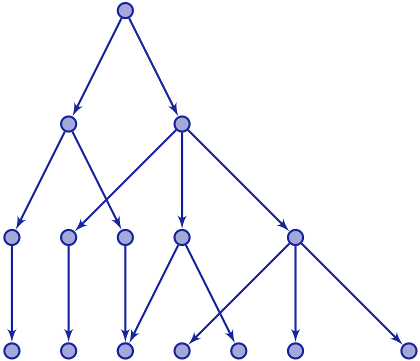
Definition (Labeled Transition System)

- Transition relation on $Q \times A \times Q$, denoted as $q \xrightarrow{a} q^+$, along with
- (possibly infinite) set A of transition actions,
- (possibly infinite) set Q of states.



Definition (Trace)

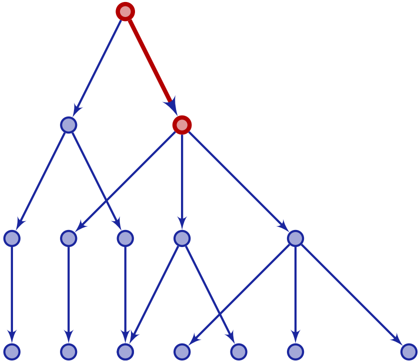
Finite/infinite series of states $q_0, q_1, q_2, \ldots \in Q$ such that $q_i \xrightarrow{a_i} q_{i+1}$ with some $a_i \in A$ for all i.



Labeled Transition Systems

Definition (Trace)

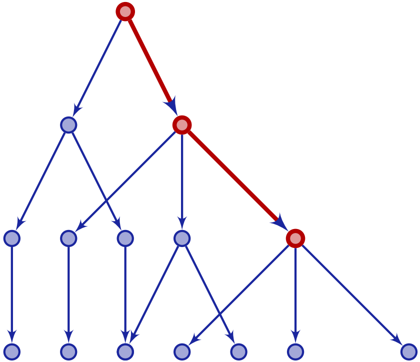
Finite/infinite series of states $q_0, q_1, q_2, \ldots \in Q$ such that $q_i \xrightarrow{a_i} q_{i+1}$ with some $a_i \in A$ for all i.



Labeled Transition Systems

Definition (Trace)

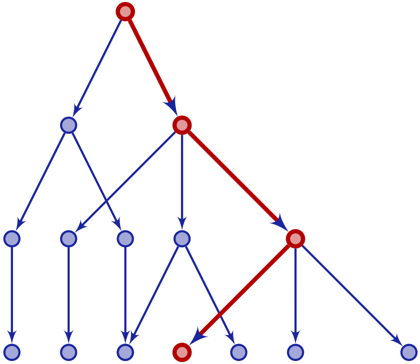
Finite/infinite series of states $q_0, q_1, q_2, \ldots \in Q$ such that $q_i \xrightarrow{a_i} q_{i+1}$ with some $a_i \in A$ for all i.



Labeled Transition Systems

Definition (Trace)

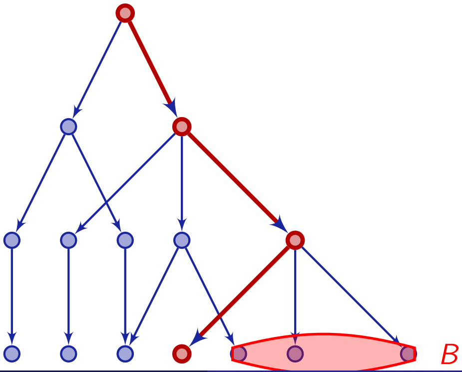
Finite/infinite series of states $q_0, q_1, q_2, \ldots \in Q$ such that $q_i \xrightarrow{a_i} q_{i+1}$ with some $a_i \in A$ for all i.



Labeled Transition Systems

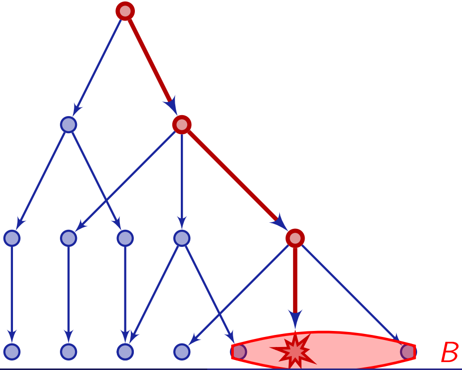
Definition (Model Checking Problem)

Given initial states $Q_0 \subseteq Q$ and bad states $B \subseteq Q$ for a transition system, check whether there is a trace from some $q_0 \in Q_0$ to some $q_b \in B$.



Definition (Model Checking Problem)

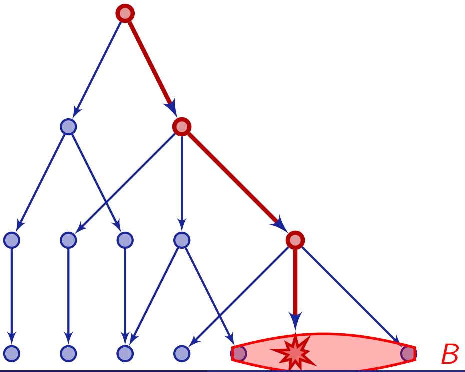
Given initial states $Q_0 \subseteq Q$ and bad states $B \subseteq Q$ for a transition system, check whether there is a trace from some $q_0 \in Q_0$ to some $q_b \in B$.



Labeled Transition Systems

Definition (Image Computation)

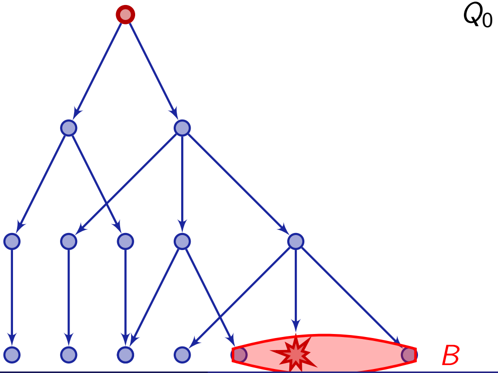
$$Post_A(Y) := \{q^+ \in Q : q \xrightarrow{a} q^+ \text{ for some } q \in Y, a \in A\}$$



Labeled Transition Systems

Definition (Image Computation)

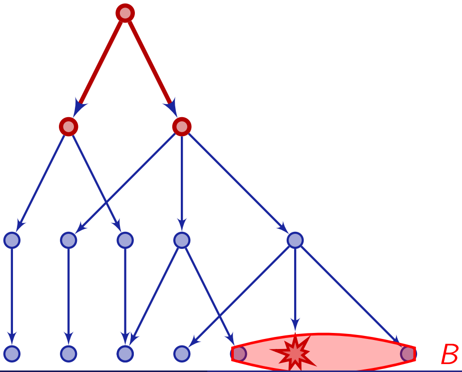
$$Post_A(Y) := \{q^+ \in Q : q \xrightarrow{a} q^+ \text{ for some } q \in Y, a \in A\}$$



Labeled Transition Systems

Definition (Image Computation)

$$Post_A(Y) := \{q^+ \in Q : q \xrightarrow{a} q^+ \text{ for some } q \in Y, a \in A\}$$



Q_0

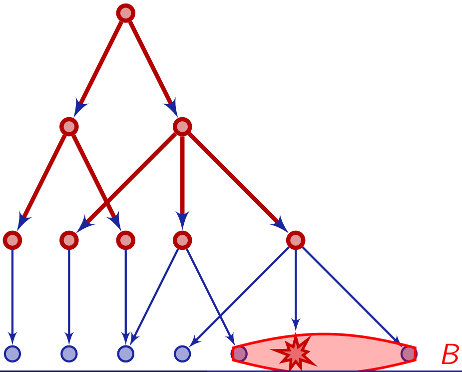
$Post_A(Q_0)$

$Q_1 = Post_A(Q_0)$

Labeled Transition Systems

Definition (Image Computation)

$$Post_A(Y) \;:=\; \{q^+ \in Q \;:\; q \xrightarrow{a} q^+ \text{ for some } q \in Y, a \in A\}$$



Q_0

$Post_A(Q_0)$

$Q_1 = Post_A(Q_0)$

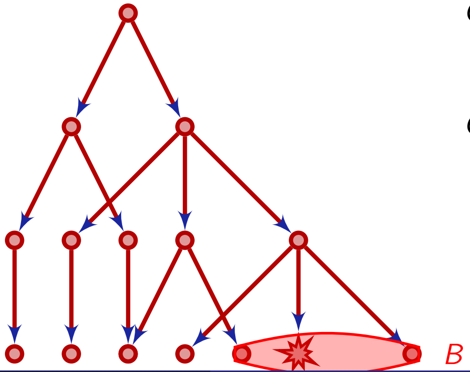
$Post_A(Q_1)$

$Q_2 = Post_A^2(Q_0)$

Labeled Transition Systems

Definition (Image Computation)

$$Post_A(Y) := \{q^+ \in Q : q \xrightarrow{a} q^+ \text{ for some } q \in Y, a \in A\}$$



$$Q_0$$

$$Post_A(Q_0)$$

$$Q_1 = Post_A(Q_0)$$

$$Post_A(Q_1)$$

$$Q_2 = Post_A^2(Q_0)$$

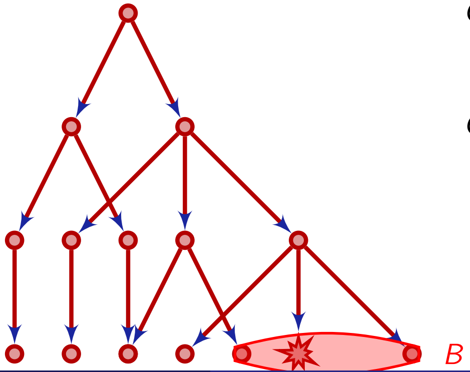
$$Post_A(Q_2)$$

$$Q_3 = Post_A^3(Q_0)$$

Labeled Transition Systems

Definition (Image Computation)

$$Post_A(Y) := \{q^+ \in Q \ : \ q \xrightarrow{a} q^+ \text{ for some } q \in Y, a \in A\}$$
$$Post^*_A(Y) := \mu Z.(Y \cup Z \cup Post_A(Z))$$



Q_0

$\quad \downarrow Post_A(Q_0)$

$Q_1 = Post_A(Q_0)$

$\quad \downarrow Post_A(Q_1)$

$Q_2 = Post^2_A(Q_0)$

$\quad \downarrow Post_A(Q_2)$

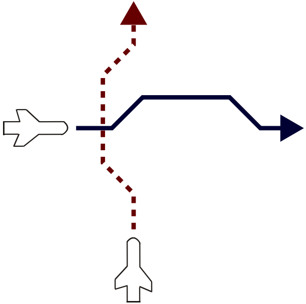
$Q_3 = Post^3_A(Q_0)$

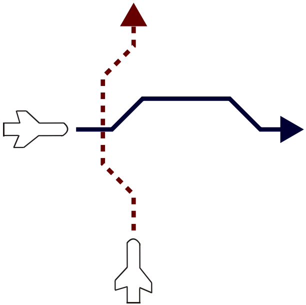
Finite Automata

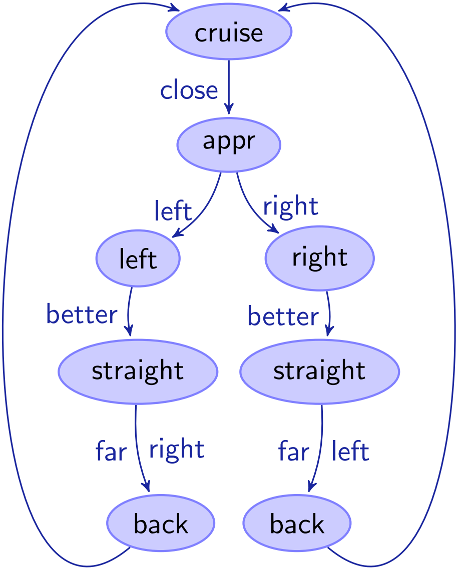
Definition (Nondeterministic Finite Automata)

- Transition relation on $Q \times A \times Q$, denoted as $q \xrightarrow{a} q^+$, along with
- finite set A of transition actions,
- finite set Q of states, initial states $Q_0 \subseteq Q$.

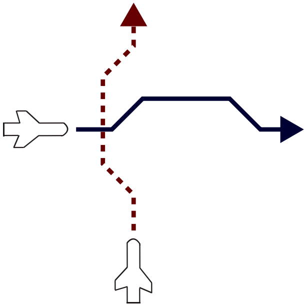
Finite Automaton for Collision Avoidance



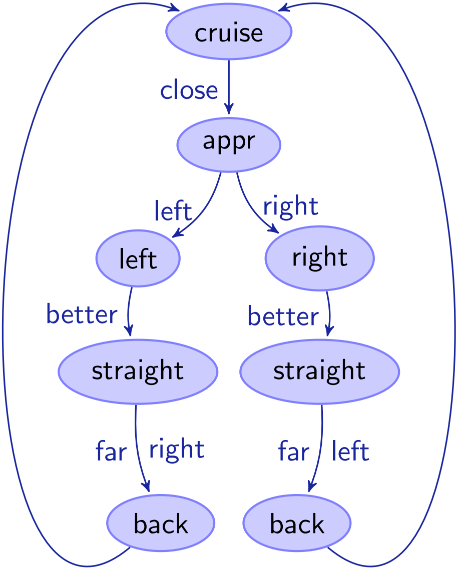



cruise
close
appr
left
right
left
right
better
better
straight
straight
far
right
far
left
back
back

Finite Automaton for Collision Avoidance



good model?



Collision avoidance is a property of controlled movement!

Hybrid Automata

Definition (Hybrid Automata)

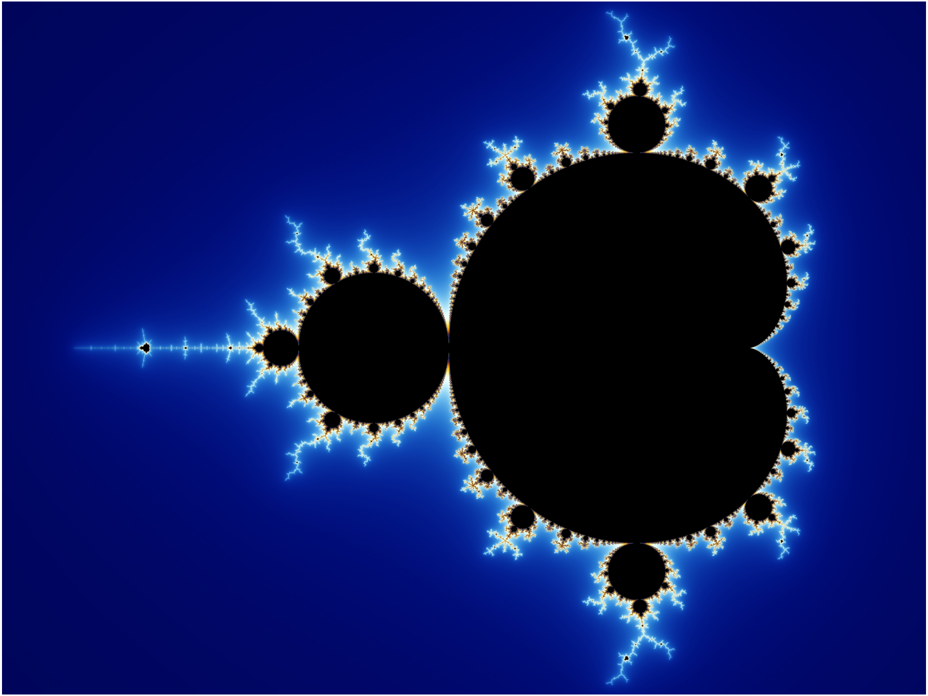
- Finite directed graph: vertices M (*modes*), edges E (*control switches*)
- continuous state space $\mathbb{R}^n$
- *flows* φ_v, where $\varphi_v(t; x) \in \mathbb{R}^n$ is the state reached after staying in mode v for time $t \geq 0$ when continuous evolution starts in state $x \in \mathbb{R}^n$
- invariant conditions $inv_v \subseteq \mathbb{R}^n$ for $v \in M$
- jump relations $jump_e \subseteq \mathbb{R}^n \times \mathbb{R}^n$ for edges $e \in E$
  usually comprising guard on current state and reset relations

Hybrid Automata

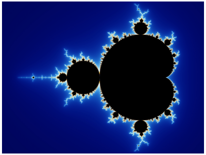
Definition (Hybrid Automata)

- Finite directed graph: vertices M (*modes*), edges E (*control switches*)
- continuous state space $\mathbb{R}^n$
- *flows* φ_v, where $\varphi_v(t;x) \in \mathbb{R}^n$ is the state reached after staying in mode v for time $t \geq 0$ when continuous evolution starts in state $x \in \mathbb{R}^n$
- invariant conditions $inv_v \subseteq \mathbb{R}^n$ for $v \in M$
- jump relations $jump_e \subseteq \mathbb{R}^n \times \mathbb{R}^n$ for edges $e \in E$
  usually comprising guard on current state and reset relations

Is this a good definition?



Mandelbrot Fractal

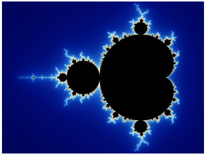


Example (Mandelbrot Set)

For complex numbers $c \in \mathbb{C}$ define $f_0(c) = c$ and $f_{n+1}(c) = f_n(c)^2 + c$. Then the Mandelbrot set is

$$\{c \in \mathbb{C} \; : \; f_n(c) \not\to \infty \text{ as } n \to \infty\}$$

Mandelbrot Fractal



Example (Mandelbrot Set)

For complex numbers $c \in \mathbb{C}$ define $f_0(c) = c$ and $f_{n+1}(c) = f_n(c)^2 + c$. Then the Mandelbrot set is

$$\{c \in \mathbb{C} \ : \ f_n(c) \not\to \infty \text{ as } n \to \infty\}$$

Theorem (Lenore Blum, Cucker, Shub, Smale'90...98)

"The Mandelbrot set is undecidable over $\mathbb{R}$ / in Real Turing Machines"

Hybrid Automata

Definition (Hybrid Automata)

- Finite directed graph: vertices M (*modes*), edges E (*control switches*)
- continuous state space $\mathbb{R}^n$
- *flows* φ_v, where $\varphi_v(t;x) \in \mathbb{R}^n$ is the state reached after staying in mode v for time $t \geq 0$ when continuous evolution starts in state $x \in \mathbb{R}^n$
- invariant conditions $inv_v \subseteq \mathbb{R}^n$ for $v \in M$
- jump relations $jump_e \subseteq \mathbb{R}^n \times \mathbb{R}^n$ for edges $e \in E$
  usually comprising guard on current state and reset relations

Is this a good definition?

Hybrid Automata

Definition (Hybrid Automata)

- Finite directed graph: vertices M (*modes*), edges E (*control switches*)
- continuous state space $\mathbb{R}^n$
- *flows* φ_v, where $\varphi_v(t;x) \in \mathbb{R}^n$ is the state reached after staying in mode v for time $t \geq 0$ when continuous evolution starts in state $x \in \mathbb{R}^n$
- invariant conditions $inv_v \subseteq \mathbb{R}^n$ for $v \in M$
- jump relations $jump_e \subseteq \mathbb{R}^n \times \mathbb{R}^n$ for edges $e \in E$ usually comprising guard on current state and reset relations

What if inv_v is a Mandelbrot set?

Hybrid Automata

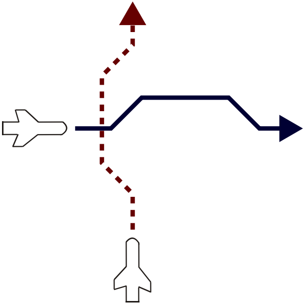
Definition (Hybrid Automata)

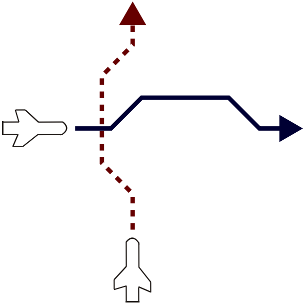
- Finite directed graph: vertices M (*modes*), edges E (*control switches*)
- continuous state space $\mathbb{R}^n$
- *flows* φ_v, where $\varphi_v(t; x) \in \mathbb{R}^n$ is the state reached after staying in mode v for time $t \geq 0$ when continuous evolution starts in state $x \in \mathbb{R}^n$
- invariant conditions $inv_v \subseteq \mathbb{R}^n$ for $v \in M$
- jump relations $jump_e \subseteq \mathbb{R}^n \times \mathbb{R}^n$ for edges $e \in E$ usually comprising guard on current state and reset relations

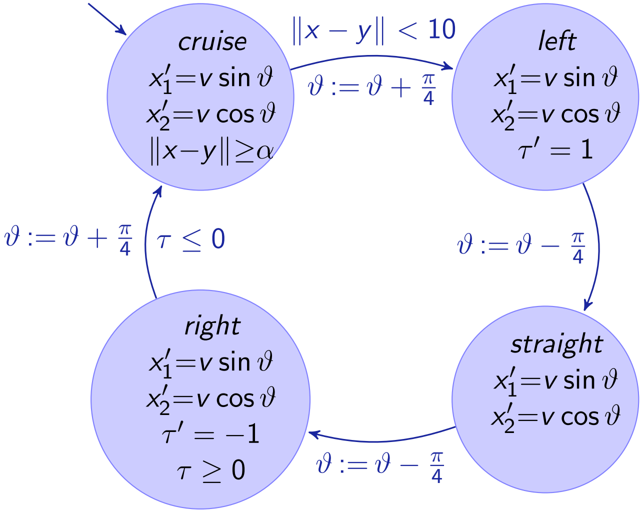
All relations decidable / definable in first-order real arithmetic . . .

Computationally relevant output
needs computational input!

Hybrid Automaton for Collision Avoidance

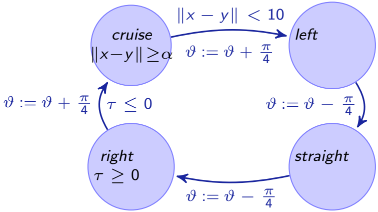





cruise
$x_1' = v \sin\vartheta$
$x_2' = v \cos\vartheta$
$\|x-y\| \geq \alpha$
$\|x - y\| < 10$
$\vartheta := \vartheta + \frac{\pi}{4}$
left
$x_1' = v \sin\vartheta$
$x_2' = v \cos\vartheta$
$\tau' = 1$
$\vartheta := \vartheta - \frac{\pi}{4}$
straight
$x_1' = v \sin\vartheta$
$x_2' = v \cos\vartheta$
$\vartheta := \vartheta - \frac{\pi}{4}$
right
$x_1' = v \sin\vartheta$
$x_2' = v \cos\vartheta$
$\tau' = -1$
$\tau \geq 0$
$\vartheta := \vartheta + \frac{\pi}{4}$
$\tau \leq 0$

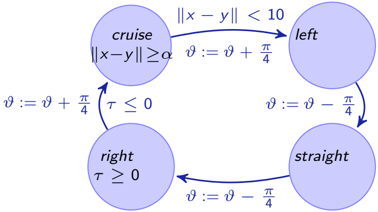
Hybrid Automaton for Collision Avoidance: Formal

$$\varphi_v(t;x,y,\tau) = \begin{pmatrix} x_1 + tv\sin\vartheta \\ x_2 + tv\cos\vartheta \\ y_1 + tu\sin\varsigma \\ y_2 + tu\cos\varsigma \\ \tau + t \end{pmatrix}$$



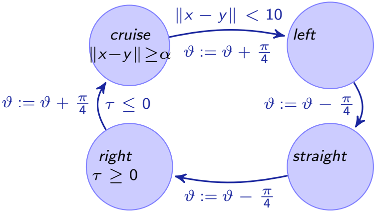
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$



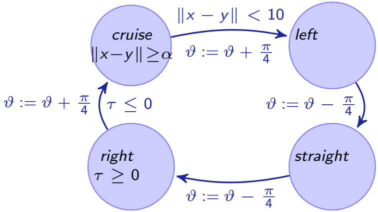
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$



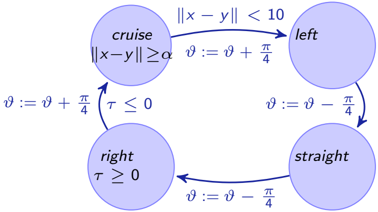
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$



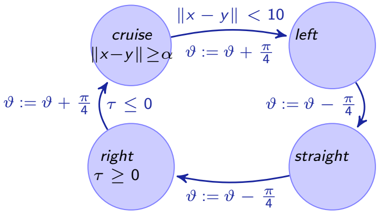
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \wedge reset_e(x, x^+)$



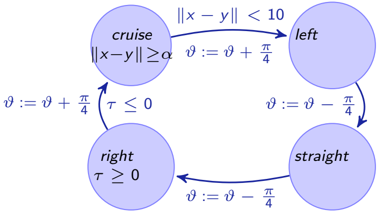
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \wedge reset_e(x, x^+)$
- $guard_{cruise,left} \equiv \|x - y\| < 10$



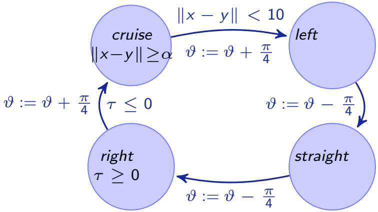
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \land reset_e(x, x^+)$
- $guard_{cruise,left} \equiv \|x - y\| < 10$
- $reset_{cruise,left} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$



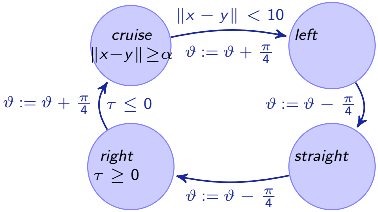
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \wedge reset_e(x, x^+)$
- $guard_{cruise,left} \equiv \|x - y\| < 10$
- $reset_{cruise,left} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$
- $reset_{left,straight} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$



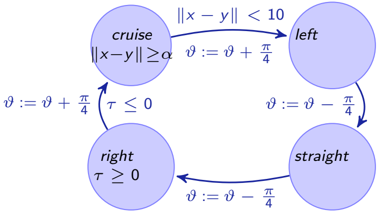
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \wedge reset_e(x, x^+)$
- $guard_{cruise,left} \equiv \|x - y\| < 10$
- $reset_{cruise,left} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$
- $reset_{left,straight} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $reset_{straight,right} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$



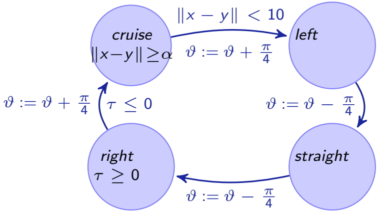
Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \wedge reset_e(x, x^+)$
- $guard_{cruise,left} \equiv \|x - y\| < 10$
- $reset_{cruise,left} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$
- $reset_{left,straight} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $reset_{straight,right} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $guard_{right,cruise} \equiv \tau \leq 0$

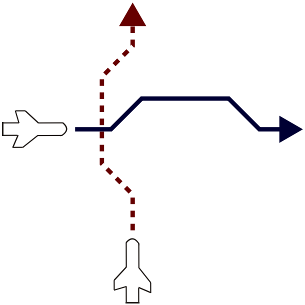


Hybrid Automaton for Collision Avoidance: Formal

- $inv_{cruise} \equiv \|x - y\| \geq \alpha$
- $inv_{right} \equiv \tau \geq 0$
- $inv_{left} \equiv inv_{straight} \equiv true$
- $jump_e(x, x^+) \equiv guard_e(x) \wedge reset_e(x, x^+)$
- $guard_{cruise,left} \equiv \|x - y\| < 10$
- $reset_{cruise,left} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$
- $reset_{left,straight} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $reset_{straight,right} \equiv \vartheta^+ = \vartheta - \frac{\pi}{4}$
- $guard_{right,cruise} \equiv \tau \leq 0$
- $reset_{right,cruise} \equiv \vartheta^+ = \vartheta + \frac{\pi}{4}$



Hybrid Automaton for Collision Avoidance



Example (Property)

If the aircraft are far apart and have compatible speed, then—when following the protocol—they will never crash?

Example (Property)

If the aircraft enter collision avoidance, then—when following the protocol—will they ever leave again, i.e. follow their old route?

Hybrid Systems

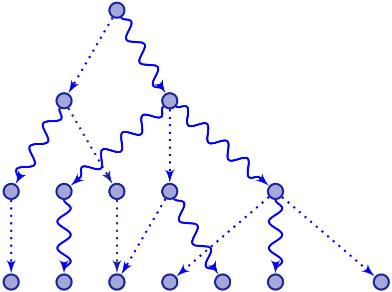
Definition (Hybrid Automata $\rightarrow$ Hybrid System)

- $Q := (M \times \mathbb{R}^n) \cap \{(v, x) \; : \; x \in inv_v\}$
- Discrete transition $(v, x) \xrightarrow{a} (v^+, x^+)$ iff there is an edge e from v to v^+ with input a such that $(x, x^+) \in jump_e$
- Continuous transition $(v, x) \xrightarrow{r} (v, x^+)$ iff $x^+ = \varphi_v(r; x)$ for $r \geq 0$ and $\varphi_v(t; x) \in inv_v$ for all $0 \leq t \leq r$.

Hybrid Systems

Definition (Hybrid Automata → Hybrid System)

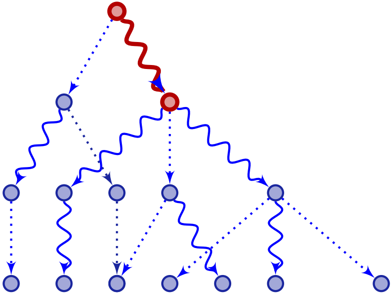
- $Q := (M \times \mathbb{R}^n) \cap \{(v,x) \ : \ x \in inv_v\}$
- Discrete transition $(v,x) \xrightarrow{a} (v^+,x^+)$ iff there is an edge e from v to v^+ with input a such that $(x,x^+) \in jump_e$
- Continuous transition $(v,x) \xrightarrow{r} (v,x^+)$ iff $x^+ = \varphi_v(r;x)$ for $r \geq 0$ and $\varphi_v(t;x) \in inv_v$ for all $0 \leq t \leq r$.



Hybrid Systems

Definition (Hybrid Automata → Hybrid System)

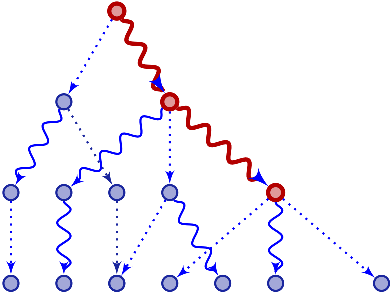
- $Q := (M \times \mathbb{R}^n) \cap \{(v, x) \ : \ x \in inv_v\}$
- Discrete transition $(v, x) \xrightarrow{a} (v^+, x^+)$ iff there is an edge e from v to v^+ with input a such that $(x, x^+) \in jump_e$
- Continuous transition $(v, x) \xrightarrow{r} (v, x^+)$ iff $x^+ = \varphi_v(r; x)$ for $r \geq 0$ and $\varphi_v(t; x) \in inv_v$ for all $0 \leq t \leq r$.



Hybrid Systems

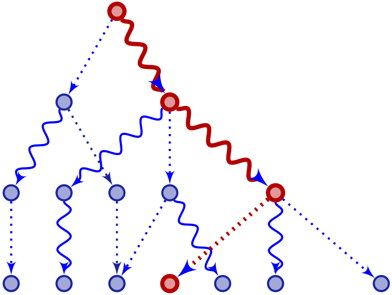
Definition (Hybrid Automata $\to$ Hybrid System)

- $Q := (M \times \mathbb{R}^n) \cap \{(v,x) \ : \ x \in inv_v\}$
- Discrete transition $(v,x) \xrightarrow{a} (v^+,x^+)$ iff there is an edge e from v to v^+ with input a such that $(x,x^+) \in jump_e$
- Continuous transition $(v,x) \xrightarrow{r} (v,x^+)$ iff $x^+ = \varphi_v(r;x)$ for $r \geq 0$ and $\varphi_v(t;x) \in inv_v$ for all $0 \leq t \leq r$.



Definition (Hybrid Automata → Hybrid System)

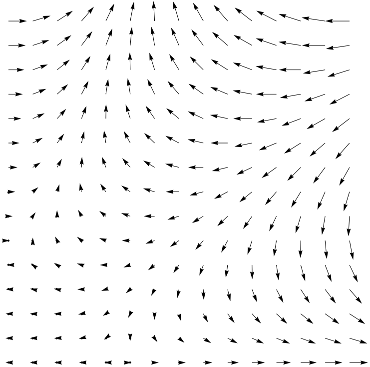
- $Q := (M \times \mathbb{R}^n) \cap \{(v, x) \ : \ x \in inv_v\}$
- Discrete transition $(v, x) \xrightarrow{a} (v^+, x^+)$ iff there is an edge e from v to v^+ with input a such that $(x, x^+) \in jump_e$
- Continuous transition $(v, x) \xrightarrow{r} (v, x^+)$ iff $x^+ = \varphi_v(r; x)$ for $r \geq 0$ and $\varphi_v(t; x) \in inv_v$ for all $0 \leq t \leq r$.



Outline

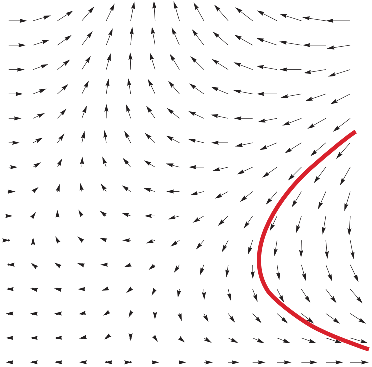
How to describe continuous change?

Relate continuously changing quantity and its rate of change (derivative)



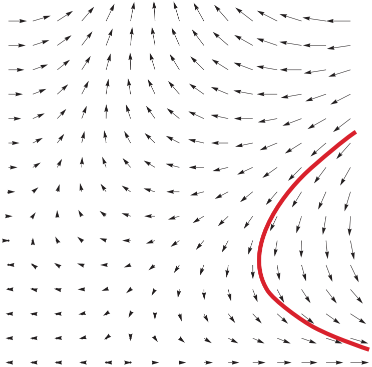
How to describe continuous change?

Relate continuously changing quantity and its rate of change (derivative)



How to describe continuous change?

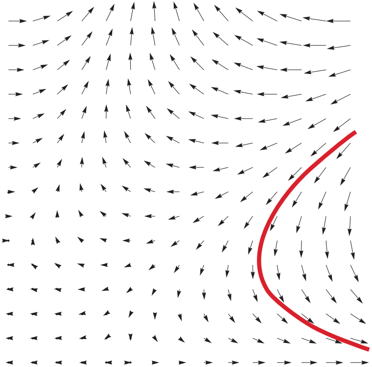
Relate continuously changing quantity and its rate of change (derivative)



$$\left[\begin{array}{rl} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{array}\right]$$

How to describe continuous change?

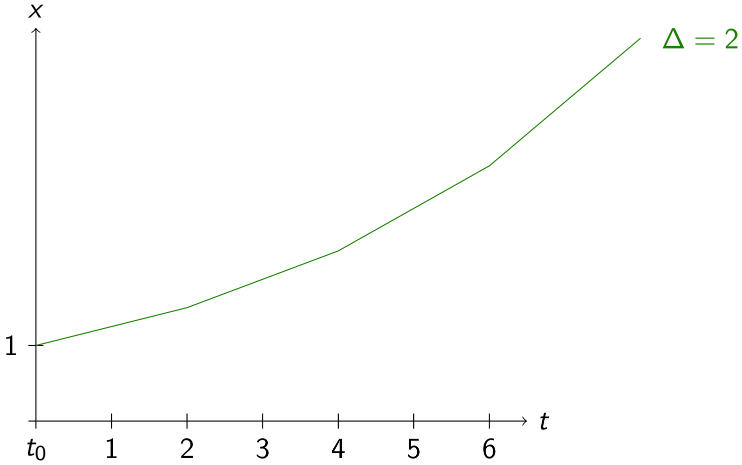
Relate continuously changing quantity and its rate of change (derivative)



$$\begin{bmatrix} y'(t) = & f(t,y) \\ y(t_0) = & y_0 \end{bmatrix}$$

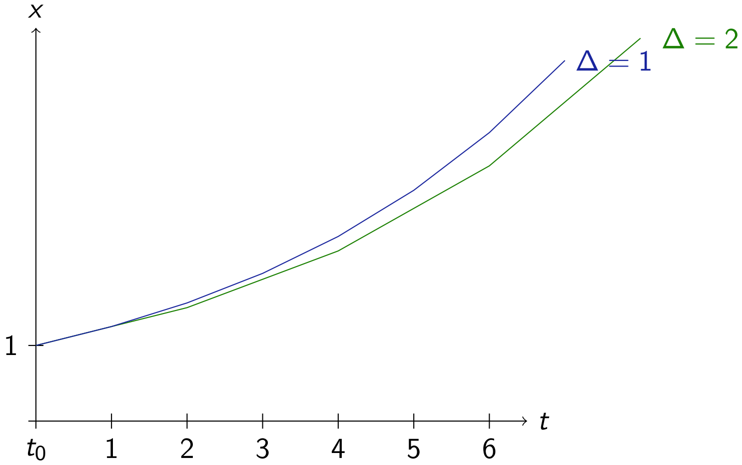
in which direction y evolves as time t progresses
where y starts at time t_0

Intuition of Differential Equations



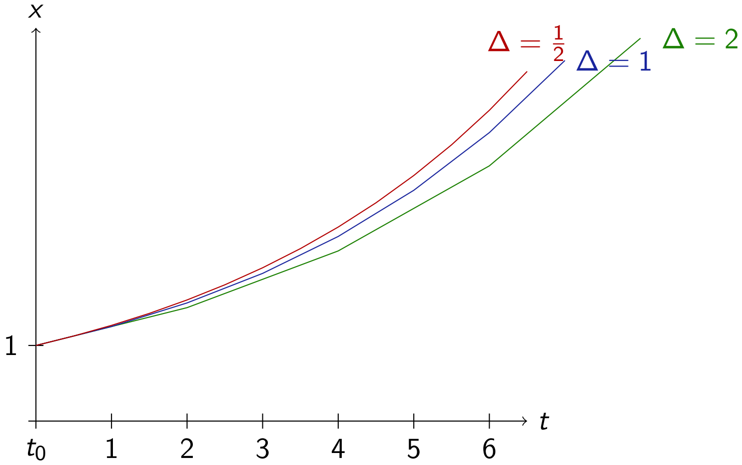
$$\begin{bmatrix} x'(t) = & \frac{1}{4}x \\ x(t_0) = & 1 \end{bmatrix}$$

Intuition of Differential Equations



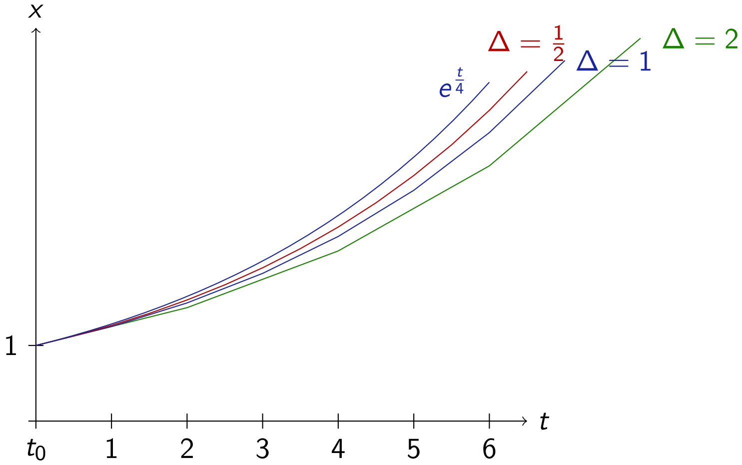
$$\left[\begin{array}{rl} x'(t) = & \frac{1}{4}x \\ x(t_0) = & 1 \end{array}\right]$$

Intuition of Differential Equations



$$\begin{bmatrix} x'(t) = & \frac{1}{4}x \\ x(t_0) = & 1 \end{bmatrix}$$

Intuition of Differential Equations



$$\left[\begin{array}{rl} x'(t) = & \frac{1}{4}x \\ x(t_0) = & 1 \end{array}\right]$$

Differential Equations & Initial-Value Problems

Definition (Ordinary Differential Equation, ODE)

$f : D \to \mathbb{R}^n$ on domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$. Then $Y : I \to \mathbb{R}^n$ is *solution* of IVP

$$\left[\begin{array}{ll} y'(t) = & f(t, y) \\ y(t_0) = & y_0 \end{array}\right]$$

on interval $I \subseteq \mathbb{R}$, iff, for all $t \in I$,

1. $(t, Y(t)) \in D$
2. $Y'(t)$ exists and $Y'(t) = f(t, Y(t))$.
3. $Y(t_0) = y_0$

Accordingly for higher-order differential equations, i.e., differential equations involving higher-order derivatives $y^{(n)}(t)$.

If $f \in C(D, \mathbb{R}^n)$, then $Y \in C^1(I, \mathbb{R}^n)$.

ODE Examples

What is a solution of the following IVP?

$$\begin{bmatrix} y'(x) = & -2xy \\ y(0) = & 1 \end{bmatrix}$$

ODE Examples

What is a solution of the following IVP?

$$\begin{bmatrix} y'(x) = & -2xy \\ y(0) = & 1 \end{bmatrix}$$

Solution:

$$y(x) = e^{-x^2}$$

ODE Examples

What is a solution of the following IVP?

$$\begin{bmatrix} y'(x) = & -2xy \\ y(0) = & 1 \end{bmatrix}$$

Solution:

$$y(x) = e^{-x^2}$$

Proof.

$$y'(x) = \frac{\mathrm{d}e^{-x^2}}{\mathrm{d}x} = e^{-x^2}(-2x) = -2xy(x)$$

$$y(0) = e^{-0^2} = 1$$

□

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - t x_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \dots$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - t x_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \ldots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx$	$x(t) = x_0 e^{\frac{t^2}{2}}$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1+2t} \ldots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = x_0$	$x(t) = \tan t \dots$

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1-tx_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1+2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = x_0$	$x(t) = \tan t \dots$
$x'(t) = \frac{2}{t^3} x(t)$	$x(t) = e^{-\frac{1}{t^2}}$ non-analytic

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - t x_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \dots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = x_0$	$x(t) = \tan t \dots$
$x'(t) = \frac{2}{t^3} x(t)$	$x(t) = e^{-\frac{1}{t^2}}$ non-analytic
$x' = x^2 + x^4$	???

ODE Examples

ODE	Solution
$x' = 1, x(0) = x_0$	$x(t) = x_0 + t$
$x' = 5, x(0) = x_0$	$x(t) = x_0 + 5t$
$x' = x, x(0) = x_0$	$x(t) = x_0 e^t$
$x' = x^2, x(0) = x_0$	$x(t) = \frac{x_0}{1 - t x_0}$
$x' = \frac{1}{x}, x(0) = 1$	$x(t) = \sqrt{1 + 2t} \ldots$
$y'(x) = -2xy, y(0) = 1$	$y(x) = e^{-x^2}$
$x'(t) = tx$	$x(t) = x_0 e^{\frac{t^2}{2}}$
$x' = \sqrt{x}, x(0) = x_0$	$x(t) = \frac{t^2}{4} \pm t\sqrt{x_0} + x_0$
$x' = y, y' = -x, x(0) = 0, y(0) = 1$	$x(t) = \sin t, y(t) = \cos t$
$x' = 1 + x^2, x(0) = x_0$	$x(t) = \tan t \ldots$
$x'(t) = \frac{2}{t^3} x(t)$	$x(t) = e^{-\frac{1}{t^2}}$ non-analytic
$x' = x^2 + x^4$	???
$x'(t) = e^{t^2}$	non-elementary

▸ ATC ▸ HA

Existence

Theorem (Existence theorem of Peano'1890)

$f \in C(D, \mathbb{R}^n)$ on open, connected domain $D \subseteq \mathbb{R} \times \mathbb{R}^n$ with $(x_0, y_0) \in D$. Then, IVP has a solution. Further, every solution can be continued arbitrarily close to the border of D.

Example (Solvable)

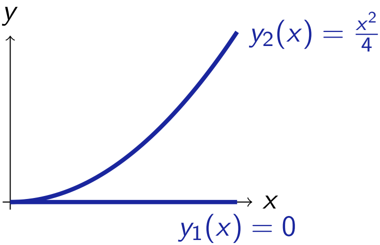
$$\left[\begin{array}{rl} y' = & \sqrt{|y|} \\ y(0) = & 0 \end{array}\right]$$

$$\left[\begin{array}{rl} y'(x) = & 3x^2 y - \frac{1}{y} \sin x \cos y \\ y(0) = & 1 \end{array}\right]$$

Existence
Peano

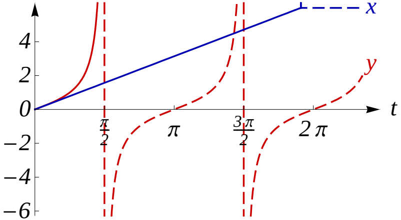
Example (Solvable but not uniquely)

$$\begin{bmatrix} y' = & \sqrt{|y|} \\ y(0) = & 0 \end{bmatrix}$$



Example (Continuable but limited)

$$\left[\begin{array}{rl} y' = & 1 + y^2 \\ y(0) = & 0 \end{array}\right]$$



Lipschitz-Continuity

Definition (Lipschitz-continuous)

$f : D \to \mathbb{R}^n$ with $D \subseteq \mathbb{R} \times \mathbb{R}^n$ is *Lipschitz-continuous* for y iff there is an $L \in \mathbb{R}$ such that for all $(x, y), (x, \bar{y}) \in D$:

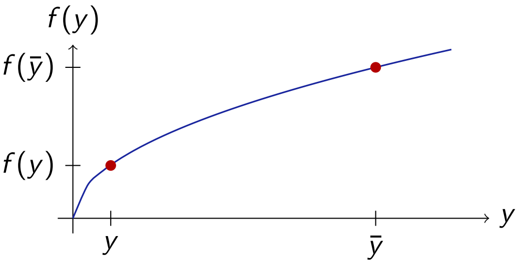
$$\|f(x, y) - f(x, \bar{y})\| \leq L\|y - \bar{y}\|$$

Lipschitz-Continuity

Definition (Lipschitz-continuous)

$f : D \to \mathbb{R}^n$ with $D \subseteq \mathbb{R} \times \mathbb{R}^n$ is *Lipschitz-continuous* for y iff there is an $L \in \mathbb{R}$ such that for all $(x, y), (x, \bar{y}) \in D$:

$$\|f(x, y) - f(x, \bar{y})\| \le L\|y - \bar{y}\|$$

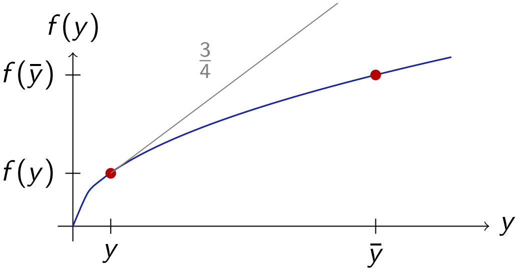


Lipschitz-Continuity

Definition (Lipschitz-continuous)

$f : D \to \mathbb{R}^n$ with $D \subseteq \mathbb{R} \times \mathbb{R}^n$ is *Lipschitz-continuous* for y iff there is an $L \in \mathbb{R}$ such that for all $(x, y), (x, \bar{y}) \in D$:

$$\|f(x, y) - f(x, \bar{y})\| \leq L\|y - \bar{y}\|$$

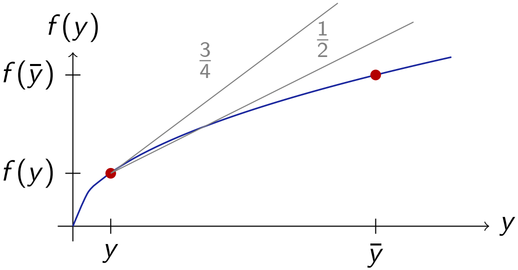


Lipschitz-Continuity

Definition (Lipschitz-continuous)

$f : D \to \mathbb{R}^n$ with $D \subseteq \mathbb{R} \times \mathbb{R}^n$ is *Lipschitz-continuous* for y iff there is an $L \in \mathbb{R}$ such that for all $(x, y), (x, \bar{y}) \in D$:

$$\|f(x, y) - f(x, \bar{y})\| \leq L\|y - \bar{y}\|$$

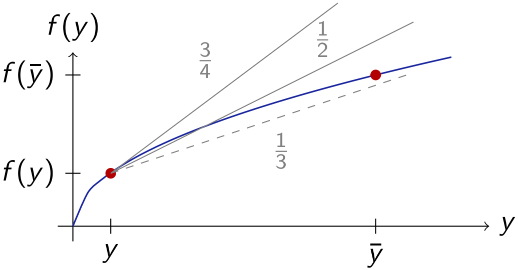


Lipschitz-Continuity

Definition (Lipschitz-continuous)

$f : D \to \mathbb{R}^n$ with $D \subseteq \mathbb{R} \times \mathbb{R}^n$ is *Lipschitz-continuous* for y iff there is an $L \in \mathbb{R}$ such that for all $(x,y),(x,\bar{y}) \in D$:

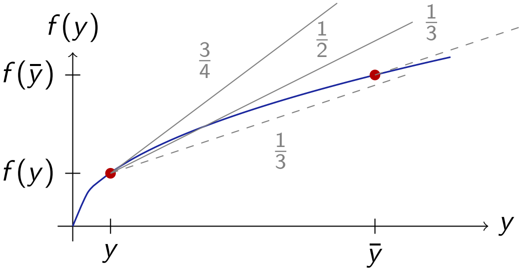
$$\|f(x,y) - f(x,\bar{y})\| \leq L\|y - \bar{y}\|$$



Definition (Lipschitz-continuous)

$f : D \to \mathbb{R}^n$ with $D \subseteq \mathbb{R} \times \mathbb{R}^n$ is *Lipschitz-continuous* for y iff there is an $L \in \mathbb{R}$ such that for all $(x, y), (x, \bar{y}) \in D$:

$$\|f(x, y) - f(x, \bar{y})\| \leq L\|y - \bar{y}\|$$



Lipschitz-Continuity

Definition (Lipschitz-continuous)

$f : D \to \mathbb{R}^n$ with $D \subseteq \mathbb{R} \times \mathbb{R}^n$ is *Lipschitz-continuous* for y iff there is an $L \in \mathbb{R}$ such that for all $(x, y), (x, \bar{y}) \in D$:

$$\|f(x,y) - f(x,\bar{y})\| \leq L\|y - \bar{y}\|$$

If $\frac{\partial f(x,y)}{\partial y}$ exists and is bounded on D then f is Lipschitz-continuous. f is *locally Lipschitz-continuous* iff for each $(x, y) \in D$, there is a neighbourhood in which f is Lipschitz-continuous.

Theorem (Uniqueness theorem of Picard-Lindelöf'1894)

In addition to Peano premisses, let f be locally Lipschitz-continuous for y (e.g. $f \in C^1(D, \mathbb{R}^n)$). Then, there is a unique solution of IVP.

Theorem (Uniqueness theorem of Picard-Lindelöf'1894)

In addition to Peano premisses, let f be locally Lipschitz-continuous for y (e.g. $f \in C^1(D, \mathbb{R}^n)$). Then, there is a unique solution of IVP.

Proposition (Global uniqueness theorem of Picard-Lindelöf)

$f \in C([0, a] \times \mathbb{R}^n, \mathbb{R}^n)$ Lipschitz-continuous for y. Then, there is a unique solution of IVP on $[0, a]$.

M. S. Branicky, V. S. Borkar, and S. K. Mitter.
A unified framework for hybrid control: Model and optimal control theory.
IEEE T. Automat. Contr., 43(1):31–45, 1998.

P. Hartman.
Ordinary Differential Equations.
John Wiley, 1964.

T. A. Henzinger.
The theory of hybrid automata.
In *LICS*, pages 278–292, Los Alamitos, 1996. IEEE Computer Society.

T. Krilavičius.
Bestiarium of hybrid systems.

W. T. Reid.
Ordinary Differential Equations.
John Wiley, 1971.

W. Walter.
Ordinary Differential Equations.