Discrete abstractions of hybrid systems for verification

George J. Pappas
Departments of ESE and CIS
University of Pennsylvania
pappasg@ee.upenn.edu
http://www.seas.upenn.edu/~pappasg

DISC Summer School on
Modeling and Control of Hybrid Systems
Veldhoven, The Netherlands
June 23-26, 2003
http://lcewww.et.tudelft.nl/~disc_hs/

Outline of this mini-course

Lecture 1 : Monday, June 23
Examples of hybrid systems, modeling formalisms

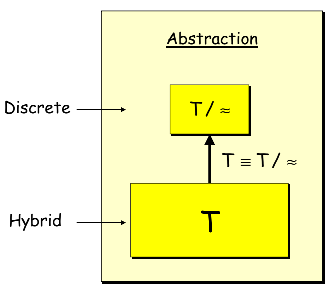
Lecture 2 : Monday, June 23
Transitions systems, temporal logic, refinement notions

Lecture 3 : Tuesday, June 24
Discrete abstractions of hybrid systems for verification

Lecture 4 : Tuesday, June 24
Discrete abstractions of continuous systems for control

Lecture 5 : Thursday, June 26
Bisimilar control systems

Hybrid to discrete (Lecture 3)



Goal : Finite quotients of hybrid systems

Hybrid System Model

A hybrid system $H = (V, \Re^n, X_0, F, Inv, R)$ consists of

- V is a finite set of states
- $\Re^n$ is the continuous state space
- $X = V \times \Re^n$ is the state space of the hybrid system
- $X_0 \subseteq X$ is the set of initial states
- $F(l, x) \subseteq \Re^n$ maps a diff. inclusion to each discrete state
- $Inv(l) \subseteq \Re^n$ maps invariant sets to each discrete state
- $R \subseteq X \times X$ is a relation capturing discontinuous changes

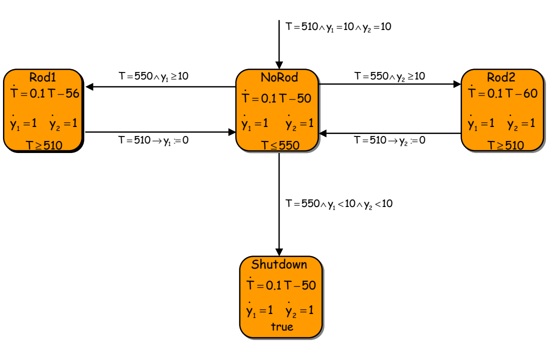
Define $E = \{(l, l') | \ \exists x \in Inv(l), x' \in Inv(l') \ ((l, x), (l', x')) \in R\}$

$$Init(l) = \{x \in Inv(l) \mid (l, x) \in X_0\}$$

$$Guard(e) = \{x \in Inv(l) | \ \exists x' \in Inv(l') \ ((l, x), (l', x')) \in R\}$$

$$Reset(e, x) = \{x' \in Inv(l') | \ ((l, x), (l', x')) \in R\}$$

An example



Transitions of Hybrid Systems

Hybrid systems can be embedded into transition systems

$$H = (V, \Re^n, X_0, F, Inv, R) \longrightarrow T_H = (Q, Q_0, \Sigma, \rightarrow, O, <\cdot>)$$

$Q = V \times \Re^n$
$Q_0 = X_0$
$\Sigma = E \cup \{\tau\}$
$\rightarrow \subseteq Q \times \Sigma \times Q$

Observation set and map depend on desired properties

Discrete transitions

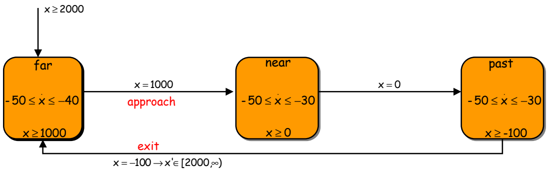
$$(l_1, x_1) \xrightarrow{e} (l_2, x_2) \quad \text{iff} \quad x_1 \in Guard(e), x_2 \in Reset(e, x_1)$$

Continuous (time-abstract) transitions

$$(l_1, x_1) \xrightarrow{\tau} (l_2, x_2) \quad \text{iff} \quad l_1 = l_2 \quad \text{and} \quad \exists \delta \geq 0 \quad x(\cdot) : [0, \delta] \rightarrow \Re^n$$
$$x(0) = x_1, x(\delta) = x_2, \quad \text{and} \quad \forall t \in [0, \delta]$$
$$\dot{x} \in F(l_1, x(t)) \quad \text{and} \quad x(t) \in Inv(l_1)$$

Rectangular hybrid automata

Rectangular sets : $\bigwedge_i x_i \sim c_i \quad \sim \in \{<, \leq, =, \geq, >\}, c_i \in Q$

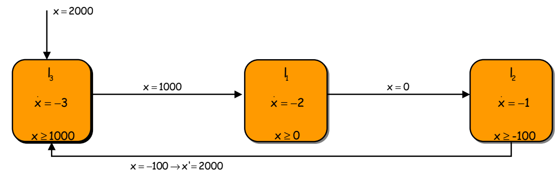


Rectangular hybrid automata are hybrid systems where

$$Init(l), Inv(l), F(l,x), Guard(e), Reset(e,x)_i$$

are rectangular sets

Multi-rate automata

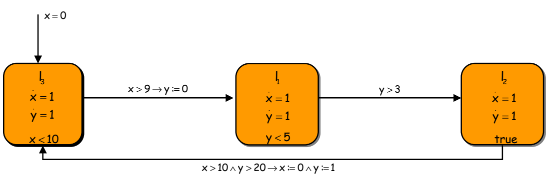


Multi-rate automata are rectangular hybrid automata where

$$Init(l), F(l,x), Reset(e,x)_i$$

are singleton sets

Timed automata



Timed automata are multi-rate automata where

$$F(l, x_i) = 1$$

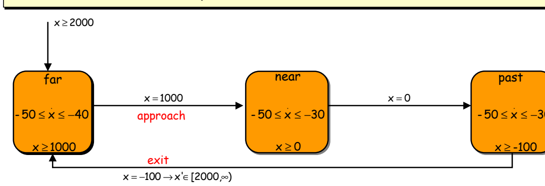
for all locations l and all variables.

Initialized automata

Rectangular hybrid automata are **initialized** if the following holds:

After a discrete transition, if the differential inclusion (equation) for a variable changes, then the variable must be reset to a fixed interval.

Timed automata are always initialized.



Bad news

Undecidability barriers

Consider the class of uninitialized multi-rate automata with n-1 clock variables, and one two slope variable (with two different rates).

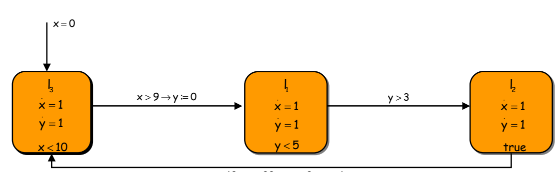
The reachability problem is undecidable for this class.

No algorithmic procedure exists.

Model checking temporal logic formulas is also undecidable

Initalization is necessary for decidability

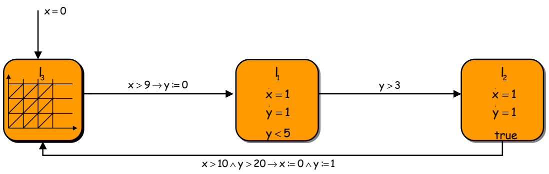
Timed automata



All timed automata admit a finite bisimulation

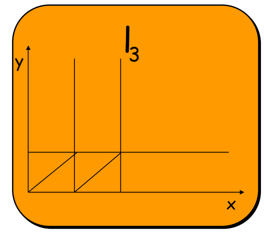
Hence CTL* model checking is decidable for timed automata

Timed automata



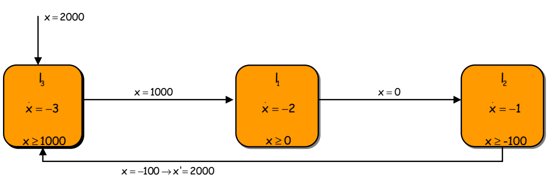
Approach : Discretize the clock dynamics using region equivalence

Region equivalence



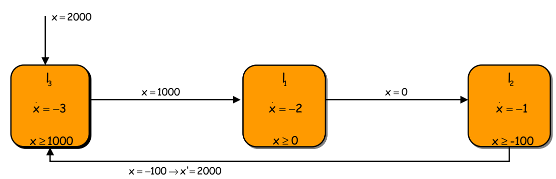
Equivalence classes : 6 corner points
14 open line segments
8 open regions

Multi-rate automata



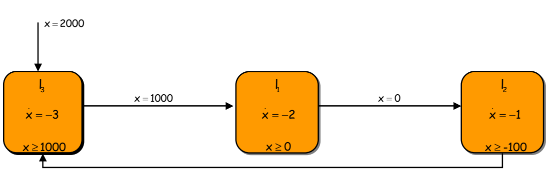
All initialized multi-rate automata admit a finite bisimulation

Rectangular automata



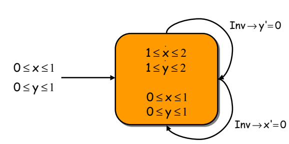
All initialized rectangular automata admit a finite bisimulation

Rectangular automata



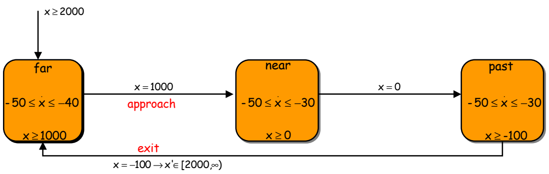
~~**All initialized rectangular automata admit a finite bisimulation**~~

No finite bisimulation



Bisimulation algorithm never terminates

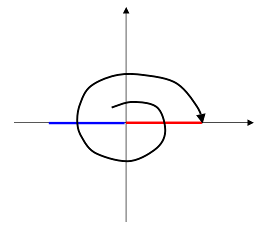
but…



All initialized rectangular automata admit a finite language equivalence quotient which can be constructed effectively.

LTL model checking of rectangular automata is decidable.

More complicated dynamics?



Bisimulation algorithm never terminates !!

Sets

$P_1 = \{(x,0) \mid 0 \le x \le 4\}$

$P_2 = \{(x,0) \mid -4 \le x < 0\}$

$P_3 = R^2 \setminus (P_1 \cup P_2)$

Dynamics

$\dot{x}_1 = 0.2x_1 + x_2$

$\dot{x}_2 = -x_1 + 0.2x_2$

Basic problems

Finite bisimulations of continuous dynamical systems

Given a vector field F(x) and a finite partition of R^n

1. Does there exist a finite bisimulation ?
2. Can we compute it ?

Reminder

Representation issues

- Symbolic representation for infinite sets
- Rectangular sets ? Semi-linear ? Semi-algebraic ?

Operations on sets

- Boolean (logical) operations
- Can we compute Pre and Post ?
- Is our representation closed under Pre and Post ?

Algorithmic termination (decidability)

- No guarantee for infinite transition systems
- We need "nice" alignment of sets and flows
- Globally finite properties

First-order logic

Every theory of the reals has an associated language

$$(\Re, <, +, -, 0, 1)$$

Universe   Relation   Functions   Constants

Variables : $x_1, x_2, x_3, \ldots$

TERMS : Variables, constants, or functions of them

$x_1 - x_2 + 1, 1 + 1, -x_3$

ATOMIC FORMULAS : Apply the relation and equality to the terms

$x_1 + x_2 < -1, 2x_1 = 1, x_1 = x_3$

(FIRST ORDER) FORMULAS : Atomic formulas are formulas

If φ_1, φ_2 are formulas, then $\varphi_1 \vee \varphi_2, \neg\varphi_1, \forall x.\varphi_1, \exists x.\varphi_1$

First-order logic

Useful languages

$(\Re, <, +, -, 0, 1)$ $\quad \forall x \forall y (x + 2y \ge 0)$

$(\Re, <, +, -, \times, 0, 1)$ $\quad \exists x. ax^2 + bx + c = 0$

$(\Re, <, +, -, \times, e^x, 0, 1)$ $\quad \exists t.(t \ge 0) \wedge (y = e^t x)$

A theory of the reals is **decidable** if there is an algorithm which in a finite number of steps will decide whether a formula is true or not

A theory of the reals admits **quantifier elimination** if there is an algorithm which will eliminate all quantified variables.

$$\exists x. ax^2 + bx + c = 0 \equiv b^2 - 4ac \ge 0$$

First-order logic

Theory	Decidable ?	Quant. Elim. ?
$(\Re, <, +, -, 0, 1)$	YES	YES
$(\Re, <, +, -, \times, 0, 1)$	YES	YES
$(\Re, <, +, -, \times, e^x, 0, 1)$	?	NO

Tarski's result : Every formula in $(\Re, <, +, -, \times, 0, 1)$ can be decided

1. Eliminate quantified variables
2. Quantifier free formulas can be decided

O-Minimal Theories

A definable set is $Y = \{(x_1, x_2, \ldots, x_n) \in \Re^n \mid \varphi(x_1, \ldots, x_n)\}$

A theory of the reals is called **o-minimal** if every definable subset of the reals is a finite union of points and intervals

Example: $Y = \{(x) \in \Re \mid p(x) \geq 0\}$ for polynomial p(x)

Recent o-minimal theories

$(\Re, <, +, -, 0, 1)$

$(\Re, <, +, -, \times, 0, 1)$

$(\Re, <, +, -, \times, e^x, 0, 1) \longrightarrow$ Related to Hilbert's 16th problem

$(\Re, <, +, -, \times, \hat{f}, 0, 1)$

$(\Re, <, +, -, \times, \hat{f}, e^x, 0, 1)$

Basic answers

Finite bisimulations of continuous dynamical systems

Consider a vector field X and a finite partition of R^n where

1. The flow of the vector field is definable in an o-minimal theory
2. The finite partition is definable in the same o-minimal theory

Then a finite bisimulation always exists.

Corollaries

$(\Re, <, +, -, 0, 1)$ Consider continuous systems where

- Finite partition is polyhedral (semi-linear)
- Vector fields have linear flows (timed, multi-rate)

Then a finite bisimulation exists.

$(\Re, <, +, -, \times, 0, 1)$ Consider continuous systems where

- Finite partition is semialgebraic
- Vector fields have polynomial flows

Then a finite bisimulation exists.

Corollaries

$(\Re, <, +, -, \times, e^x, 0, 1)$ Consider continuous systems where

- Finite partition is semi-algebraic
- Vector fields are linear with real eigenvalues

Then a finite bisimulation exists.

$(\Re, <, +, -, \times, \hat{f}, 0, 1)$ Consider continuous systems where

- Finite partition is sub-analytic
- Vector fields are linear with purely imaginary eigenvalues

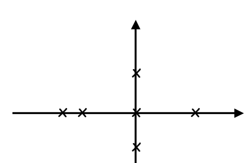
Then a finite bisimulation exists.

Corollaries

$(\Re, <, +, -, \times, \hat{f}, e^x, 0, 1)$ Consider continuous systems where

- Finite partition is semi-algebraic
- Vector fields are linear with real or imginary eigenvalues

Then a finite bisimulation exists.



Conditions are sufficient but tight

Computability

Finite bisimulations exist, but can we compute them ?

Bisimulation Algorithm

initialize $Q/_\sim = \{p \sim q \ \text{ iff } \ <q>=<p>\}$
while $\exists P, P' \in Q/_\sim$ **such that** $\emptyset \neq \subseteq P \cap Pre(P') \neq \subseteq P'$
$P_1 := P \cap Pre(P')$
$P_2 := P \setminus Pre(P')$
$Q/_\sim := (Q/_\sim \setminus \{P\}) \cup \{P_1, P_2\}$
end while

Need to : Check emptiness
Perform boolean operations
Compute Pre (or Post)

Use $(\Re,<,+,-,\times,0,1)$

Computing reachable sets

Consider a linear system

$$\frac{dx}{dt} = Ax \quad A \in Q^{n \times n}$$

Rational entries

and a semi-algebraic set Y. If

$$Y = \{y \in \Re^n \mid p(y)\}$$

Then

$$Pre(Y) = \{x \in \Re^n \mid \exists y \exists t. p(y) \wedge t \geq 0 \wedge x = e^{-tA}y\}$$

Problem?

Nilpotent Linear Systems

Nilpotent matrices: $\exists n \geq 0 \quad A^n = 0$

Then flow of linear system is polynomial

$$e^{-tA} = \sum_{k=0}^{n-1} (-1)^k \frac{t^k}{k!} A^k$$

Therefore Pre(Y) completely definable in $(\Re,<,+,-,\times,0,1)$

$$Pre(Y) = \{x \in \Re^n \mid \exists y \exists t. p(y) \wedge t \geq 0 \wedge x = \sum_{k=0}^{n-1} (-1)^k \frac{t^k}{k!} A^k y\}$$

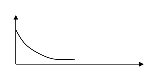
Diagonalizable, rational eigenvalues

Example system : $\dot{x} = 2x$

Compute all states that can reach the set Y = { y=5 }

$$Pre(Y) = \{x \in \Re \mid \exists y \exists t.\ y = 5 \wedge t \geq 0 \wedge x = e^{-2t}y\}$$

Let $s = e^{-t}$, then



$$Pre(Y) = \{x \in \Re \mid \exists y \exists t.\ y = 5 \wedge 1 \geq s \geq 0 \wedge x = s^2 y\}$$

$$Pre(Y) = \{x \in \Re \mid \ 0 < x \leq 5\}$$

Diagonalizable, rational eigenvalues

More generally $\dot{x} = Ax \Rightarrow x(t) = Te^{\Lambda t}T^{-1}x(0)$

Therefore $\quad e^{-tA} = \left[\sum_{k=1}^{n} a_{ijk} e^{-\lambda_k t}\right]_{ij}$

1. Rescale rational eigenvalues to integer eingenvalues.
2. Eliminate negative integer eigenvalues
3. Perform the substitution $\quad s = e^{-t}$

Consider diagonalizable linear vector fields with real, rational eigenvalues, and let Y be a semi-algebraic set. Then Pre(Y) is also semi-algebraic (and computable)

Diagonalizable, imaginary eigenvalues

Procedure is similar if system is diagonalizable with purely imaginary, rational eigenvalues

Equivalence is obtained by $\ z_1 = \cos(t) \quad z_2 = \sin(t)$
Suffices to compute over a period

Consider diagonalizable linear vector fields with real, rational eigenvalues, and let Y be a semi-algebraic set. Then Pre(Y) is also semi-algebraic (and computable)

Composing all computability results together results in…

Decidable problems for continuous systems

Consider linear vector fields of the form F(x)=Ax where

A is rational and nilpotent
A is rational, diagonalizable, with rational eigenvalues
A is rational, diagonalizable, with purely imaginary, rational eigenvalues

Then

1. The reachability problem between semi-algebraic sets is decidable.
2. Consider a finite semi-algebraic partition of the state space. Then a finite bisimulation always, exists and can be computed.
3. Consider a CTL* formula where atomic propositions denote semi-algebraic sets. Then CTL* model checking is decidable.

Decidable problems for hybrid systems

A hybrid system H is said to be o-minimal if

1. In each discrete state, all relevant sets and the flow of the vector field are definable in the same o-minimal theory.
2. After every discrete transition, state is reset to a constant set (forced initialization)

All o-minimal hybrid systems admit a finite bisimulation.

CTL* model checking is decidable for the class of o-minimal hybrid systems.

Decidable problems for hybrid systems

Consider a linear hybrid system H where

1. For each discrete state, all relevant sets are semi-algebraic
2. After every discrete transition, state is reset to a constant semi-algebraic set (forced initialization)
3. In each discrete location, the vector fields are of the form F(x)=Ax where
   A is rational and nilpotent
   A is rational, diagonalizable, with rational eigenvalues
   A is rational, diagonalizable, with purely imaginary, rational eigenvalues

Then

CTL* model checking is decidable for this class of linear hybrid systems.

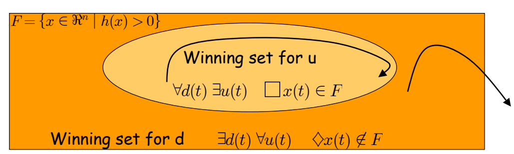
The reachability problem is decidable for such linear hybrid systems.

Safety games

Consider the following differential game

$$\dot{x} = Ax + Bu + Ed \quad u \in U \ \ d \in D$$

Objective for control : Remain in semi-algebraic set F
Objective for disturbance : Exit semi-algebraic set F



Optimal control

The Hamiltonian

$$H(x,p,u,d) = p^T Ax + p^T Bu + p^T Ed$$

must satisfy the Hamilton-Jacobi-Isaacs condition

$$\max_{u\in U} \min_{d\in D} H(x,p,u,d) = \min_{d\in D} \max_{u\in U} H(x,p,u,d)$$

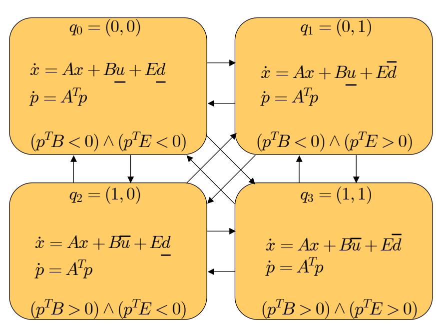
Optimum (bang-bang) policies satisfy

$$\dot{x} = \frac{\partial H}{\partial p} \qquad u^* = \arg\ \max_{u\in U}\ p^T Bu$$

$$\dot{p} = \left(\frac{\partial H}{\partial x}\right)^T \qquad d^* = \arg\ \min_{d\in D}\ p^T Ed$$

$$p(x,0) = \frac{\partial h}{\partial x}$$

Encoding game as hybrid system



Pontryagin Maximum Principle

A linear system $\dot{x} = Ax + Bu$ is **normal** if for each input column b_i, the pair (A, b_i) is completely controllable.

If the linear system is **normal** with respect to both control and disturbance, then for any initial state the optimal control and optimal disturbance are **well-defined**, **unique** and **piece-wise constant** taking values on the **vertices** of U and D.

If the linear system is normal and A has **purely real eigenvalues**, then there is a **global**, **uniform upper bound**, independent of the initial state on the number of switchings of the optimal control and optimal disturbance.

Decidable games

Combining optimal control and decidable logics we get…

Consider the differential game

$$\dot{x} = Ax + Bu + Ed \quad u \in U \;\; d \in D$$

with target set

$$F = \{x \in \Re^n \mid h(x) > 0\}$$

If the system is normal and A has real eigenvalues, then the differential game can be decided.

Winning sets for u and d can be computed.
Least restrictive controllers can be computed.

Extension to chained form

Consider chained system

$$\begin{aligned}
\dot{x}_j^0 &= u_j & & j = 1, \ldots, m \\
\dot{x}_{ij}^1 &= x_i^0 u_j & & j = 1, \ldots, m \text{ and } i < j \\
\dot{x}_{ij}^k &= x_{ij}^{k-1} u_j & & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j.
\end{aligned}$$

Construct Hamiltonian

$$H(x,p,u) = p^T f(x,u) = \sum_{j=1}^m \left(p_j^0 + \sum_{i=1}^{j-1} \left(p_{ij}^1 x_i^0 + \sum_{k=2}^{n_j} p_{ij}^k x_{ij}^{k-1}\right)\right) u_j$$

Co-state dynamics

$$\begin{aligned}
\dot{p}_{ij}^{n_j} &= 0 & & j = 1, \ldots, m \text{ and } i < j \\
\dot{p}_{ij}^{k-1} &= -p_{ij}^k u_j & & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\
\dot{p}_i^0 &= -\sum_{j=1}^m p_{ij}^1 u_j & & i = 1, \ldots, m.
\end{aligned}$$

Optimal control satisfies maximum principle:

$$u_j^* = \arg\max_{u_j \in [\underline{U}_j, \overline{U}_j]} \left(p_j^0 + \sum_{i=1}^{j-1} \left(p_{ij}^1 x_i^0 + \sum_{k=2}^{n_j} p_{ij}^k x_{ij}^{k-1}\right)\right) u_j$$

Polynomial flows

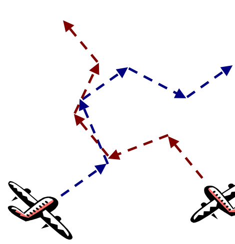
Dynamics in discrete state (optimal input is constant)

$$\begin{aligned}
\dot{x}_j^0 &= u_j^* & & j = 1, \ldots, m \\
\dot{x}_{ij}^1 &= x_i^0 u_j^* & & j = 1, \ldots, m \text{ and } i < j \\
\dot{x}_{ij}^k &= x_{ij}^{k-1} u_j^* & & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\
\dot{p}_{ij}^{n_j} &= 0 & & j = 1, \ldots, m \text{ and } i < j. \\
\dot{p}_{ij}^{k-1} &= -p_{ij}^k u_j^* & & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 2, \ldots, n_j \\
\dot{p}_i^0 &= -\sum_{j=1}^m p_{ij}^1 u_j^* & & i = 1, \ldots, m,
\end{aligned}$$

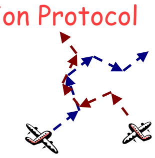
Polynomial flow in each discrete state

$$\begin{aligned}
x_i^0(t) &= x_i^0(0) + u_i^* t & & i = 1, \ldots, m \\
x_{ij}^1(t) &= x_{ij}^1(0) + x_i^0(0) u_j^* t + \tfrac{1}{2} u_i^* u_j^* t^2 & & \\
&\;\;\vdots & & \\
p_{ij}^{n_j}(t) &= p_{ij}^{n_j}(0) & & j = 1, \ldots, m \text{ and } i < j \\
p_{ij}^k(t) &= \sum_{l=0}^{n_j - k} \frac{(-u_j^* t)^l}{l!} p_{ij}^{k+l}(0) & & j = 1, \ldots, m \text{ and } i < j \text{ and } k = 1, \ldots, n_j \\
p_i^0(t) &= p_i^0(0) + \sum_{l=1}^{n_j - 1} \frac{(-u_j^* t)^l}{l!} p_{ij}^l(0) & & i = 1, \ldots, m.
\end{aligned}$$

Conflict Resolution in ATM*



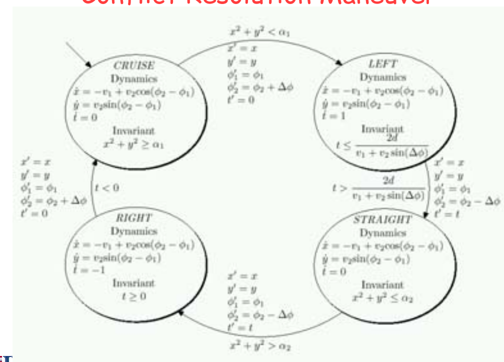
Conflict Resolution Protocol



1. Cruise until a_1 miles away
2. Change heading by $\Delta\Phi$
3. Maintain heading until lateral distance d
4. Change to original heading
5. Change heading by - $\Delta\Phi$
6. Maintain heading until lateral distance - d
7. Change to original heading

Is this protocol safe ?

Conflict Resolution Maneuver



Computing Unsafe Sets

$$v_1 = 4; v_2 = 5; \lambda = 0$$

$$\begin{aligned}
\texttt{unsafeCruise} &= \texttt{Resolve}\left[\exists t > 0 \wedge (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1-\lambda^2}v_2 t)^2 \leq 25\right] \\
&= \left(y < -\tfrac{20}{\sqrt{41}} \wedge -\sqrt{41} - \tfrac{4y}{5} \leq x \leq \sqrt{41} - \tfrac{4y}{5}\right) \vee \left(y = -\tfrac{20}{\sqrt{41}} \wedge -\sqrt{41} - \tfrac{4y}{5} < x \leq \sqrt{41} - \tfrac{4y}{5}\right) \vee \\
&\quad \left(y = \tfrac{20}{\sqrt{41}} \wedge -\sqrt{25-y^2} < x < \sqrt{41} - \tfrac{4y}{5}\right) \vee \left(\tfrac{20}{\sqrt{41}} \leq y < 5 \wedge -\sqrt{25-y^2} < x < \sqrt{25-y^2}\right) \vee \\
&\quad \left(-\tfrac{20}{\sqrt{41}} < y < \tfrac{20}{\sqrt{41}} \wedge -\sqrt{25-y^2} < x \leq \sqrt{41} - \tfrac{4y}{5}\right)
\end{aligned}$$

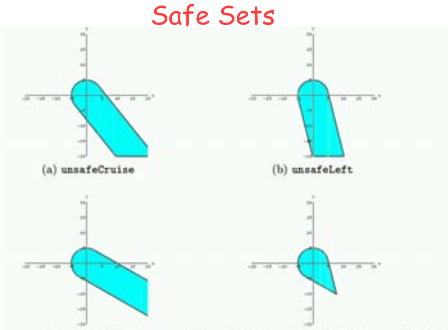
$$v_1 = 4; v_2 = 5; \lambda = \tfrac{3}{5}$$

$$\begin{aligned}
\texttt{unsafeLeft} &= \texttt{Resolve}\left[\exists t > 0 \wedge (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1-\lambda^2}v_2 t)^2 \leq 25\right] \\
&= \left(y < -\tfrac{5}{\sqrt{17}} \wedge -\tfrac{5\sqrt{17}}{4} - \tfrac{y}{4} \leq x \leq \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right) \vee \left(y = -\tfrac{5}{\sqrt{17}} \wedge -\tfrac{5\sqrt{17}}{4} - \tfrac{y}{4} < x \leq \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right) \vee \\
&\quad \left(y = \tfrac{5}{\sqrt{17}} \wedge -\sqrt{25-y^2} < x < \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right) \vee \left(\tfrac{5}{\sqrt{17}} < y < 5 \wedge -\sqrt{25-y^2} < x < \sqrt{25-y^2}\right) \vee \\
&\quad \left(-\tfrac{5}{\sqrt{17}} < y < \tfrac{5}{\sqrt{17}} \wedge -\sqrt{25-y^2} < x \leq \tfrac{5\sqrt{17}}{4} - \tfrac{y}{4}\right)
\end{aligned}$$

$$v_1 = 4; v_2 = 5; \lambda = -\tfrac{3}{5}$$

$$\begin{aligned}
\texttt{unsafeRight} &= \texttt{Resolve}\left[\exists t > 0 \wedge (x - v_1 t + \lambda v_2 t)^2 + (y + \sqrt{1-\lambda^2}v_2 t)^2 \leq 25\right] \\
&= \left(y < -7\sqrt{\tfrac{5}{13}} \wedge -\tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4} \leq x \leq \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right) \vee \left(y = -7\sqrt{\tfrac{5}{13}} \wedge -\tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4} < x \leq \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right) \vee \\
&\quad \left(y = 7\sqrt{\tfrac{5}{13}} \wedge -\sqrt{25-y^2} < x < \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right) \vee \left(7\sqrt{\tfrac{5}{13}} < y < 5 \wedge -\sqrt{25-y^2} < x < \sqrt{25-y^2}\right) \vee \\
&\quad \left(-7\sqrt{\tfrac{5}{13}} < y < 7\sqrt{\tfrac{5}{13}} \wedge -\sqrt{25-y^2} < x \leq \tfrac{5\sqrt{65}}{4} - \tfrac{7y}{4}\right)
\end{aligned}$$

Safe Sets



(a) unsafeCruise (b) unsafeLeft (c) unsafeRight (d) unsafeCruise ∧ unsafeLeft ∧ unsafeRight

Continuous to discrete (Lectures 3 & 4)

Lecture 3

T / ≈

T ≡ T / ≈

T $\frac{dx}{dt} = Ax$

Restricted dynamical systems
Semi-algebraic partitions
Verification semantics

Lecture 4

T / ≈

T ≡ T / ≈

T $\frac{dx}{dt} = Ax + Bu$

Linear control systems
Restricted partitions
Synthesis semantics