ESE601: Hybrid Systems

Reachability and Safety Analysis

Spring 2006
Transition Systems

A transition system

\[ T = (Q, \Sigma, \rightarrow, O, \langle \cdot \rangle) \]

consists of

- A set of states \( Q \)
- A set of events \( \Sigma \)
- A set of observations \( O \)
- The transition relation \( q_1 \rightarrow q_2 \)
- The observation map \( \langle q_1 \rangle = o_0 \)

Initial or final states may be incorporated
The sets \( Q, \Sigma, \) and \( O \) may be infinite
A painful example

The parking meter

States $Q = \{0, 1, 2, \ldots, 60\}$

Events $\{\text{tick}, 5\text{p}\}$

Observations $\{\text{exp}, \text{act}\}$

A possible string of observations $(\text{exp}, \text{act}, \text{act}, \text{act}, \text{act}, \text{act}, \text{exp}, \ldots)$
A familiar example

Transition System $T^\Delta$

State set $Q = X = \mathbb{R}^n$

Label set $\Sigma = U = \mathbb{R}^m$

Observation set $O = Y = \mathbb{R}^p$

Linear Observation Map $\langle x \rangle = C x$

Transition Relation $\rightarrow \subseteq X \times U \times X$

$x_{k+1} = Ax_k + Bu_k$

$\gamma_k = C x_k$

$x_1 \rightarrow x_2 \iff x_2 = Ax_1 + Bu$
Transition Systems

A region is a subset of states $P \subseteq Q$

We define the following operators:

- $Pre_\sigma(P) = \{q \in Q \mid \exists p \in P \quad q \xrightarrow{\sigma} p\}$
- $Pre(P) = \{q \in Q \mid \exists \sigma \in \Sigma \quad \exists p \in P \quad q \xrightarrow{\sigma} p\}$
- $Post_\sigma(P) = \{q \in Q \mid \exists p \in P \quad p \xrightarrow{\sigma} q\}$
- $Post(P) = \{q \in Q \mid \exists \sigma \in \Sigma \quad \exists p \in P \quad p \xrightarrow{\sigma} q\}$
Pre and Post operator

\[ \text{Post}_\alpha(P) \]

\[ \text{Post}_\sigma(P) \]
Pre and Post operator

\[ \text{Pre}_{\alpha}(P) \]

\[ \text{Pre}_{\sigma}(P) \]

\[ \text{Pre}(P) \]
Transition Systems

We can recursively define

\[
\text{Pre}_\sigma^1(P) = \text{Pre}_\sigma(P)
\]

\[
\text{Pre}_\sigma^n(P) = \text{Pre}_\sigma(\text{Pre}_\sigma^{n-1}(P))
\]

Similarly for the other operators. Also

\[
\text{Pre}^*(P) = \bigcup_{n \in \mathbb{N}} \text{Pre}^n(P)
\]

\[
\text{Post}^*(P) = \bigcup_{n \in \mathbb{N}} \text{Post}^n(P)
\]
Basic safety problems

Given transition system $T$ and regions $P, S$ determine

**Forward Reachability**

$$\text{Post}^*(P) \cap S \neq \emptyset$$

**Backward Reachability**

$$P \cap \text{Pre}^*(S) \neq \emptyset$$
Conflict Resolution in ATM*

See paper (R8) on the website
Conflicts 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?
Safe Sets

(a) unsafeCruise

(b) unsafeLeft

(c) unsafeRight

(d) unsafeCruise \land unsafeLeft \land unsafeRight
Hybrid model of nuclear reactor

Analysis: Is shutdown reachable?
Algorithmic verification: NO

unsafe states!!
Forward reachability algorithm

**Forward Reachability Algorithm**

initialize \( R := P \)
while TRUE do
  if \( R \cap S \neq \emptyset \) return UNSAFE ; end if;
  if \( Post(R) \subseteq R \) return SAFE ; end if;
  \( R := R \cup Post(R) \)
end while

If \( T \) is finite, then algorithm terminates (decidability).

Complexity : \( O(n_I + m_R) \)

- initial states
- reachable transitions
If T is infinite, then there is no guarantee of termination.
Algorithmic issues

Representation issues
  Enumeration for finite sets
  Symbolic representation for infinite (or finite) sets

Operations on sets
  Boolean operations
  Pre and Post computations (closure?)

Algorithmic termination (decidability)
  Guaranteed for finite transition systems
  No guarantee for infinite transition systems
Continuous Dynamical Systems

\[ \dot{x}(t) = f(x(t), u(t)) \]
\[ x(t) \in \mathbb{R}^n, \, x(0) \in I, \, u(t) \in U \]

Continuous dynamics given differential equations

- Input \( u(t) \) is internal (disturbance rather than control)
- Dimension (scale) of the system: \( n \)
- Classification:
  - Linear system \( f(x,u) = Ax + Bu \)
  - Deterministic system \( f(x,u) = f(x) \)
Reachable Set

\[
\dot{x}(t) = f(x(t), u(t)) \\
x(t) \in \mathbb{R}^n, \ x(0) \in I, \ u(t) \in U
\]

\( x_f \) is reachable (at time \( t \)) if
\( \exists \ x_0 \in I, \ \exists \ u: [0, t] \rightarrow U, \text{ such that } x(t) = x_f. \)

- The reachable set is \( \text{Reach}(S) = \{x_f | x_f \text{ is reachable} \} \)
- The timed reachable set is \( \text{Reach}_{[0,T]}(S) = \{x_f | x_f \text{ is reachable at time } t \leq T \} \)

![Diagram of reachable sets](image)
Reachability Problem

Given a set $F \subseteq \mathbb{R}^n$, evaluate the expressions

$$\text{Reach}_{[0,T]}(S) \cap F = \emptyset$$
$$\text{Reach}(S) \cap F = \emptyset$$

- Safety verification ($F$ is an unsafe set)
- Exact computation difficult (impossible for most systems):
  $\Rightarrow$ Compute over-approximations the reachable set

$\Rightarrow S$ is safe
Several Approaches

1. Numerical Analysis:
   • Level Sets Methods
     [Tomlin, Mitchell and Bayen]
   • Flow Pipes
     [Krogh; Dang; Kurzhanski and Varaiya; Girard]

2. Convex Optimization:
   • Barrier Certificates
     [Prajna and Jadbabaie]

3. Computer Science:
   • Discrete Abstractions of Continuous Dynamics
     [Alur, Dang and Ivancic; Tiwari, Belta]
   • Hybridization
     [Henzinger; Asarin, Dang and Girard; Frehse]
Several Tools

- Level Sets Toolbox [Mitchell]
- Checkmate [Chutinan and Krogh]
- $d/dt$ [Dang and Maler]
- Ellipsoidal Toolbox [Kurzhanski and Varaiya]
- Sostools [Parillo and Prajna]
- Hytech [Henzinger]
- PHAVer [Frehse]
- ...

Check the Hybrid Systems Tools Wiki Page!

http://wiki.grasp.upenn.edu/~graspdoc/hst/
Main observation:
Given a time step $r$ and $T = Nr$,

$$\text{Reach}_{[0,T]}(S) = \bigcup_{k=0}^{k=N-1} \text{Reach}_{[kr,(k+1)r]}(S).$$

and

$$\text{Reach}_{[kr,(k+1)r]}(S) = \Phi_r\left(\text{Reach}_{[(k-1)r, kr]}(S)\right)$$

where $\Phi_r(X)$ is the set of points reachable at time $r$ from $X$. 
Flow Pipe Approximation

Choice of the representation of the reachable set:

- closed under linear maps and Minkowski sums
  -> Polytopes [Krogh; Dang]
  -> Accurate
  -> Not scalable (exponential complexity)

- scalable representations
  -> Ellipsoids [Kurzhanski and Varaiya]
  -> Oriented rectangular hull [Krogh]
  -> Not closed under linear maps and Minkowski sums
  -> Additional computations and approximations

- Zonotopes [Girard]
  -> Closed under linear maps and Minkowski sums
  -> Accurate
  -> Scalable (polynomial complexity/dimension)
Flow Pipe Approximation

Algorithm:

- Over-approximate $\text{Reach}_{[0,r]}(S)$
- Propagate the reachable set using $\Phi_r$

• For linear systems ($f(x,u)=Ax+Bu$):

$$\Phi_r(X) = \Phi_r X \oplus V \text{ where } \Phi_r = e^{rA}$$

• After initialization, only requires
  - linear transformations
  - Minkowski sums
Linear Systems

Linear systems: \( \dot{x} = Ax + Bu. \)

\[
x(t) = e^{At}x(0) + \int_0^t e^{A(t-\tau)}Bu(\tau)d\tau
\]

If \( u(t) \in \mathbb{R}^m : \text{im}[B \ AB \ \cdots \ A^{n-1}B] \)

If \( \|u(t)\|_\infty \leq \mu, \)

\[
\left\| \int_0^t e^{(t-\tau)A}Bu(\tau)d\tau \right\|_\infty \leq \int_0^t \left\| e^{(t-\tau)A}Bu(\tau) \right\|_\infty d\tau
\]
Linear Systems

\[
\int_0^t \left\| e^{(t-\tau)A} Bu(\tau) \right\|_\infty \, d\tau \leq \int_0^t \left\| e^{(t-\tau)A} B \right\|_\infty \left\| u(\tau) \right\|_\infty \, d\tau \\
\leq \int_0^t \left\| e^{(t-\tau)A} B \right\|_\infty \mu \, d\tau \\
= \mu \int_0^t \left\| e^{(t-\tau)A} B \right\|_\infty \, d\tau \\
= \mu \cdot \beta
\]

Thus \( \int_0^t e^{A(t-\tau)} Bu(\tau) \, d\tau \) is approximated with a rectangle.
What is a zonotope?

- Zonotope: Minkowski sum of a finite number of segments.

\[ Z = \left\{ x \in \mathbb{R}^n, x = c + \sum_{i=1}^{i=p} x_i g_i, -1 \leq x_i \leq 1 \right\}. \]

- \( c \) is the center of the zonotope, \( \{g_1, \ldots, g_p\} \) are the generators. The ratio \( p/n \) is the order of the zonotope.

Two dimensional zonotope with 3 generators
Some Properties of Zonotopes

• The encoding of a zonotope has a polynomial complexity with the dimension.

• The set of zonotopes is closed under linear transformation

\[ Z = (c, <g_1,\ldots,g_p>), LZ = (Lc, <Lg_1,\ldots,Lg_p>). \]

• The set of zonotopes is closed under the Minkowski sum

\[ Z_1 = (c_1, <g_1,\ldots,g_p>), Z_2 = (c_2, <h_1,\ldots,h_q>). \]

\[ Z_1 \oplus Z_2 = (c_1+c_2, <g_1,\ldots,g_p,h_1,\ldots,h_q>). \]

• Exactly what we need for our reachability algorithm
Reachability Algorithm with Zonotopes

APPROXIMATE Reach\(_{[0,T]}(S)\)

1. \( r = \frac{T}{N} \)

2. Obtain a zonotope \( Q_0 \) as an over approximation of \( \text{Reach}_{[0,r]}(S) \).

3. \( R_0 = Q_0 \).

4. \( Q_{i+1} = e^{At}Q_i \oplus \Box \).

5. \( R_{i+1} = R_i \cup Q_{i+1} \).

6. \( \text{Reach}_{[0,T]}(S) \approx R_N \)
Two dimensional example

Reachable set on the interval \([0,2]\), 100 iterations.
Five dimensional example

Projections of the reachable set on the interval [0,1], 200 iterations.
Flow Pipe Approximation

Advantages:
- Using a time step small enough, can approximate the reachable set at any desired accuracy.
- Suitable for the verification of large scale systems.

Drawbacks:
- Not so good for nonlinear systems.
- Needs further work for hybrid systems
Ellipsoidal techniques

- Approximate the reachable set of
  \[ \dot{x} = A(t)x + B(t)u, \quad 0 \leq t \leq T \]
  with \( u(t) \) contained in an ellipsoid
  \[ (u - q)^T Q (u - q) \leq 1 \]

- \( q \) is the center of the ellipsoid, \( Q \) is a positive definite matrix.

- The reachable set is approximated from the inside and outside with ellipsoids.
Application to Hybrid Systems

- This method can be used for checking reachability within each location.

- To be applied to hybrid systems, we need to be able to detect intersection of the reachable set and the guard.

- Assuming that the guard is given by a hyperplane $d^T x = e$, the intersection of the reachable sets with the guard can be detected by detecting the intersection of $Q_i$ and the guard.

- Note that intersection of a hyperplane and a zonotope is not necessarily a zonotope.