Controller synthesis

Antoine Girard

CNRS, Laboratoire des Signaux et Systèmes
Gif-sur-Yvette, France

Ph.D. Course on Hybrid Systems
Politecnico di Milano, July 1-5, 2019

Outline of the lecture

1. Qualitative synthesis
   Safety, reachability, stability, recurrence, automata-based specifications...
2. Quantitative synthesis
   Safety, reachability, stability...

Controllers for transition systems

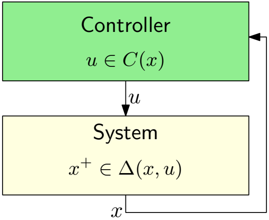
Consider a symbolic transition system $T = (X, U, \Delta)$.

Definition

A (static state-feedback) controller for T is a map $C : X \rightrightarrows U$ such that for all $x \in \mathrm{dom}(C)$, $C(x) \subseteq \mathrm{enab}_\Delta(x)$.

The dynamics of the controlled system is described by the transition system $T_C = (X, U, \Delta_C)$ where

$$x^+ \in \Delta_C(x, u) \iff \big(u \in C(x) \text{ and } x^+ \in \Delta(x, u)\big).$$



Safety controllers

Given a subset of safe states $X_s \subseteq X$:

Definition

$C : X \rightrightarrows U$ is a safety controller if all maximal trajectories of T_C, $((x_k)_{k=0}^{k=N}, (u_k)_{k=0}^{k=N-1})$, starting in $\mathrm{dom}(C)$, are complete and satisfy:

$$\forall k \in \mathbb{N},\ x_k \in X_s.$$

Definition

A state x is safety controllable if there exists a safety controller C such that $x \in \mathrm{dom}(C)$.

The set of safety controllable states is denoted $\text{S-cont}(T, X_s)$.

Reachability controllers

Given a subset of target states $X_t \subseteq X$:

Definition

$C : X \rightrightarrows U$ is a reachability controller if all maximal trajectories of T_C, $((x_k)_{k=0}^{k=N}, (u_k)_{k=0}^{k=N-1})$, starting in $\mathrm{dom}(C)$, satisfy:

$$\exists k \in \mathbb{N},\ x_k \in X_t.$$

Definition

A state x is reachability controllable if there exists a reachability controller C such that $x \in \mathrm{dom}(C)$.

The set of reachability controllable states is denoted $\text{R-cont}(T, X_t)$.

Synthesis - safety and reachability

Controllable predecessors of a subset $P \subseteq X$:

$$Pre(P) = \{x \in X | \; \exists u \in \text{enab}_\Delta(x), \; \Delta(x,u) \subseteq P\}.$$

Safety synthesis

$P_0 = X_s$
loop
| $P_{k+1} = X_s \cap Pre(P_k)$
until $P_{k+1} = P_k$
return $P^* = P_k$

Reachability synthesis

$Q_0 = X_t$
loop
| $Q_{k+1} = X_t \cup Pre(Q_k)$
until $Q_{k+1} = Q_k$
return $Q^* = Q_k$

For symbolic systems, termination guaranteed by finiteness of X.

Theorem

For symbolic systems, we have $P^* = S\text{-}cont(T, X_s)$, $Q^* = R\text{-}cont(T, X_t)$.

Stability and recurrence

Given a set of target states $X_t \subseteq X$:

Definition

$C : X \rightrightarrows U$ is a stability controller if all maximal trajectories of T_C, $((x_k)_{k=0}^{k=N}, (u_k)_{k=0}^{k=N-1})$, starting in $\mathrm{dom}(C)$, are complete and satisfy:

$$\exists j \in \mathbb{N},\ \forall k \geq j,\ x_k \in X_t.$$

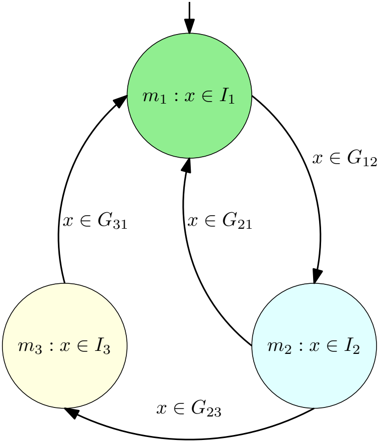
Definition

$C : X \rightrightarrows U$ is a recurrence controller if all maximal trajectories of T_C, $((x_k)_{k=0}^{k=N}, (u_k)_{k=0}^{k=N-1})$, starting in $\mathrm{dom}(C)$, are complete and satisfy:

$$\forall j \in \mathbb{N},\ \exists k \geq j,\ x_k \in X_t.$$

- Synthesis through nested fixed point computation
- Termination guaranteed by finiteness of X

Automata-based specifications



- Hybrid automata semantics
- Compute the product of symbolic model and automaton
- Specifications and controllers defined on the product space:
  - safety, reachability...
  - stability and...
  - recurrence

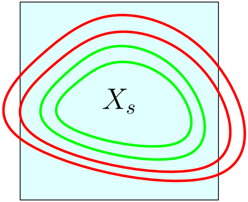
    $\Longrightarrow$ Linear Temporal Logic (LTL)

Outline of the lecture

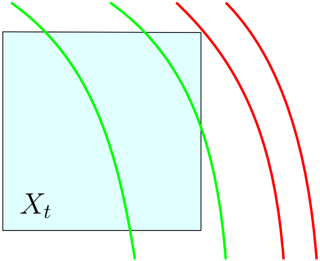
1. Qualitative synthesis
   Safety, reachability, stability, recurrence, automata-based specifications...
2. Quantitative synthesis
   Safety, reachability, stability...

Quantitative approach to safety and reachability

Safety

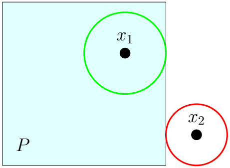


Reachability



Signed distance:

$$d(x,P) = \begin{cases} \sup\{\delta \geq 0 |\ B_\delta(x) \cap P \neq \emptyset\} & \text{if } x \notin P \\ -\sup\{\delta \geq 0 |\ B_\delta(x) \subseteq P\} & \text{if } x \in P \end{cases}$$



Quantitative safety synthesis

Optimal control formulation:

$$\text{Minimize } \sup_{k \in \mathbb{N}} d(x_k, X_s)$$

Quantitative safety synthesis

$V_0(x) = d(x, X_s)$

loop

$$V_{k+1}(x) = \begin{cases} \max\left(d(x,X_s), \min\limits_{u \in \text{enab}_\Delta(x)} \max\limits_{x' \in \Delta(x,u)} V_k(x')\right) & \text{if } x \in \text{nbs}_\Delta \\ +\infty & \text{if } x \notin \text{nbs}_\Delta \end{cases}$$

until $V_{k+1} = V_k$

return $V^* = V_k$

- Termination guaranteed by finiteness of X
- Extension of the fixed point computation for qualitative synthesis

Quantitative safety synthesis

Consider the controller given for $x \in X$, such that $V^*(x) \neq +\infty$ by

$$C(x) = \arg \min_{u \in \text{enab}_\Delta(x)} \max_{x' \in \Delta(x,u)} V^*(x').$$

Theorem

All maximal trajectories of T_C, $((x_k)_{k=0}^{k=N}, (u_k)_{k=0}^{k=N-1})$, *starting in* $\text{dom}(C)$, *are complete and satisfy:*

$$\forall k \in \mathbb{N},\ d(x_k, X_s) \leq V^*(x_0).$$

For all $\delta \in \mathbb{R}$, *S-cont*$(T, B_\delta(X_s)) = \{x \in X |\ V^*(x) \leq \delta\}$.

- Computation of a parameterized family of safety controllable sets
- Common safety controller for all the family

Optimal control formulation:

$$\text{Minimize } \inf_{k \in \mathbb{N}} d(x_k, X_t)$$

Quantitative reachability synthesis

$V_0(x) = d(x, X_t)$

loop

$$V_{k+1}(x) = \begin{cases} \min\left(d(x, X_t), \min\limits_{u \in \mathrm{enab}_\Delta(x)} \max\limits_{x' \in \Delta(x,u)} V_k(x')\right) & \text{if } x \in \mathrm{nbs}_\Delta \\ d(x, X_t) & \text{if } x \notin \mathrm{nbs}_\Delta \end{cases}$$

until $V_{k+1} = V_k$

return $V^* = V_k$

- Termination guaranteed by finiteness of X
- Extension of the fixed point computation for qualitative synthesis

Let $k^*(x) = \min\{k \in \mathbb{N} |\ V_k(x) = V^*(x)\}$.
Consider the controller given for $x \in X$, such that $k^*(x) \neq 0$ by

$$C(x) = \arg \min_{u \in \mathrm{enab}_\Delta(x)} \max_{x' \in \Delta(x,u)} V_{k^*(x)-1}(x').$$

Theorem

All maximal trajectories of T_C, $((x_k)_{k=0}^{k=N}, (u_k)_{k=0}^{k=N-1})$, starting in $dom(C)$, satisfy:

$$\exists k \in \mathbb{N},\ d(x_k, X_t) \leq V^*(x_0).$$

For all $\delta \in \mathbb{R}$, R-cont$(T, B_\delta(X_s)) = \{x \in X |\ V^*(x) \leq \delta\}$.

- Parameterized family of reachability controllable sets
- Common safety controller for all the family

Qualitative stability synthesis

Stability as "reachability then safety"

Quantitative stability synthesis

$V_0(x) = d(x, X_s)$

loop

$$V_{k+1}(x) = \begin{cases} \max\left(d(x, X_s), \min\limits_{u \in \mathrm{enab}_\Delta(x)} \max\limits_{x' \in \Delta(x,u)} V_k(x')\right) & \text{if } x \in \mathrm{nbs}_\Delta \\ +\infty & \text{if } x \notin \mathrm{nbs}_\Delta \end{cases}$$

until $V_{k+1} = V_k$

$V^*(x) = V_k(x),\ W_0(x) = V^*(x)$

loop

$$W_{k+1}(x) = \begin{cases} \min\left(V^*(x), \min\limits_{u \in \mathrm{enab}_\Delta(x)} \max\limits_{x' \in \Delta(x,u)} W_k(x')\right) & \text{if } x \in \mathrm{nbs}_\Delta \\ V^*(x) & \text{if } x \notin \mathrm{nbs}_\Delta \end{cases}$$

until $W_{k+1} = W_k$

return $W^* = W_k$

Quantitative stability synthesis

Let $k^*(x) = \min\{k \in \mathbb{N} | \; W_k(x) = W^*(x)\}$.
Consider the controller given for $x \in X$, such that $W^*(x) \neq +\infty$ by

$$C(x) = \begin{cases} \arg \min\limits_{u \in \mathrm{enab}_\Delta(x)} \max\limits_{x' \in \Delta(x,u)} W_{k^*(x)-1}(x') & \text{if } k^*(x) \neq 0 \\ \arg \min\limits_{u \in \mathrm{enab}_\Delta(x)} \max\limits_{x' \in \Delta(x,u)} V^*(x') & \text{if } k^*(x) = 0 \end{cases}$$

Theorem

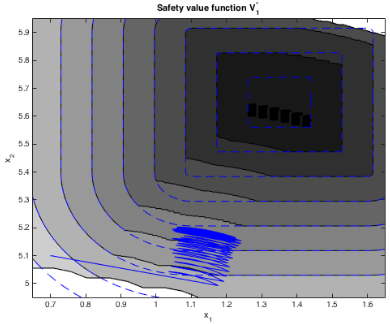
All maximal trajectories of T_C, $((x_k)_{k=0}^{k=N}, (u_k)_{k=0}^{k=N-1})$, starting in $dom(C)$ are complete and satisfy:

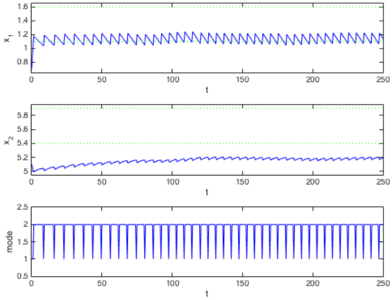
$$\exists j \in \mathbb{N}, \forall k \geq j, \;\; d(x_k, X_t) \leq W^*(x_0).$$

Example - DC/DC converter

Model: $\dot{x} = A_p x + b_p, \ p \in \{1, 2\}$

Safety specification: $X_s = [1.1, 1.6] \times [5.4, 5.9]$



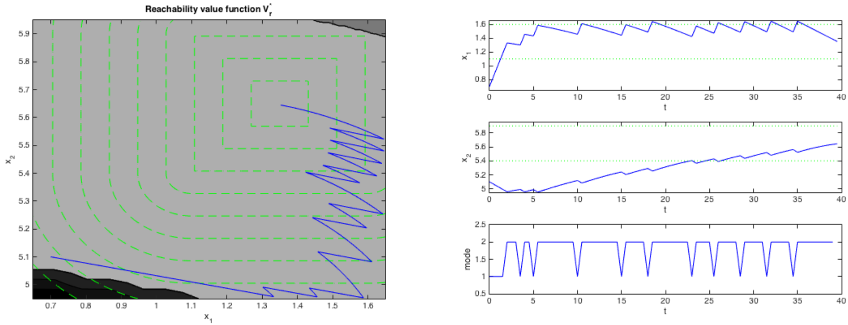


Quantitative safety
(left: value function, right: trajectory)

Example - DC/DC converter

Model: $\dot{x} = A_p x + b_p, \ p \in \{1, 2\}$

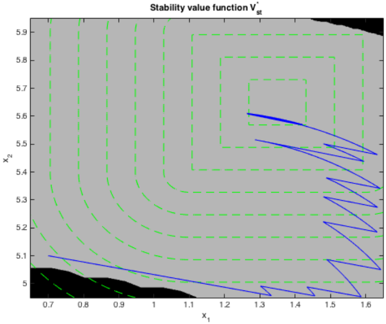
Reachability specification: $X_t = [1.1, 1.6] \times [5.4, 5.9]$

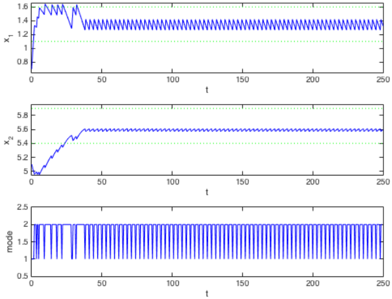


Quantitative reachability
(left: value function, right: trajectory)

Model: $\dot{x} = A_p x + b_p, \ p \in \{1, 2\}$

Stability specification: $X_t = [1.1, 1.6] \times [5.4, 5.9]$





Quantitative stability

(left: value function, right: trajectory)

Further reading

Oded Maler.
Control from computer science.
Annual Reviews in Control, 26(2):175–187, 2002.

Paulo Tabuada.
Verification and control of hybrid systems: a symbolic approach.
Springer Science & Business Media, 2009.

Krishnendu Chatterjee and Thomas A Henzinger.
Value iteration.
In *25 Years of Model Checking*, pages 107–138. Springer, 2008.

Alina Eqtami and Antoine Girard.
Safety control, a quantitative approach.
IFAC-PapersOnLine, 51(16):187–192, 2018.