Formal Methods for the Control of Large-scale Networked Nonlinear Systems with Logic Specifications

Basilica di Santa Maria di Collemaggio, L'Aquila (Italy), 1287

Lecture L4b:

Modeling logic specifications as regular languages

Speaker: Giordano Pola

Modeling logic specifications

- Consider a finite collection Y_Q of vectors of $\mathbb{R}^n$
- Logic specification defined as a regular language

$$L_Q \subseteq Y_Q^*$$

Definition above of specification is rather general and comprise many specifications of interest when controlling CPSoS

In the next slides we illustrate some examples of:

- Safety specifications
- Reachability specifications
- Reach and stay with obstacle avoidance specifications
- Synchronization specifications

Safety specifications

Specification: Given a subset of good states G of $\mathbb{R}^n$, stay all the time inside G

- Let η be the accuracy of the specification approximation
- Suppose that G has interior and is given as the union of a finite collection of hyperrectangles
- Consider the collection of vectors g_j in

$$G_\eta = G \cap \eta\mathbb{Z}^n \subseteq G$$

- There exists $\hat{\eta} > 0$ s.t. $G_\eta \neq \emptyset$ for any $\eta < \hat{\eta}$

Regular expression: words with symbols g_j, i.e.

$$\left(\sum_{g_j \in G_\eta} g_j\right)\left(\sum_{g_j \in G_\eta} g_j\right)^*$$

Reachability specifications

Specification: Starting from a set of initial states $I \subseteq \mathbb{R}^n$ reach a target set $T \subseteq \mathbb{R}^n$ in finite time

- Let η be the accuracy of the specification approximation
- Let $D \subseteq \mathbb{R}^n$ be the domain of interest and containing I and T
- Suppose that I, T and D have interior and are given as the union of a finite collection of hyperrectangles
- Consider the collections of vectors
  - i_j in I_η where I_η is the collection of vectors in $\eta\mathbb{Z}^n$ far away from I no more than η (with infinity norm metric)
  - t_j in $T_\eta = T \cap \eta\mathbb{Z}^n \subseteq T$
  - d_j in $D_\eta = D \cap \eta\mathbb{Z}^n \subseteq D$
- For any $\eta > 0$, $I_\eta \neq \emptyset$ and there exists $\hat{\eta} > 0$ s.t. $T_\eta \neq \emptyset$ and $D_\eta \neq \emptyset$ for any $\eta < \hat{\eta}$

Regular expression: words starting with i_j and ending with t_j, i.e.

$$\left(\sum_{i_j \in I_\eta} i_j\right)\left(\sum_{d_j \in D_\eta} d_j\right)^*\left(\sum_{t_j \in T_\eta} t_j\right)$$

Reach and stay with obstacle avoidance specifications (1/2)

Specification: Starting from a set of initial states $I \subseteq \mathbb{R}^n$ reach a target set $T \subseteq \mathbb{R}^n$ in finite time, while avoiding a set of obstacles $O \subseteq \mathbb{R}^n$ and then remain definitely in T

- We suppose $I \cap O \cap T = \emptyset$
- Let η be the accuracy of the specification approximation
- Let $D \subseteq \mathbb{R}^n$ be the domain of interest and containing I, T and O
- Suppose that I, T, O and D have interior and are given as the union of a finite collection of hyperrectangles
- Consider the collections of vectors
  - i_j in I_η where I_η is the collection of vectors in $\eta\mathbb{Z}^n$ far away from I no more than η (with infinity norm metric)
  - o_j in O_η where O_η is the collection of vectors in $\eta\mathbb{Z}^n$ far away from O no more than η (with infinity norm metric)
  - t_j in $T_\eta = T \cap \eta\mathbb{Z}^n \subseteq T$
  - d_j in $D_\eta = D \cap \eta\mathbb{Z}^n \subseteq D$
- For any $\eta > 0$, $I_\eta \neq \emptyset$ and $O_\eta \neq \emptyset$ and there exists $\hat{\eta} > 0$ s.t. $T_\eta \neq \emptyset$ and $D_\eta \neq \emptyset$ for any $\eta < \hat{\eta}$

Reach and stay with obstacle avoidance specifications (2/2)

Specification: Starting from a set of initial states $I \subseteq \mathbb{R}^n$ reach a target set $T \subseteq \mathbb{R}^n$ in finite time, while avoiding a set of obstacles $O \subseteq \mathbb{R}^n$ and then remain definitely in T

Regular expression: words starting with i_j, ending with t_j and with no o_j, i.e.

$$\left(\sum_{i_j \in I_\eta} i_j\right)\left(\sum_{d_j \in D_\eta \setminus O_\eta} d_j\right)^* \left(\sum_{t_j \in T_\eta} t_j\right)\left(\sum_{t_j \in T_\eta} t_j\right)^*$$

Synchronization specifications (1/2)

Specification: Starting from a set of initial states $I \subseteq \mathbb{R}^n$ reach a set $R \subseteq \mathbb{R}^n$ in no more than 2s, stay there for at most 4s and then reach a target set $T \subseteq \mathbb{R}^n$ in no less than 3s but in finite time

- We suppose $I \cap R \cap T = \emptyset$
- Let η be the accuracy of the specification approximation
- Let $D \subseteq \mathbb{R}^n$ be the domain of interest and containing I, R and T
- Suppose that I, T, O and D have interior and are given as the union of a finite collection of hyperrectangles
- Consider the collections of vectors
  - i_j in I_η where I_η is the collection of vectors in $\eta\mathbb{Z}^n$ far away from I no more than η (with infinity norm metric)
  - r_j in $R_\eta = R \cap \eta\mathbb{Z}^n \subseteq R$
  - t_j in $T_\eta = T \cap \eta\mathbb{Z}^n \subseteq T$
  - d_j in $D_\eta = D \cap \eta\mathbb{Z}^n \subseteq D$
- For any $\eta > 0$, $I_\eta \neq \emptyset$ and there exists $\hat{\eta} > 0$ s.t. $T_\eta \neq \emptyset$, $R_\eta \neq \emptyset$, and $D_\eta \neq \emptyset$ for any $\eta < \hat{\eta}$

Synchronization specifications (2/2)

Specification: Starting from a set of initial states $I \subseteq \mathbb{R}^n$ reach a set $R \subseteq \mathbb{R}^n$ in no more than 2s, stay there for at most 4s and then reach a target set $T \subseteq \mathbb{R}^n$ in no less than 3s but in finite time

- Set regular expressions

$$I' = \sum_{i_j \in I_\eta} i_j \,, \quad R' = \sum_{r_j \in R_\eta} r_j \,, \quad T' = \sum_{t_j \in T_\eta} t_j \,, \; D' = \sum_{d_j \in D_\eta \setminus R_\eta} d_j \,, \quad D'' = \sum_{d_j \in D_\eta \setminus T_\eta} d_j$$

- Suppose internal clock of the digital controller with $\tau = 1s$

Regular expression:

$$I'(\varepsilon + D')(R' + R'R' + R'R'R' + R'R'R'R')(D''D''(D'')^*)T'$$