Switching Controller Synthesis for Hybrid Systems Against STL Formulas

Han Su, Shenghua Feng, Sinong Zhan, Naijun Zhan

北京大学 PEKING UNIVERSITY
Northeastern University

FM · Milan · September 2024

Cyber-Physical Systems

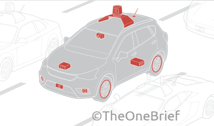
"Cyber-Physical Systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities ..."

— Radhakisan Baheti and Helen Gill : CPS. The Impact of Control Technology, 2011

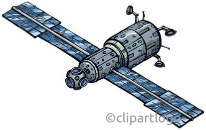
Cyber-Physical Systems

"Cyber-Physical Systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities ..."

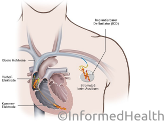
— Radhakisan Baheti and Helen Gill : CPS. The Impact of Control Technology, 2011



Automobiles



Avionics

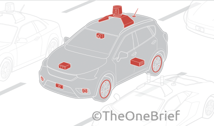


Medical Devices

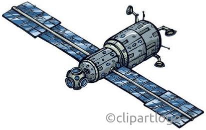
Cyber-Physical Systems

"Cyber-Physical Systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities ..."

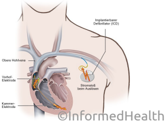
— Radhakisan Baheti and Helen Gill : CPS. The Impact of Control Technology, 2011



Automobiles



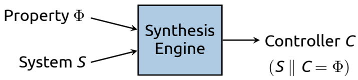
Avionics



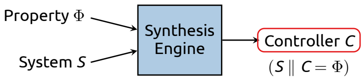
Medical Devices

Question : Can we design a Cyber-Physical System to meet a given specification?

Controller Synthesis

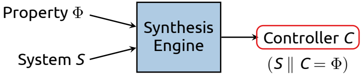


Controller Synthesis

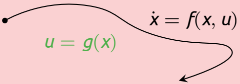


- Feedback Controller
- Switching Controller
- Reset Controller

Controller Synthesis

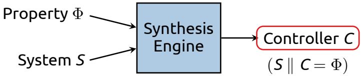


- Feedback Controller

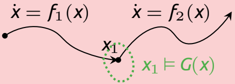


- Switching Controller
- Reset Controller

Controller Synthesis

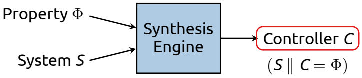


- Feedback Controller
- Switching Controller

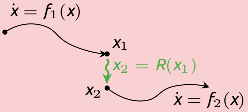


- Reset Controller

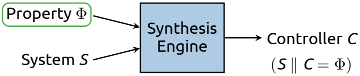
Controller Synthesis



- Feedback Controller
- Switching Controller
- Reset Controller



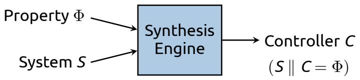
Controller Synthesis



- Feedback Controller
- Switching Controller
- Reset Controller

- Safety Properties
- Liveness Properties
- Linear Temporal Logic (LTL)
- Signal Temporal Logic (STL)
- ...

Controller Synthesis

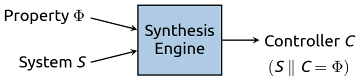


- Feedback Controller
- Switching Controller
- Reset Controller

STL Property + Feedback Controller :

- *V. Raman et al. "Model predictive control with signal temporal logic specifications."* —— MILP-based Method
- *L. Lindemann et al. "Control barrier functions for signal temporal logic tasks"* —— Barrier Certificate based Method
- *V. Raman et al. "Reactive synthesis from signal temporal logic specifications"* —— CEGIS based Method
- *C. Fan et al. "Signal temporal logic neural predictive control"* —— NN based Method

Controller Synthesis



- Feedback Controller
- **Switching Controller**
- Reset Controller

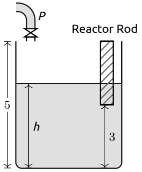
STL Property + Feedback Controller :

- *V. Raman et al. "Model predictive control with signal temporal logic specifications."* —— MILP-based Method
- *L. Lindemann et al. "Control barrier functions for signal temporal logic tasks"* —— Barrier Certificate based Method
- *V. Raman et al. "Reactive synthesis from signal temporal logic specifications"* —— CEGIS based Method
- *C. Fan et al. "Signal temporal logic neural predictive control"* —— NN based Method

We considered switching controller synthesis of hybrid system, with respect to Signal Temporal Logic.

Signal Temporal Logic (STL)

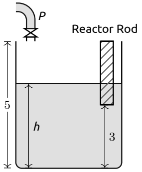
1. Keep liquid level in safe region (i.e., $0 \leq h \leq 4$)
2. Reaction between liquid and Reactor Rod happens at reaction phase $3 \leq t \leq 4$



Signal Temporal Logic (STL)

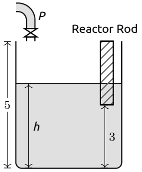
1. Keep liquid level in safe region (i.e., $0 \leq h \leq 4$)
2. Reaction between liquid and Reactor Rod happens at reaction phase $3 \leq t \leq 4$

$$\varphi = (0 \leq h \leq 4)\mathcal{U}_{[3,4]}(3 \leq h \leq 5)$$



Signal Temporal Logic (STL)

1. Keep liquid level in safe region (i.e., $0 \leq h \leq 4$)
2. Reaction between liquid and Reactor Rod happens at reaction phase $3 \leq t \leq 4$



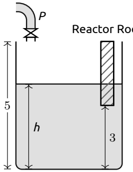
$$\varphi = (0 \leq h \leq 4)\mathcal{U}_{[3,4]}(3 \leq h \leq 5)$$

STL

$$\varphi := \top \mid \mu \geq 0 \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2$$

Signal Temporal Logic (STL)

1. Keep liquid level in safe region (i.e., $0 \leq h \leq 4$)
2. Reaction between liquid and Reactor Rod happens at reaction phase $3 \leq t \leq 4$



$$\varphi = (0 \leq h \leq 4)\mathcal{U}_{[3,4]}(3 \leq h \leq 5)$$

STL

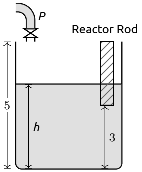
$$\varphi := \top \mid \mu \geq 0 \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2$$

ST-RA

$$\phi := \top \mid \mu \geq 0 \mid \neg\phi \mid \phi_1 \vee \phi_2$$
$$\varphi := \varphi_1 \mathcal{U}_I \varphi_2$$

Signal Temporal Logic (STL)

1. Keep liquid level in safe region (i.e., $0 \leq h \leq 4$)
2. Reaction between liquid and Reactor Rod happens at reaction phase $3 \leq t \leq 4$



$$\varphi = (0 \leq h \leq 4)\mathcal{U}_{[3,4]}(3 \leq h \leq 5)$$

STL

$$\varphi := \top \mid \mu \geq 0 \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2$$

ST-RA

$$\phi := \top \mid \mu \geq 0 \mid \neg\phi \mid \phi_1 \vee \phi_2$$
$$\varphi := \varphi_1 \mathcal{U}_I \varphi_2$$

- No nested “until” operator.
- No negation outside “until” operator.

Switched System

A switched system is defined as a tuple $\Phi = (Q, F, \mathtt{Init}, \pi)$, where

- $Q \triangleq \{ q_1, q_2, \ldots, q_m \}$ - Set of discrete modes,
- $F \triangleq \{ f_q \mid q \in Q \}$ - Set of vector fields,
- $\mathtt{Init} \subseteq \mathbb{R}^n$ - Set of initial states,
- $\pi \colon \mathtt{Init} \to (\mathbb{R}_{\geq 0} \to Q)$ - Switching controller.

Switched System

A switched system is defined as a tuple $\Phi = (Q, F, \texttt{Init}, \pi)$, where

- $Q \triangleq \{ q_1, q_2, \ldots, q_m \}$ - Set of discrete modes,
- $F \triangleq \{ f_q \mid q \in Q \}$ - Set of vector fields,
- $\texttt{Init} \subseteq \mathbb{R}^n$ - Set of initial states,
- $\pi : \texttt{Init} \to (\mathbb{R}_{\geq 0} \to Q)$ - Switching controller.

For any initial state x, $\pi(x)$ specifies the control mode in which the system resides at time t

Switched System

A switched system is defined as a tuple $\Phi = (Q, F, \mathtt{Init}, \pi)$, where

- $Q \triangleq \{ q_1, q_2, \ldots, q_m \}$ - Set of discrete modes,
- $F \triangleq \{ f_q \mid q \in Q \}$ - Set of vector fields,
- $\mathtt{Init} \subseteq \mathbb{R}^n$ - Set of initial states,
- $\pi : \mathtt{Init} \to (\mathbb{R}_{\geq 0} \to Q)$ - Switching controller.

For any initial state x, $\pi(x)$ specifies the control mode in which the system resides at time t

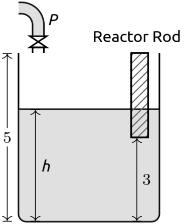
- Two Modes :

q_1 : P is ON $\qquad \dot{h} = 1,$

q_2 : P is OFF $\qquad \dot{h} = -1,$

- Switching Controller :

$$\pi(h_0) = \begin{cases} (q_1, 0), & \text{if } 0 \leq h_0 \leq 1 \\ (q_2, 0)(q_1, \frac{h_0 - 1}{2}), & \text{if } 1 < h_0 \leq 4. \end{cases}$$



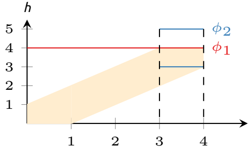
State-Time Sets X_q^i

$(x, \tau) \in X_q^i \iff$ The system, initiating from state x at time τ in mode q, satisfies the STL specification within i switch occurrences.

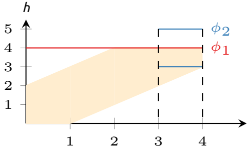
State-Time Sets X_q^i

$(x, \tau) \in X_q^i \iff$ The system, initiating from state x at time τ in mode q, satisfies the STL specification within i switch occurrences.

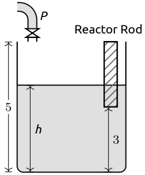
$$\varphi = \overbrace{(0 \le h \le 4)}^{\phi_1} \mathcal{U}_{[3,4]} \overbrace{(3 \le h \le 5)}^{\phi_2}$$



$X_{q_1}^0$



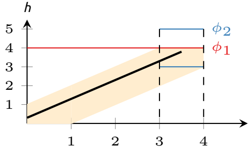
$X_{q_1}^1$



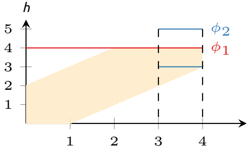
State-Time Sets X_q^i

$(x, \tau) \in X_q^i \iff$ The system, initiating from state x at time τ in mode q, satisfies the STL specification within i switch occurrences.

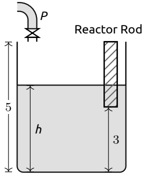
$$\varphi = \overbrace{(0 \le h \le 4)}^{\phi_1} \mathcal{U}_{[3,4]} \overbrace{(3 \le h \le 5)}^{\phi_2}$$



$X_{q_1}^0$



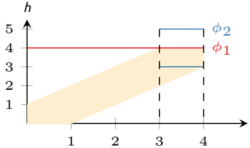
$X_{q_1}^1$



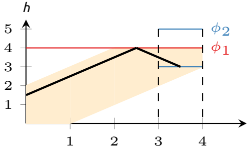
State-Time Sets X_q^i

$(x, \tau) \in X_q^i \iff$ The system, initiating from state x at time τ in mode q, satisfies the STL specification within i switch occurrences.

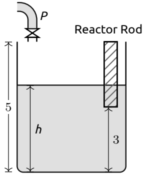
$$\varphi = \overbrace{(0 \le h \le 4)}^{\phi_1} \mathcal{U}_{[3,4]} \overbrace{(3 \le h \le 5)}^{\phi_2}$$



$X_{q_1}^0$



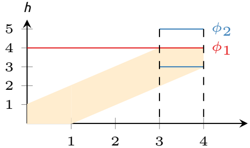
$X_{q_1}^1$



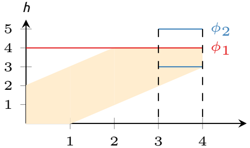
State-Time Sets X_q^i

$(x, \tau) \in X_q^i \iff$ The system, initiating from state x at time τ in mode q, satisfies the STL specification within i switch occurrences.

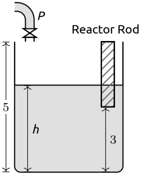
$$\varphi = \overbrace{(0 \leq h \leq 4)}^{\phi_1} \mathcal{U}_{[3,4]} \overbrace{(3 \leq h \leq 5)}^{\phi_2}$$



$X_{q_1}^0$

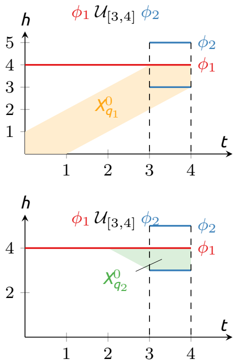


$X_{q_1}^1$

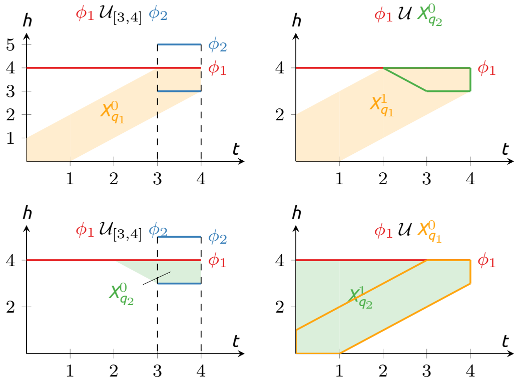


- $\cup_{i \in \mathbb{N}} \cup_{q \in Q} X_q^i[t=0]$ is all the initial states that can be driven to satisfy the given STL formula.
- Switching controller can be extracted from the state-time sets.

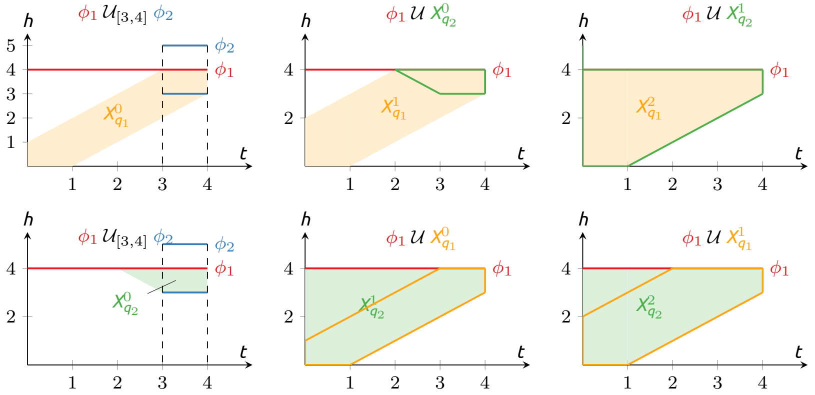
Iteratively Compute State-Time Set



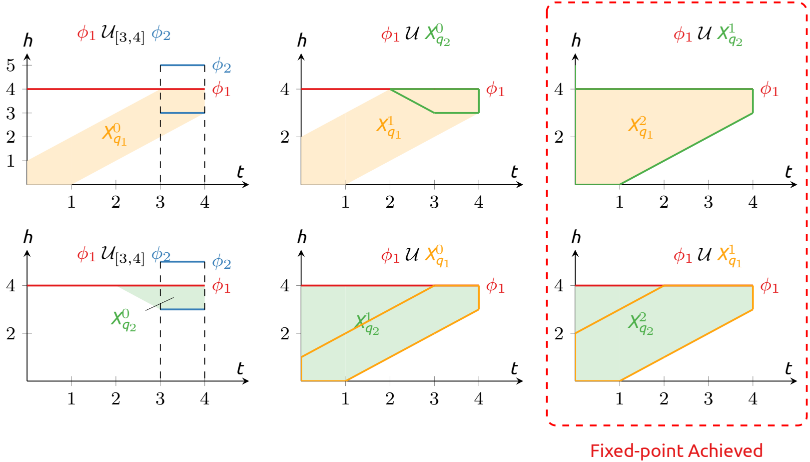
Iteratively Compute State-Time Set



Iteratively Compute State-Time Set



Iteratively Compute State-Time Set



Synthesizing Switching Controller

Theorem

For any $q \in Q$, suppose the solution of ODE $\dot{\mathbf{x}}(t) = f_q(\mathbf{x}(t))$ with initial x at time τ is denoted by $\Psi(\,\cdot\,; x, \tau, q)$, then the state-time sets can be inductively represented by

$$X_q^0 = \mathrm{QE}\left(\exists \delta \geq 0,\ \left(\phi_2[(x,t) = (\Psi(t+\delta; x, t, q), t+\delta)] \wedge (t + \delta \in I)\right) \wedge \left(\forall 0 \leq h \leq \delta,\ \phi_1[(x,t) = (\Psi(t+h; x, t, q), t+h)]\right)\right) \quad (1)$$

$$X_q^i = \bigvee_{q' \neq q} \mathrm{QE}\left(\exists \delta \geq 0,\ \left(X_{q'}^{i-1}[(x,t) = (\Psi(t+\delta; x, t, q), t+\delta)]\right) \wedge \left(\forall 0 \leq h \leq \delta,\ \phi_1[(x,t) = (\Psi(t+h; x, t, q), t+h)]\right)\right) \quad (2)$$

for any $q \in Q$ and any $i \in \mathbb{N}$.

Synthesizing Switching Controller

Theorem

For any $q \in Q$, suppose the solution of ODE $\dot{\boldsymbol{x}}(t) = f_q(\boldsymbol{x}(t))$ with initial x at time τ is denoted by $\Psi(\,\cdot\,; x, \tau, q)$, then the state-time sets can be inductively represented by

$$X_q^0 = \mathrm{QE}\Big(\exists \delta \geq 0,\ \big(\phi_2[(x,t) = (\Psi(t+\delta; x, t, q), t+\delta)] \wedge (t+\delta \in I)\big) \wedge \big(\forall 0 \leq h \leq \delta,\ \phi_1[(x,t) = (\Psi(t+h; x, t, q), t+h)]\big)\Big) \tag{1}$$

$$X_q^i = \bigvee_{q' \neq q} \mathrm{QE}\Big(\exists \delta \geq 0,\ \big(X_{q'}^{i-1}[(x,t) = (\Psi(t+\delta; x, t, q), t+\delta)]\big) \wedge \big(\forall 0 \leq h \leq \delta,\ \phi_1[(x,t) = (\Psi(t+h; x, t, q), t+h)]\big)\Big) \tag{2}$$

for any $q \in Q$ and any $i \in \mathbb{N}$.

- For a Switched System with constant dynamics, X_q^i can be explicitly calculated in polynomial time
- For a Switched System with general dynamics, the explicit calculation of X_q^i is undecidable; however, it can be inner-approximated.

Theoretical Guarantee

- This method is sound :

$$\Phi = (Q, F, \texttt{Init}, \pi) \models \varphi$$

Theoretical Guarantee

- This method is sound :

$$\Phi = (Q, F, \texttt{Init}, \pi) \models \varphi$$

- This method is relatively complete for constant dynamics system :

  For any $x \in \mathbb{R}^n$, if x can be driven to satisfy φ with some controller π, then there exists $k \in \mathbb{N}$, such that the initial set of the synthesized switched system contains x.

Theoretical Guarantee

- This method is sound :

$$\Phi = (Q, F, \texttt{Init}, \pi) \models \varphi$$

- This method is relatively complete for constant dynamics system :

  For any $x \in \mathbb{R}^n$, if x can be driven to satisfy φ with some controller π, then there exists $k \in \mathbb{N}$, such that the initial set of the synthesized switched system contains x.

- The controller synthesized features minimal switching property for constant dynamics :

  For any $x_0 \in \texttt{Init}$, there does not exists any controller π', that can drive x_0 to satisfy φ with switching time less than $\pi(x_0)$.

Experimental Results

Table 1: ST-RA Specifications

Model	ST-RA Formulas
Reactor [55]	φ : $(10 \le tempe \le 90) \wedge (0 \le cooling \le 1)\, \mathcal{U}_{[15,20]}\, (40 \le tempe \le 50)$
WaterTank [33]	φ_1 : $(10 \le lev_0 \le 95) \wedge (10 \le lev_1 \le 95) \wedge (\lvert lev_0 - lev_1 \rvert \le 10)\, \mathcal{U}_{[50,60]}\, (50 \le lev_0 \le 80) \wedge (50 \le lev_1 \le 80)$
	φ_2 : $(10 \le lev_0 \le 95) \wedge (10 \le lev_1 \le 95) \wedge (\lvert lev_0 - lev_1 \rvert \le 10)\, \mathcal{U}_{[30,40]}\, (50 \le lev_0 \le 80) \wedge (50 \le lev_1 \le 80)$
	φ_3 : $(10 \le lev_0 \le 95) \wedge (10 \le lev_1 \le 95)\, \mathcal{U}_{[30,40]}\, (50 \le lev_0 \le 80) \wedge (50 \le lev_1 \le 80)$
CarSeq [5]	φ_1 : $(1 \le pos_0 - pos_1 \le 3)\, \mathcal{U}_{[2,3]}\, (20 \le pos_0 \le 25)$
	φ_2 : $(1 \le pos_0 - pos_1 \le 3) \wedge (1 \le pos_1 - pos_2)\, \mathcal{U}_{[2,3]}\, (20 \le pos_0 \le 25)$
	φ_3 : $(1 \le pos_0 - pos_1 \le 3) \wedge (1 \le pos_1 - pos_2 \le 3) \wedge (1 \le pos_2 - pos_3)\, \mathcal{U}_{[2,3]}\, (20 \le pos_0 \le 25)$
Oscillator [52]	φ : $(x^2 + y^2 \le 1)\, \mathcal{U}_{[3,4]}\, (x^2 + y^2 \le 0.01)$
Temperature [5]	φ_1 : $\wedge_{i=1,2,3} (23 \le temp_i \le 29)\, \mathcal{U}_{[8,10]} \wedge_{i=1,2,3} (26 \le temp_i \le 28)$
	φ_2 : $\wedge_{i=1,2,3} (23 \le temp_i \le 29)\, \mathcal{U}_{[8,10]} \wedge_{i=1,2,3} (26 \le temp_i \le 28) \wedge (temp_2 \le temp_1)$
	φ_3 : $\wedge_{i=1,2,3} (23 \le temp_i \le 29)\, \mathcal{U}_{[8,10]} \wedge_{i=1,2,3} (26 \le temp_i \le 28) \wedge (temp_2 \le temp_1) \wedge (temp_3 \le temp_2)$

Experimental Results

Table 2: Empirical results on benchmark examples

Model	Dynamics	ST-RA	Model Scale		Synthesis Time	
			n_{dim}	n_{mode}	#Iter.	Time (s)
Reactor [55]	Const	φ	2	4	6 (fp)	0.31
		φ	2	8	6 (fp)	4.14
		φ	2	10	6 (fp)	8.01
WaterTank [33]	Const	φ_1	2	7	9 (fp)	18.04
		φ_2	2	7	6 (fp)	10.63
		φ_3	2	7	6 (fp)	5.24
CarSeq [5]	Const	φ_1	2	4	5 (fp)	1.12
		φ_2	3	8	7 (fp)	47.41
		φ_3	4	16	4	134.79
Oscillator [52]	Poly	φ	2	3	6	77.20
		φ	2	4	6	106.09
		φ	2	5	6	155.77
Temperature [5]	Linear	φ_1	3	8	5	236.99
		φ_2	3	8	5	293.66
		φ_3	3	8	5	252.32

Dynamics: the type of continuous dynamics; ST-RA: formulas to be satisfied (cf. Table 1); n_{dim}: dimension of state; n_{mode}: number of modes; #Iter.: number of iterations, (fp) means the synthesized set X_q^i (cf. Sect. 5) reach a fixpoint at current iteration.

- For constant dynamics system :

  Efficiency $\propto$ n_{dim}, n_{mode}, and complexity of ST-RA formulas,
- For non-constant dynamics system :

  Efficiency $\propto$ n_{dim} and n_{mode},
  Efficiency $\not\propto$ complexity of ST-RA formulas

Summary

- **Contribution** :
  - This work presents for the first time a method for generating hybrid system switching controllers under STL constraints and implements a prototype.
  - The proposed algorithm in this work is theoretically guaranteed to be sound, relatively complete, and minimally switching.

⇒ Su, Feng, S. Zhan, N. Zhan : *Switching Controller Synthesis for Hybrid Systems Against STL Formulas*. FM '24.

Summary

- **Contribution** :
  - This work presents for the first time a method for generating hybrid system switching controllers under STL constraints and implements a prototype.
  - The proposed algorithm in this work is theoretically guaranteed to be sound, relatively complete, and minimally switching.
- **Future Work** :
  - Enlarge the range of STL specification under consideration : nested STL formulas
  - Generalize the hybrid system under consideration : stochastic, delay

⇒ Su, Feng, S. Zhan, N. Zhan : *Switching Controller Synthesis for Hybrid Systems Against STL Formulas*. FM'24.