A contract negotiation scheme for safety verification of interconnected systems

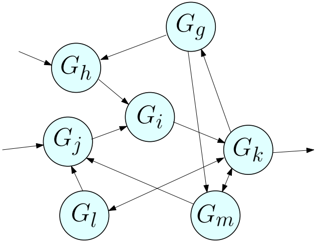
Xiao Tan[a], Antonis Papachristodoulou[b], Dimos V. Dimarogonas[a]

[a] School of EECS, KTH Royal Institute of Technology, Sweden
[b] Department of Engineering Science, University of Oxford, United Kingdom

27th June 2024

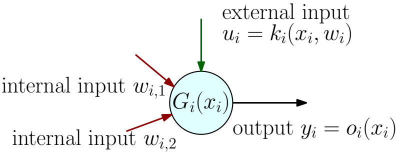
EUROPEAN CONTROL CONFERENCE

Safety verification for interconnected systems

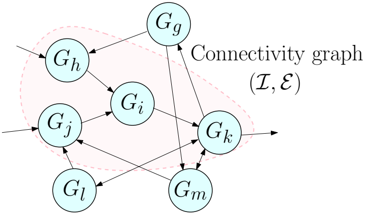


- Engineering systems are becoming more complex, closely interconnected in dynamics and safety requirements;
- Before deployment of new control schemes, verifying safety of the closed-loop interconnected systems is vital;
- Simulation/experiments/tests require extensive resources with possible existence of corner cases;
- Yet, most existing safety verification algorithms are restricted to small-size problems.

Safety of interconnected systems



Subsystem $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$

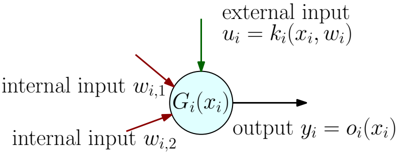


interconnected system $G = \langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$

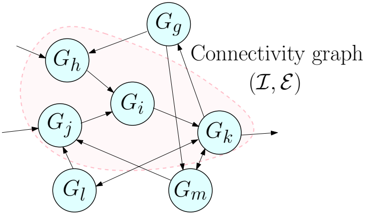
Continuous-time system: $G = (U, W, X, Y, X^0, \mathcal{T})$

$$\mathcal{T} : \quad \dot{x}(t) = f(x, w) + g(x, w)u, \quad o : x \mapsto y \tag{1}$$

Safety of interconnected systems



Subsystem $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$



interconnected system $G = \langle (G_i)_{i\in\mathcal{I}}, \mathcal{E} \rangle$

Continuous-time system: $G = (U, W, X, Y, X^0, \mathcal{T})$

$$\mathcal{T}: \quad \dot{x}(t) = f(x, w) + g(x, w)u, \quad o : x \mapsto y \tag{1}$$

Denote by I_B the set of signals that only take values in the set B.

Safety: given safe region $\mathcal{Q} \subseteq X$, G is *safe w.r.t.* $\underline{W} \subseteq W$ if

$$\exists u|_{[0,t]} \in I_U \text{ s.t. } x|_{[0,t]} \in I_{\mathcal{Q}} \text{ for all } t > 0$$

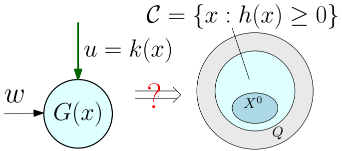
for all initial states $x_0 \in X^0$ and all internal input signals $w|_{[0,t]} \in I_{\underline{W}}$.

Existing works on safety verification

The existence of a safety certificate $\implies$ system safety is verified.

Incomplete list of existing methods for small-size systems

1. sum-of-squares approaches[1,2]
2. data-driven/learning-based approaches[3,4]
3. Hamiltonian-Jacobi reachability analysis[5]



[1] A. Clark, "Verification and synthesis of control barrier functions," in 2021 60th IEEE Conference on Decision and Control (CDC), 2021, pp. 6105–6112.

[2] H. Wang, K. Margellos, and A. Papachristodoulou, "Safety verification and controller synthesis for systems with input constraints," IFAC-PapersOnLine, vol. 56, no. 2, pp. 1698–1703, 2023.

[3] A. Robey, H. Hu, L. Lindemann, H. Zhang, D. V. Dimarogonas, S. Tu, and N. Matni, "Learning control barrier functions from expert demonstrations," in 2020 59th IEEE Conference on Decision and Control (CDC), IEEE, 2020, pp. 3717–3724.

[4] A. Abate, D. Ahmed, A. Edwards, M. Giacobbe, and A. Peruffo, "FOSSIL: A software tool for the formal synthesis of Lyapunov functions and barrier certificates using neural networks," in Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control, 2021, pp. 1–11.

[5] J. J. Choi, D. Lee, K. Sreenath, C. J. Tomlin, and S. L. Herbert, "Robust control barrier–value functions for safety-critical control," in 2021 60th IEEE Conference on Decision and Control (CDC), IEEE, 2021, pp. 6814–6821.

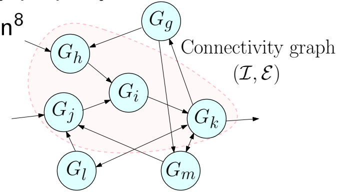
Existing works on safety verification

The existence of a safety certificate $\implies$ system safety is verified.

Methods for large-size systems: compositional reasoning.

1. small-gain-like conditions on local ISSafety property[6,7]
2. centralized Lyapunov function construction[8]

However, adaptation on local safety property usually requires a central computation node.



interconnected system $G = \langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$

---

[6] P. Jagtap, A. Swikir, and M. Zamani, "Compositional construction of control barrier functions for interconnected control systems," in Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control, 2020, pp. 1–11.

[7] Z. Lyu, X. Xu, and Y. Hong, "Small-gain theorem for safety verification of interconnected systems," Automatica, vol. 139, p. 110 178, 2022.

[8] S. Coogan and M. Arcak, "A dissipativity approach to safety verification for interconnected systems," IEEE Transactions on Automatic Control, vol. 60, no. 6, pp. 1722–1727, 2014.

Problem and proposed solution

Problems

Given interconnected system $\langle (G_i)_{i\in\mathcal{I}}, \mathcal{E}\rangle, G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$, control laws $k_i(x_i, w_i)$, and safe region $\Pi_{i\in\mathcal{I}}\mathcal{Q}_i$.

Determine if the closed-loop system is safe.

Problem and proposed solution

Problems

Given interconnected system $\langle (G_i)_{i\in\mathcal{I}}, \mathcal{E}\rangle, G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$, control laws $k_i(x_i, w_i)$, and safe region $\Pi_{i\in\mathcal{I}}\mathcal{Q}_i$.

Determine if the closed-loop system is safe.

Design a computationally tractable approach that locally constructs and adapts safety properties for compositional reasoning

Problem and proposed solution

Problems

Given interconnected system $\langle (G_i)_{i\in\mathcal{I}}, \mathcal{E}\rangle, G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$, control laws $k_i(x_i, w_i)$, and safe region $\Pi_{i\in\mathcal{I}}\mathcal{Q}_i$.

Determine if the closed-loop system is safe.

Design a computationally tractable approach that locally constructs and adapts safety properties for compositional reasoning

Proposed solution:

Sum-of-squares (SOS) for constructing local barrier certificates

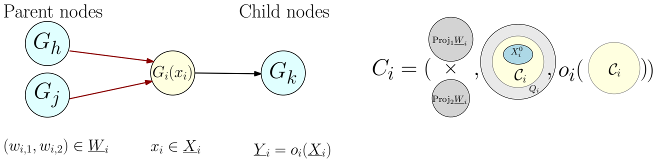
$+$

Assume-guarantee contracts (AGC) for compositional reasoning.

$+$

Contract negotiation scheme with completeness guarantee

Overall verification scheme

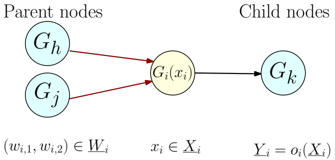


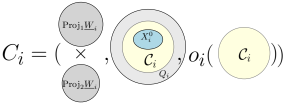
1. For subsystem G_i and its safe region $\mathcal{Q}_i$
   - SOS approach constructs an assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$, meaning

$$\text{Assume } w_i(\cdot) \in I_{\underline{W}_i}, \text{ then it guarantees } x_i(\cdot) \in I_{\underline{X}_i}$$

[9] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," Automatica, vol. 134, p. 109 910, 1.

Overall verification scheme





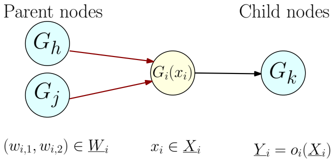
1. For subsystem G_i and its safe region $\mathcal{Q}_i$
   - SOS approach constructs an assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$, meaning

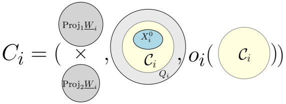
     Assume $w_i(\cdot) \in I_{\underline{W}_i}$, then it guarantees $x_i(\cdot) \in I_{\underline{X}_i}$

   - local safety condition $\underline{X}_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i$

[9] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," Automatica, vol. 134, p. 109 910, 1.

Overall verification scheme





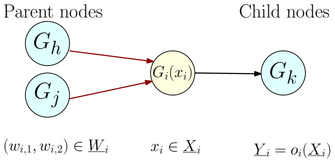
1. For subsystem G_i and its safe region $\mathcal{Q}_i$
   - SOS approach constructs an assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$, meaning

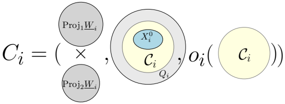
     Assume $w_i(\cdot) \in I_{\underline{W}_i}$, then it guarantees $x_i(\cdot) \in I_{\underline{X}_i}$

   - local safety condition $\underline{X}_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i$
2. safety property composition $(I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$

[9] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," Automatica, vol. 134, p. 109 910, 1.

Overall verification scheme





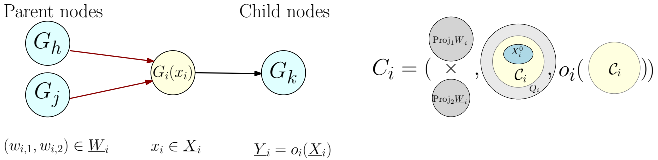
1. For subsystem G_i and its safe region $\mathcal{Q}_i$
   - SOS approach constructs an assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$, meaning

     Assume $w_i(\cdot) \in I_{\underline{W}_i}$, then it guarantees $x_i(\cdot) \in I_{\underline{X}_i}$

   - local safety condition $\underline{X}_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i$
2. safety property composition $(I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$
   - composition condition

[9] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," Automatica, vol. 134, p. 109 910, 1.

Overall verification scheme



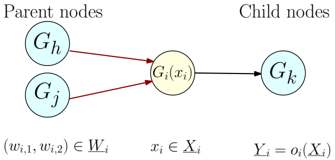
1. For subsystem G_i and its safe region $\mathcal{Q}_i$
   - SOS approach constructs an assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$, meaning

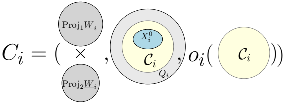
     Assume $w_i(\cdot) \in I_{\underline{W}_i}$, then it guarantees $x_i(\cdot) \in I_{\underline{X}_i}$

   - local safety condition $\underline{X}_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i$
2. safety property composition $(I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$
   - composition condition
   - circular reasoning issue: mild regularity condition required by assume-guarantee contracts[9]

[9] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," Automatica, vol. 134, p. 109 910, 1.

Overall verification scheme





1. For subsystem G_i and its safe region $\mathcal{Q}_i$
   - SOS approach constructs an assume-guarantee contract $C_i = (I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i})$, meaning

     Assume $w_i(\cdot) \in I_{\underline{W}_i}$, then it guarantees $x_i(\cdot) \in I_{\underline{X}_i}$

   - local safety condition $\underline{X}_i^0 \subseteq \underline{X}_i \subseteq \mathcal{Q}_i$
2. safety property composition $(I_{\underline{W}_i}, I_{\underline{X}_i}, I_{\underline{Y}_i}), i \in \mathcal{I}$
   - composition condition
   - circular reasoning issue: mild regularity condition required by assume-guarantee contracts[9]
3. How to locally adapt AGCs if composition condition is not met?

[9] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," Automatica, vol. 134, p. 109 910, 1.

Assumptions

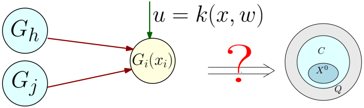
We assume the following:

1. The local feedback law $u_i = k_i(x_i, w_i) \in U_i$ is known. Denote the closed-loop dynamics $\dot{x}_i = F_i(x_i, w_i)$;
2. The class $\mathcal{K}$ function $\alpha(\cdot)$ in CBF conditions is chosen to be a linear function with constant gain a.
3. The initial set X_i^0, safe region $\mathcal{Q}_i$, and the internal input set W_i are super-level sets, i.e., $X_i^0 = \{x_i : b_i^0(x_i) \geq 0\}, \mathcal{Q}_i = \{x_i : q_i(x_i) \geq 0\}, W_i = \{(y_{j_1}, y_{j_2}, \ldots, y_{j_p}) : d_{j_k}^i(y_{j_k}) \geq 0, k = 1, 2, \ldots, p\}$, where $N(i) = \{j_1, j_2, \ldots, j_p\}$.
4. All the functions $b_i^0, q_i, d_{j_k}^i(y_{j_k}), f_i, g_i, k_i$ are polynomials.
5. The subsets of $W_i, \mathcal{Q}_i$, i.e., $\underline{W}_i, \underline{\mathcal{Q}}_i$ are chosen in the form of

$$\underline{\mathcal{Q}}_i = \{x_i : q_i(x_i) \geq \zeta \mathbf{1} \text{ for some } \zeta \geq 0\},$$
$$\underline{W}_i = \{(y_{j_1}, \ldots, y_{j_p}) : d_{j_k}^i(y_{j_k}) \geq \delta \mathbf{1} \text{ for some } \delta \geq 0\}.$$

6. We restrict the search for non-negative polynomials to the set of SOS polynomials up to a certain degree.

Local AGC construction



$\underline{W} = \{(..., y_{j_k}, ...) : d_{j_k}(y_{j_k}) \geq \delta\}$

$\mathcal{C} = \{x : h(x) \geq 0\}$
$X^0 = \{x : b^0(x) \geq 0\}$
$\mathcal{Q} = \{x : q(x) \geq 0\}$

If there exist SOS polynomials $\sigma_{init}, \sigma_{safe} \in \Sigma[x]$, $\sigma_k \in \Sigma[x, y_k]$, $k = 1, 2, \ldots, p$, polynomial $h \in \mathcal{R}(x)$, and positive ϵ, a, δ such that

initial set: $$h(x) - \sigma_{init} b^0(x) \in \Sigma[x]; \tag{2a}$$

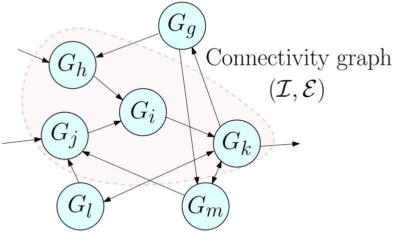
safe region: $$-h(x) + \sigma_{safe} q(x) \in \Sigma[x]; \tag{2b}$$

BF condition: $$\nabla h(x) F(x, y_1, \ldots, y_p) + a h(x) - \sum_{k=1}^{p} \sigma_k (d_k(y_k) - \delta) - \epsilon \in \Sigma[x, y_1, \ldots, y_p]. \tag{2c}$$

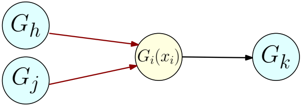
then, letting $\underline{W} = \{(y_1, \ldots, y_k \ldots, y_p) : d_k(y_k) \geq \delta\}$, we find an assume-guarantee contract $C = (I_{\underline{W}}, I_{\underline{X}}, I_{\underline{Y}})$

*Subscript i is neglected for notational brevity.

AGC composition and negotiations



interconnected system $G = \langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$

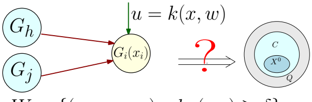


Composition condition $\underline{Y}_h \times \underline{Y}_j \subseteq \underline{W}_i$

Composition condition: $\Pi_{j \in N(i)} \underline{Y}_j \subseteq \underline{W}_i, \forall i \in \mathcal{I}$

1. We refer to the process of refining local AGCs as negotiations.
2. Negotiations under two special cases are discussed.

Two special sets when constructing local AGCs



$\mathcal{C} = \{x : h(x) \geq 0\}$
$X^0 = \{x : b^0(x) \geq 0\}$
$\mathcal{Q} = \{x : q(x) \geq 0\}$

$\underline{W} = \{(..., y_{j_k}, ...) : d_{j_k}(y_{j_k}) \geq \delta\}$

- Intuitively, the larger $\underline{W}_i$ is, the smaller $\underline{X}_i$ could be.
- Maximal internal input set $\underline{W}^\star$: largest disturbance a subsystem can tolerate while still remaining safe

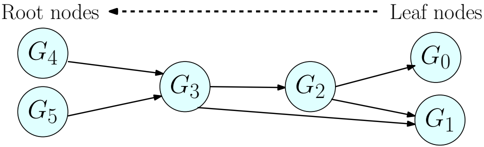
$$\begin{aligned} &\min \delta \\ &\text{s.t. } (2a), (2b), (2c), \delta \geq 0 \end{aligned} \tag{3}$$

- Minimal safe region $\underline{\mathcal{Q}}^\star$ under the maximal internal input set: smallest impact a subsystem to its child nodes

$$\begin{aligned} &\max \zeta \\ &\text{s.t. } (2a), (2c), \zeta \geq 0 \\ &\quad -h(x) + \sigma_{safe}(q(x) - \zeta) \in \Sigma[x] \end{aligned} \tag{4}$$

*Subscript i is neglected for notational brevity.

Special case: Acyclic connectivity graph



When the connectivity graph is a tree, the hierarchical structure resembles a client-contractor relation model.

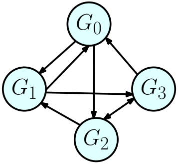
Algorithm 1

1. Start with the leaf nodes. Calculate the maximal internal input sets;
2. For node i, if all child nodes have specified the largest internal input set, then compute its maximal internal input set.
3. Propagate towards root nodes. Return `False` if infeasible.

- Algorithm 1 terminates in finite steps and returns either `True` or `False`.
- If Algorithm 1 returns `True`, then compatible local AGCs are found .
- If Algorithm 1 returns `False`, then there exist no compatible iAGCs under our Assumption.

Special case: Homogeneous interconnected system

homogeneous interconnected system $G = \langle (G_i)_{i \in \mathcal{I}}, \mathcal{E} \rangle$



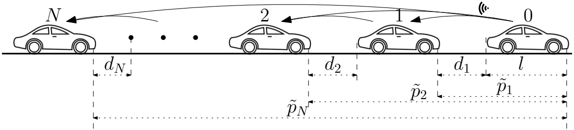
$G_i = G_j, Q_i = Q_j, \forall i, j \in \mathcal{I}$

Algorithm 2

1. Take an arbitrary node G_i, calculate the AGC $C_i = (I_{\underline{W}_i^\star}, I_{\underline{X}_i^\star}, I_{\underline{Y}_i^\star})$ with $\underline{W}_i^\star$ the maximal internal input sets and $\underline{X}_i^\star$ the corresp. minimal safe region;
2. If not compatible, update $\mathcal{Q}_i$ to be the largest inner-approximation of $\bigcap_{k \in \mathsf{Child}(i)} o_i^{-1}(\mathsf{Proj}_i(\underline{W}_k)) \cap \mathcal{Q}_i$
3. Goto Step 1. Return `False` if infeasible.

- Algorithm 2 terminates eventually and returns either `True` or `False`.
- If Algorithm 2 returns `True`, then compatible local AGCs are found.
- If Algorithm 2 returns `False`, then there exist no common and compatible AGCs under our Assumption.

Vehicular platooning: an acyclic graph example



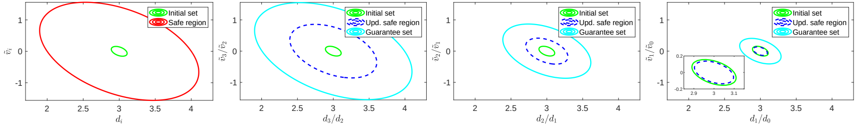
Vehicle dynamics relative to vehicle 0 (leader):

$$\dot{\tilde{p}}_i = \tilde{v}_i, \qquad \dot{\tilde{v}}_i = \tilde{u}_i - (\tilde{v}_i - \tilde{v}_{i-1})^3 \tag{5}$$

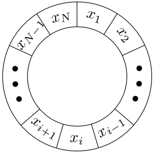
Choose local variable $x_i = (d_i, \tilde{v}_i)$, $d_i = \tilde{p}_i - \tilde{p}_{i-1} - l$. Local controller

$$\tilde{u}_i = -(\tilde{v}_i - \tilde{v}_{i-1}) - (d_i - 3) - (d_i - 3)^3, i \in \mathcal{I}.$$

The initial state set, safe region as well as local AGCs are:



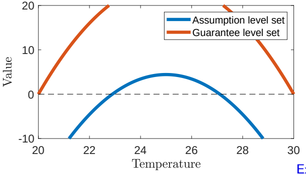
(a) X_i^0 and Q_i, $i = 1, 2, 3$. (b) AGC sets for vehicle 3. (c) AGC sets for vehicle 2. (d) AGC sets for vehicle 1.

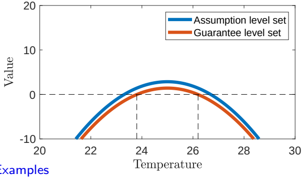


Room temperature model and its controller over a circular building

$$
\begin{aligned}
\dot{x}_i(t) &= \alpha(x_{i+1} + x_{i-1} - 2x_i) + \beta(t_e - x_i) + \gamma(t_h - x_i)u_i, \\
y_i(t) &= x_i, \\
u_i &= 0.05(x_{i+1} + x_{i-1} - 2x_i) + 0.05(25 - x_i)
\end{aligned}
$$

Each subsystem $G_i = (U_i, W_i, X_i, Y_i, X_i^0, \mathcal{T}_i)$ has x_i as the state, (x_{i-1}, x_{i+1}) as the internal input, u_i as the external input, $o_i(x_i) = x_i$,
$U_i, X_i, Y_i = \mathbb{R}, W_i = \mathbb{R}^2$.
$X_i^0 = \{x_i : 1 - (x_i - 25)^2 \geq 0\}$, and $\mathcal{Q}_i = \{x_i : 5^2 - (x_i - 25)^2 \geq 0\}$.





Summary

1. In this work, we proposed an SOS and AGC framework for safety verification of interconnected systems;
2. Proposed contract negotiation algorithms are shown to be complete for acyclic graphs or homogeneous systems;
3. Future work includes extension to general graphs with completeness guarantees as well as better implementation.

Any questions? Contact us!

erc
Swedish Research Council
WASP WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM