Software science applied to manufacturing

Automatic Design of Reliable Systems by Cooperation of Numerical Optimization and Logic

Research Center for Mathematical Trust in Software and Systems & HASUO Laboratory

Our research

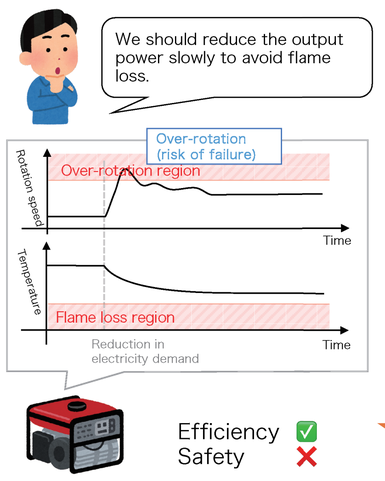
- We achieved **automatic & efficient discovery** of reliable gas turbine system designs
- **Without mathematical re-modeling** of the system, our method directly uses a realistic (**black-box**) simulators as a model
- The key enabler is the **logical structure** of requirement specifications

Advantage

- Design process is automated and the result is **comarable to a manual tuning by human expertise**, in our case study
- The method is generally applicable to black-box control systems. Expected to be useful in **various fields of system design** such as autonomous driving

Background & Goals

Background: Quality assurance of black-box system



Finding an input such that the corresponding output satisfies all of requirements

Mandatory 1	:	Both of $H_1 \geq \theta_4^1$ and $H_2 \geq \theta_3^2$ must be true at certain stage.
Mandatory 2	:	The value of G must not reach Region 4, i.e., must keep $G \leq \Theta^g$.
Desirable 1	:	(H_1, H_2) should not reach Region 2.
Desirable 2	:	H_2 should not reach Region 1, i.e., should keep $H_2 \leq \theta_4^2$.
Desirable 3	:	F should not reach Region 3, i.e., should keep $F \leq \Theta^f$.

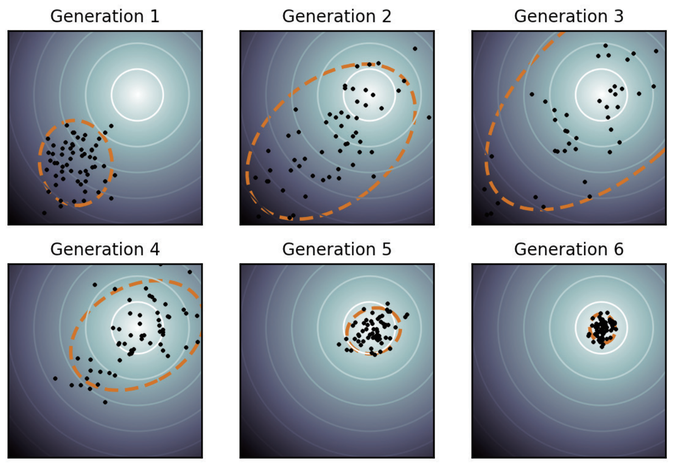
Translation to STL formula

$$
\begin{aligned}
\varphi_1^{\text{Mand}} &: \Diamond_{[0,60]}(H_1 \geq \theta_4^1 \wedge H_2 \geq \theta_3^2) \\
\varphi_2^{\text{Mand}} &: \Box_{[0,60]}\,(G \leq \Theta^g) \\
\varphi_1^{\text{Desir}} &: \Box_{[0,60]}\,\neg(H_1 > \theta_1^1 \wedge H_2 < \theta_3^2 \wedge H_2 > \theta_1^2 \wedge H_2 > \alpha_1 H_1 + \beta_1 \wedge H_2 > \alpha_2 H_1 + \beta_2) \\
\varphi_2^{\text{Desir}} &: \Box_{[0,60]}\,(H_2 \leq \theta_4^2) \\
\varphi_3^{\text{Desir}} &: \Box_{[0,60]}\,(F \leq \theta^f) \\
&\text{where} \quad \alpha_1 = \frac{\theta_3^2 - \theta_2^2}{\theta_4^1 - \theta_3^1}, \alpha_2 = \frac{\theta_2^2 - \theta_1^2}{\theta_3^1 - \theta_2^1}, \beta_1 = -\alpha_1 \theta_3^1 + \theta_2^2, \beta_2 = -\alpha_2 \theta_2^1 + \theta_1^2
\end{aligned}
$$

Only the correspondence of output and input values provided

often there apeears trade-off, so careful balancing is required

Goals: Exploiting domain knowledge to effectively find a desirable design



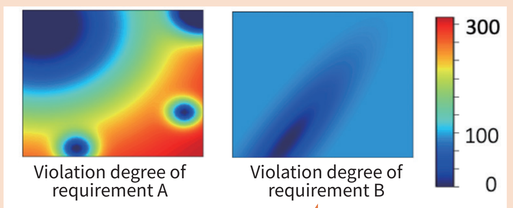
By quantifying how “nearly satisfying” the output is, system design is translated into numerical optimization.

To solve it in realistic time frame, we need to adress:
1) Broad search space (30 dim)
2) Stuck in local optimum or plateau

Method

Multiple constraint technique

- We treat some of violation degrees as “contraint functions”
- Each violation degree is seperately evaluated in scale-invariant way



Specification $\varphi^{\text{AT}} :\equiv \varphi_1^{AT} \wedge \varphi_2^{AT} \wedge \varphi_3^{AT}$

Robustness for each conjuncts

		φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}
Individual	u_1	1400	59.9	-3
	u_2	-9	2	1
	u_3	-180	2	-1

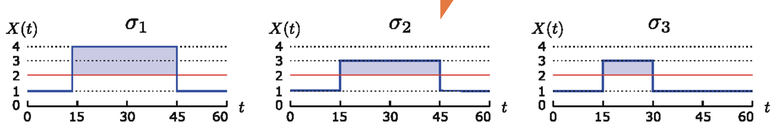
$$
F_x(u) := \begin{cases} \text{RVNum}_x(u) + \sum_{j=2}^{m} \text{RCon}_x^j(u) & \text{(if no feasible solution)} \\ \text{RObj}_x(u) + \text{RVNum}_x(u) + \sum_{j=2}^{m} \text{RCon}_x^j(u) & \text{(otherwise)} \end{cases}
$$

	RObj_x / robustness of φ_1^{AT}	RCon_x^2 / violation deg. of φ_2^{AT}	RCon_x^3 / violation deg. of φ_3^{AT}	RVNum_x / # of violated constraints	F_x
u_1	**1st** / 1400	**1st** / 0	**3rd** / -3	**2nd** / 1	7 (= 1 + 1 + 3 + 2)
u_2	**2nd** / -9	**1st** / 0	**1st** / 0	**1st** / 0	5 (= 2 + 1 + 1 + 1)
u_3	**3rd** / -180	**1st** / 0	**2nd** / -1	**2nd** / 1	8 (= 3 + 1 + 2 + 1)

Merging two violation degree into one objective function may result a masking of small-scale one

Area modality

Requirement: the signal value should not be above 2



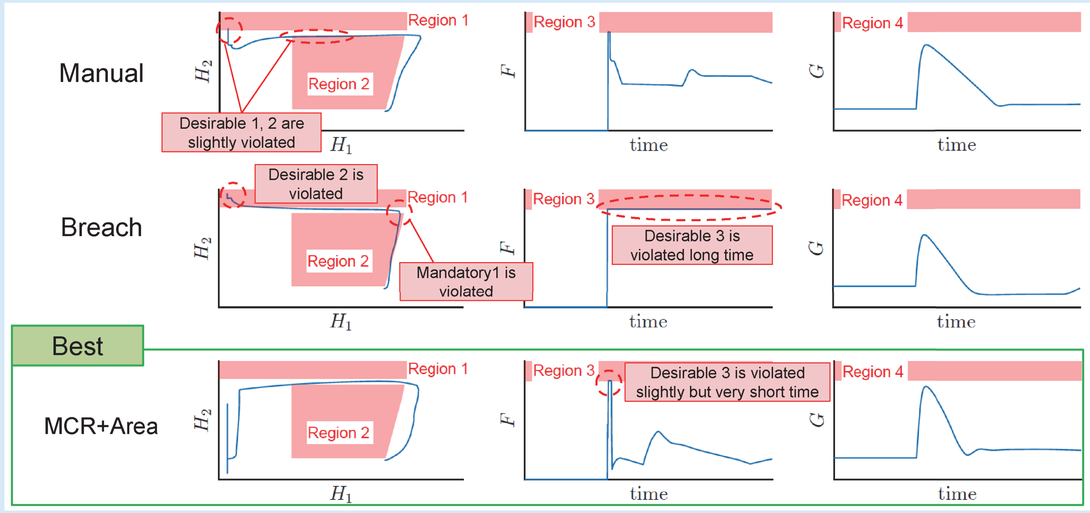
- Counterintuitively, these signals are equally valued in conventional framework of STL formula evaluation
- We introduced new modality into STL system to reflect the time-and-value violation degree

$$
\begin{aligned}
\varphi_1^{\text{Mand}} &: \Diamond_{[0,60]}(H_1 \geq \theta_4^1 \wedge H_2 \geq \theta_3^2) \\
\varphi_2^{\text{Mand}} &: \Box_{[0,60]}\,(G \leq \Theta^g) \\
(\varphi_1^{\text{Desir}})^{\text{Area}} &: \neg\text{Area}_{[0,60]}(H_1 > \theta_1^1 \wedge H_2 < \theta_3^2 \wedge H_2 > \theta_1^2 \wedge H_2 > \alpha_1 H_1 + \beta_1 \wedge H_2 > \alpha_2 H_1 + \beta_2) \\
(\varphi_2^{\text{Desir}})^{\text{Area}} &: \neg\text{Area}_{[0,60]}\left(\neg(H_2 \leq \theta_4^2)\right) \\
(\varphi_3^{\text{Desir}})^{\text{Area}} &: \neg\text{Area}_{[0,60]}\left(\neg(F \leq \Theta^f)\right)
\end{aligned}
$$

Result

Our method automates the design process that costs 7 person-days of manual tuning

	Quality	Automation	Cost
Manual	+	no	−−(7 person-days)
Existing tool	−	yes	+(3 hours)
Our method	++	yes	+(3 hours)



The resulting behavior is comparable to the one by human expertise

連絡先： 国立情報学研究所 アーキテクチャ科学研究系 佐藤創太
URL： https://group-mmm.org/~sotasato/ Email : sotasato@nii.ac.jp