Constrained Optimization for Hybrid System Falsification and Application to Conjunctive Synthesis

Sota Sato, Masaki Waga, Ichiro Hasuo

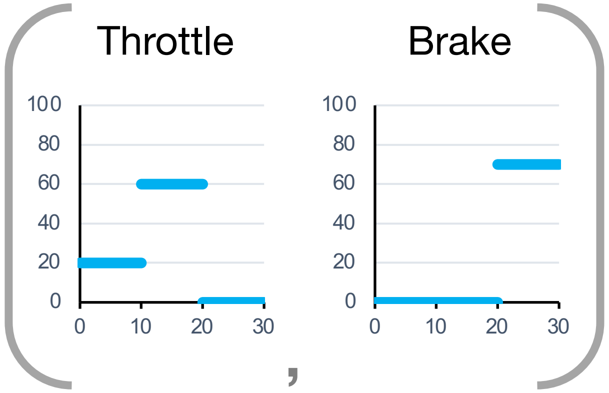
National Institute of Informatics, Tokyo, Japan

The Graduate University for Advances Studies (SOKENDAI), Hayama, Japan

Hybrid system falsification of CPS

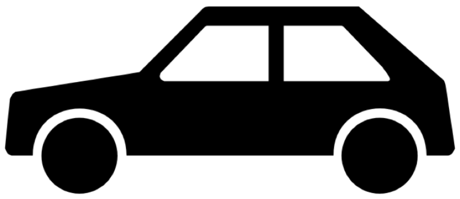
[Fainekos & Pappas, Theor. Comput. Sci. 2009]

Input u

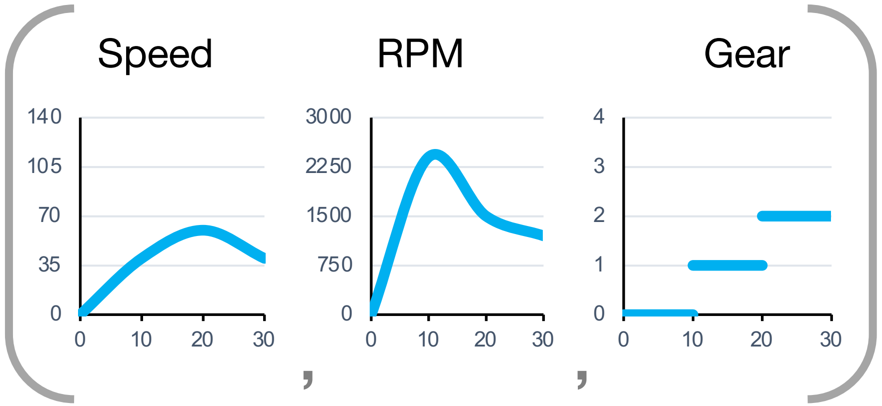


System model $\mathcal{M}$

Automatic transmission system (Simulink)



Output $\mathcal{M}(u)$



Specification φ

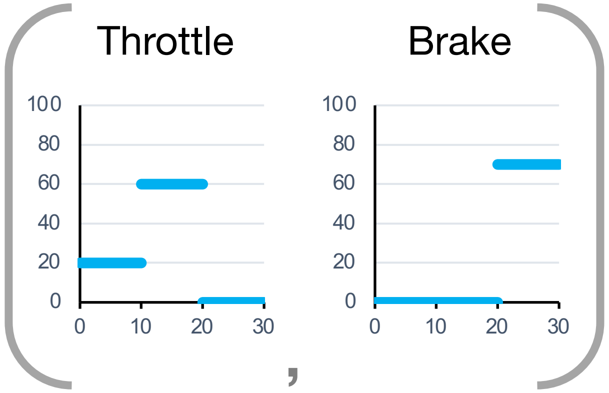
$$\varphi :\equiv \square_{[0,30]}(\text{speed} < 100)$$

Goal: to find an input signal u, s.t. $\mathcal{M}(u) \not\models \varphi$

Hybrid system falsification of CPS

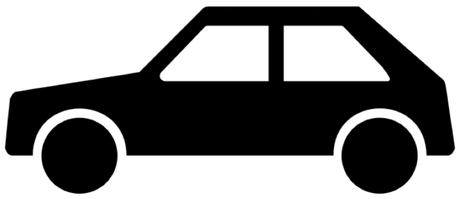
[Fainekos & Pappas, Theor. Comput. Sci. 2009]

Input u

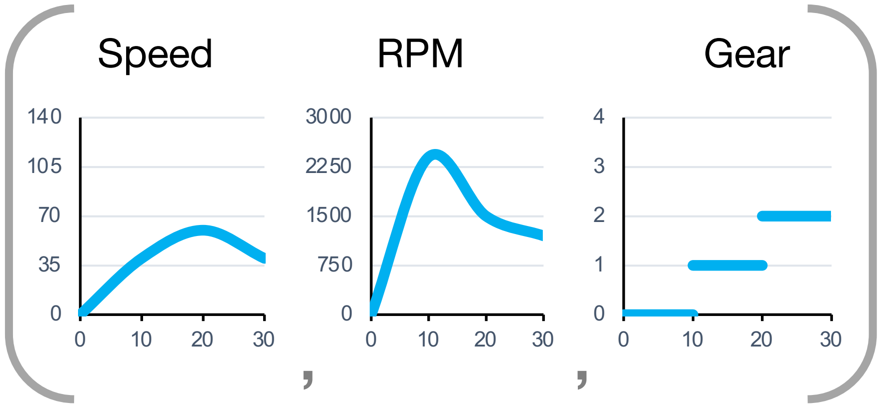


System model $\mathcal{M}$

Automatic transmission system (Simulink)



Output $\mathcal{M}(u)$



Specification φ

$$\varphi :\equiv \Box_{[0,30]}(\text{speed} < 100)$$

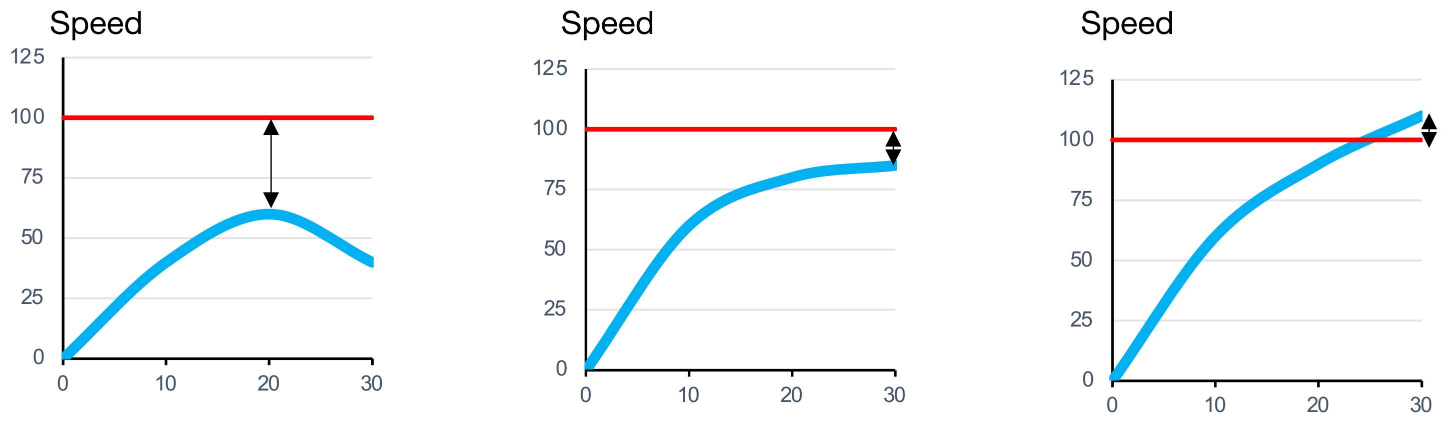
Always for $t \in [0,30]$

Speed is below 100

Goal: to find an input signal u, s.t. $\mathcal{M}(u) \not\models \varphi$

Robust semantics of STL [Donze & Maler, FORMATS'10]

Specification: $\varphi \equiv \Box_{[0,30]}(\mathrm{speed}(t) < 100)$



Violation degree	Far from violation	Almost violated	Violated
Robustness $[\![\mathcal{M}(\mathrm{u}), \varphi]\!]$	40	10	-10

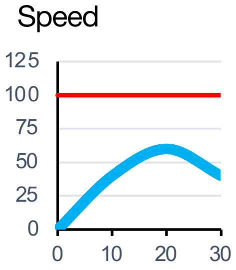
$$\mathcal{M}(u) \not\models \varphi \Leftrightarrow [\![\mathcal{M}(\mathrm{u}), \varphi]\!] < 0$$

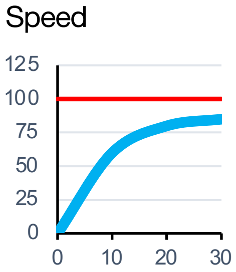
Optimization-based falsification

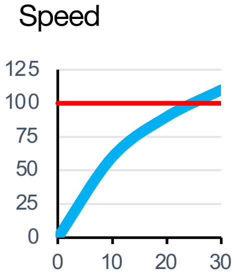
Falsification Problem is translated into:

Try minimizing $[\![\mathcal{M}(\mathrm{u}), \varphi]\!]$ and finish if $[\![\mathcal{M}(\mathrm{u}), \varphi]\!] < 0$

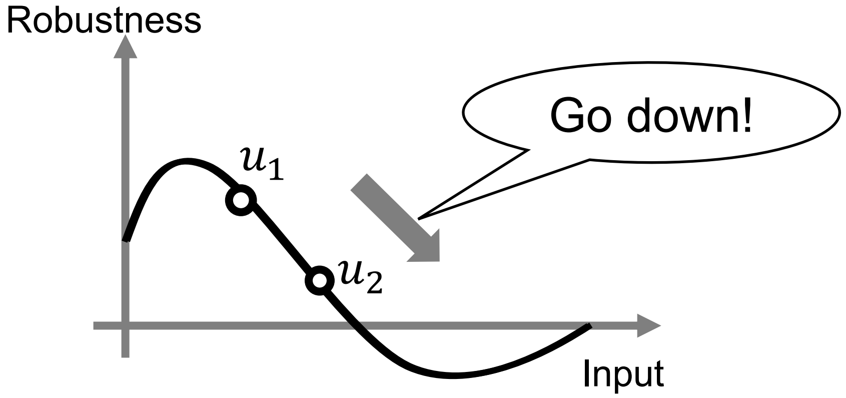
Input	u_1	Less robust →	u_2	Less robust →	u_3
Robustness $[\![\mathcal{M}(\mathrm{u}), \varphi]\!]$	40		10		**-10**







Optimized by
Hill-climbing style algorithms
(HC, SA, GNM, CMA-ES, …)



Synthesis is the dual of falsification

Falsification problem

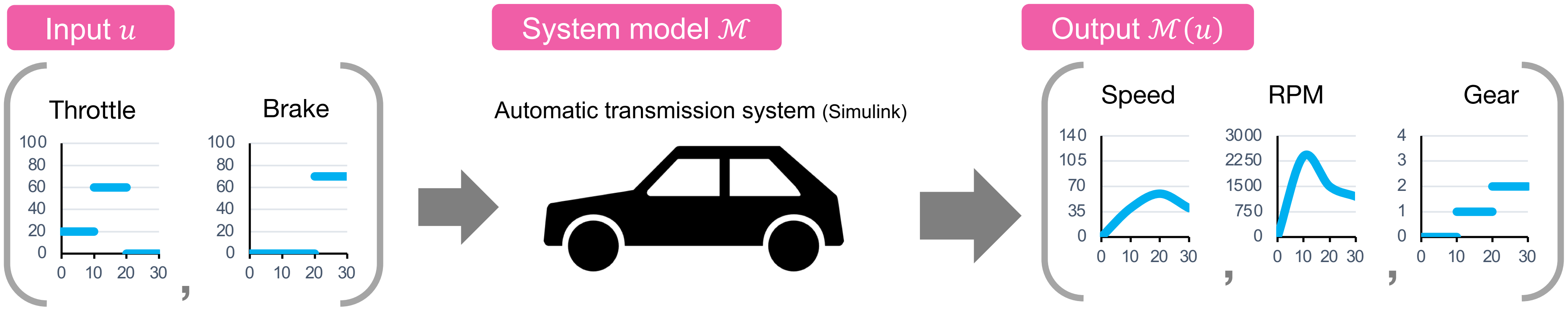
Try minimizing $[\![\mathcal{M}(\mathrm{u}), \neg\varphi]\!]$ **and finish if** $[\![\mathcal{M}(\mathrm{u}), \neg\varphi]\!] < 0$

$\mathcal{M}(u) \nvDash \neg\varphi \;\Leftrightarrow\; \mathcal{M}(u) \vDash \varphi$

Synthesis problem

Try maximizing $[\![\mathcal{M}(\mathrm{u}), \varphi]\!]$ **and finish if** $[\![\mathcal{M}(\mathrm{u}), \varphi]\!] > 0$

Conjunctive synthesis



Specification φ

and

$$\varphi :\equiv \varphi_1 \land \cdots \land \varphi_m$$

Goal: to find an input signal u, s.t. $\mathcal{M}(u) \vDash \varphi_1 \land \cdots \land \varphi_m$

$(\Leftrightarrow \mathcal{M}(u) \vDash \varphi_1, \ \ldots, \mathcal{M}(u) \vDash \varphi_m)$

S. Sato <sotasato@nii.ac.jp>

Example of Conjunctive synthesis

Conjunctive specification $\varphi^{\mathrm{AT}} :\equiv \varphi_1^{AT} \land \varphi_2^{AT} \land \varphi_3^{AT}$

$\varphi_1^{AT} :\equiv \Box_{[0,30]}(\mathrm{rpm} \leq 2400)$, $\varphi_2^{AT} :\equiv \Box_{[0,30]}(\mathrm{speed} \leq 60)$, $\varphi_3^{AT} :\equiv \Diamond_{[0,30]}(\mathrm{gear} \geq 3)$

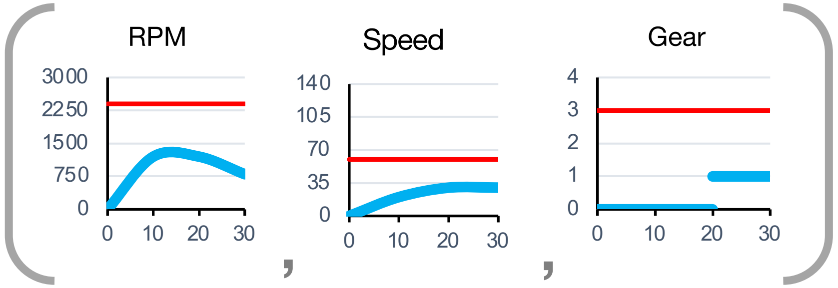
Eventually reach $\mathrm{gear} \geq 3$

Example of Conjunctive synthesis

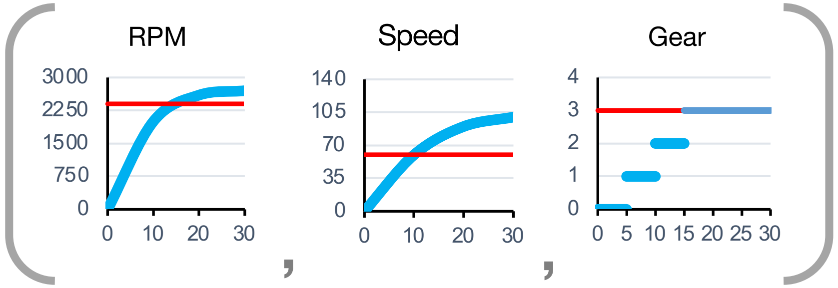
Conjunctive specification $\varphi^{\mathrm{AT}} :\equiv \varphi_1^{AT} \wedge \varphi_2^{AT} \wedge \varphi_3^{AT}$

$\varphi_1^{AT} :\equiv \Box_{[0,30]}(\mathrm{rpm} \leq 2400)$, $\varphi_2^{AT} :\equiv \Box_{[0,30]}(\mathrm{speed} \leq 60)$, $\varphi_3^{AT} :\equiv \Diamond_{[0,30]}(\mathrm{gear} \geq 3)$

Eventually reach $\mathrm{gear} \geq 3$



φ_1^{AT} : Satisfied φ_2^{AT} : Satisfied φ_3^{AT} : **Violated**



φ_1^{AT} : **Violated** φ_2^{AT} : **Violated** φ_3^{AT} : Satisfied

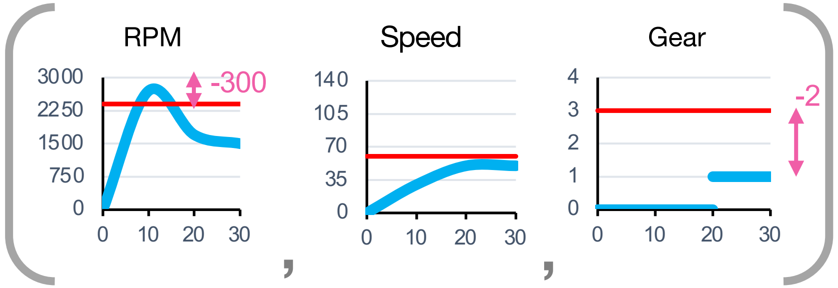
Satisfying all conjuncts are required

Challenge: Scale problem

- Usual robust semantics of conjunction [Fainekos & Pappas, FATES & RV'06]

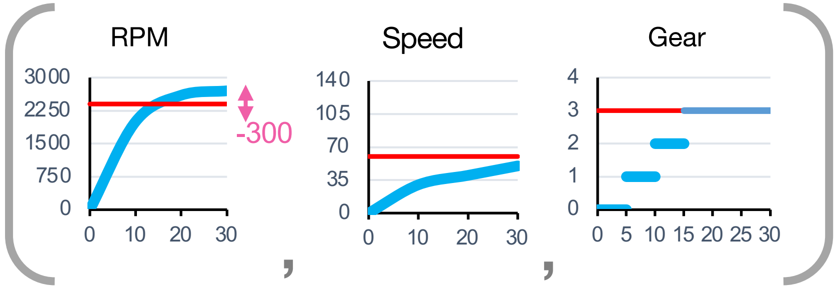
$$[\![\mathcal{M}(u), \varphi^{AT}]\!] = [\![\mathcal{M}(u), \varphi_1^{AT}]\!] \sqcap \cdots \sqcap [\![\mathcal{M}(u), \varphi_3^{AT}]\!]$$

infimum



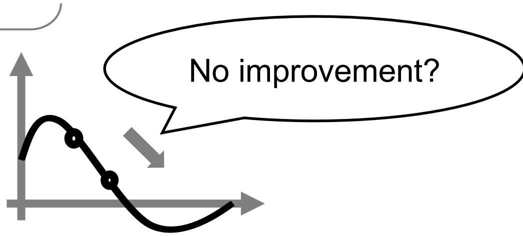
φ_1^{AT} : **Violated** φ_2^{AT} : Satisfied φ_3^{AT} : **Violated**

$[\![\mathcal{M}(u), \varphi^{AT}]\!]$ = **-300**



φ_1^{AT} : **Violated** φ_2^{AT} : Satisfied φ_3^{AT} : **Satisfied**

$[\![\mathcal{M}(u), \varphi^{AT}]\!]$ = **-300**



👎 **Contribution of small-scale conjunct is masked**

Conjunctive synthesis by constrained optim.

Maximize $[\![\mathcal{M}(u), \varphi_1^{AT}]\!] \sqcap \cdots \sqcap [\![\mathcal{M}(u), \varphi_3^{AT}]\!]$

Maximize $[\![\mathcal{M}(u), \varphi_1^{AT}]\!]$

Subject to $[\![\mathcal{M}(u), \varphi_2^{AT}]\!] > 0,\ [\![\mathcal{M}(u), \varphi_3^{AT}]\!] > 0$

Choose one conjunct as the optimization target

No masking

Multiple constraint ranking

How to effectively search the solution of constrained optimization?
➔ MCR [de Paula Garcia et al., Computers and Structures 2017]

- Balances multiple preferences of the solution of constrained optimization
  - Objective function, violation degrees, the number of violated constraints
- Scale-invariant
- No hyper-parameter

Preferred solutions of constrained optim.

Robustness for each conjuncts

	φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}
u_1	1400	-10	-3
$\underline{u_2}$	1400	59.9	0

Feasible is preferred

	φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}
u_1	1400	59.9	-2
$\underline{u_2}$	1400	59.9	-1

Small violation degree is preferred

	φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}
u_1	-1000	59.9	0
$\underline{u_2}$	-30	59.9	0

Large fitness is preferred

Formal definition of MCR

For a population X of candidate inputs, one prioritizes individuals $u \in X$ by

Feasibles are always prior to infeasibles

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

Smaller is better

- **RObj** compares the value of objective function
- **RCon** compares the violation degree of each constraints
- **RVNum** compares the number of violated constraints

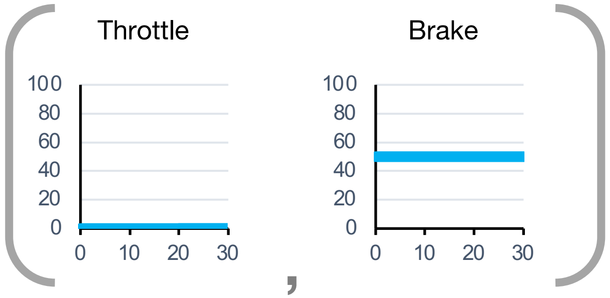
Example: Usual semantics

Robustness for each conjuncts

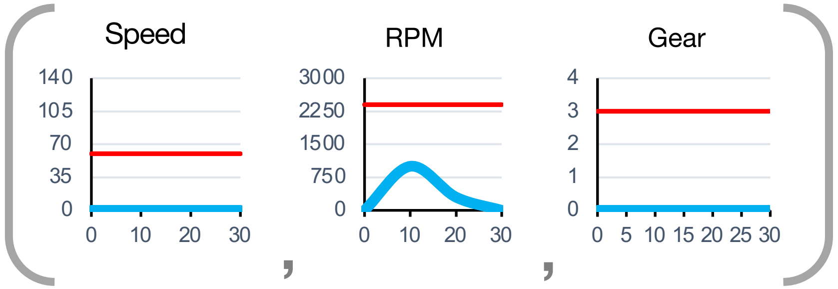
		φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}
Individual	u_1	1400	59.9	-3
	u_2	-9	2	0
	u_3	-180	2	-1

(Naive input)

$u_1 =$

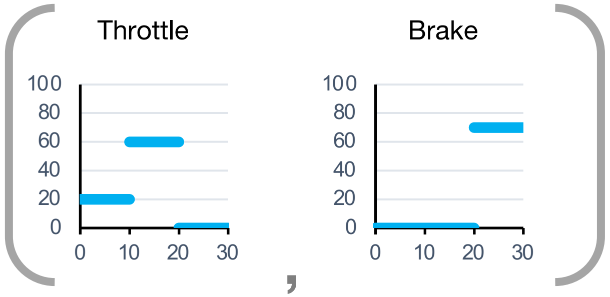


$\mathcal{M}(u_1) =$

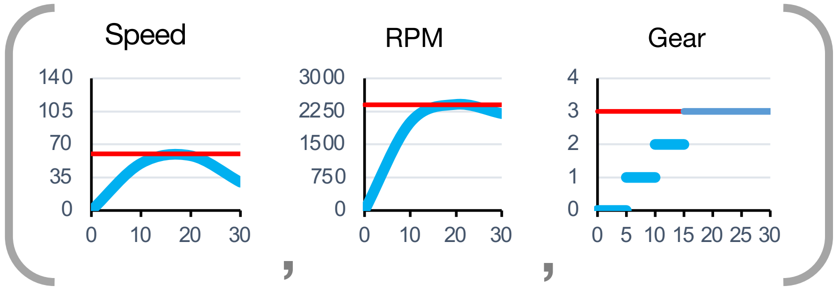


(Almost-satisfying input)

$u_2 =$



$\mathcal{M}(u_2) =$



Example: Usual semantics

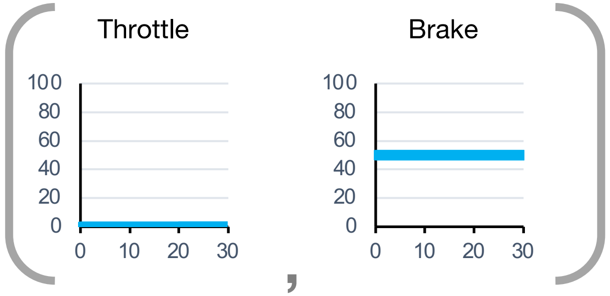
Robustness for each conjuncts

		φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}	infimum
Individual	u_1	1400	59.9	**-3**	**-3**
	u_2	**-9**	2	0	**-9**
	u_3	**-180**	2	-1	**-180**

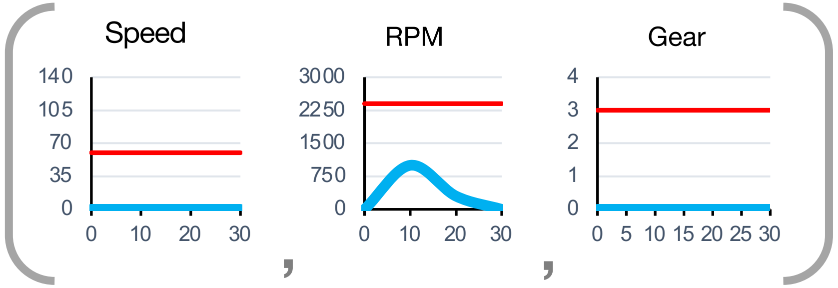
Usual (infimum) semantics says u_1 is the most preferred

(Naive input)

$u_1 =$

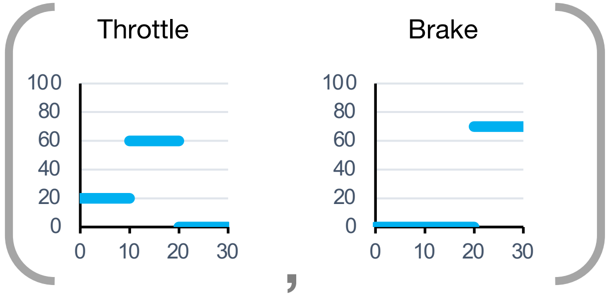


$\mathcal{M}(u_1) =$

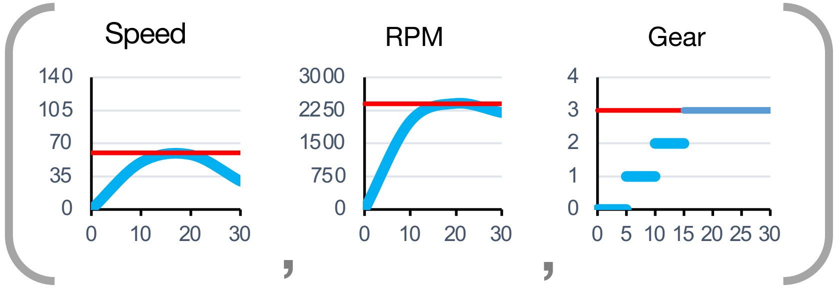


(Almost-satisfying input)

$u_2 =$



$\mathcal{M}(u_2) =$



Example: Calculating MCR

Robustness for each conjuncts

Individual		φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}
	u_1	1400	59.9	-3
	u_2	-9	2	0
	u_3	-180	2	-1

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

	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)

MCR says u_2 is the most preferred

Example: Usual semantics vs. MCR

Usual semantics

	φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}	infimum
u_1	1400	59.9	-3	**-3**
u_2	-9	2	0	-9
u_3	-180	2	-1	-180

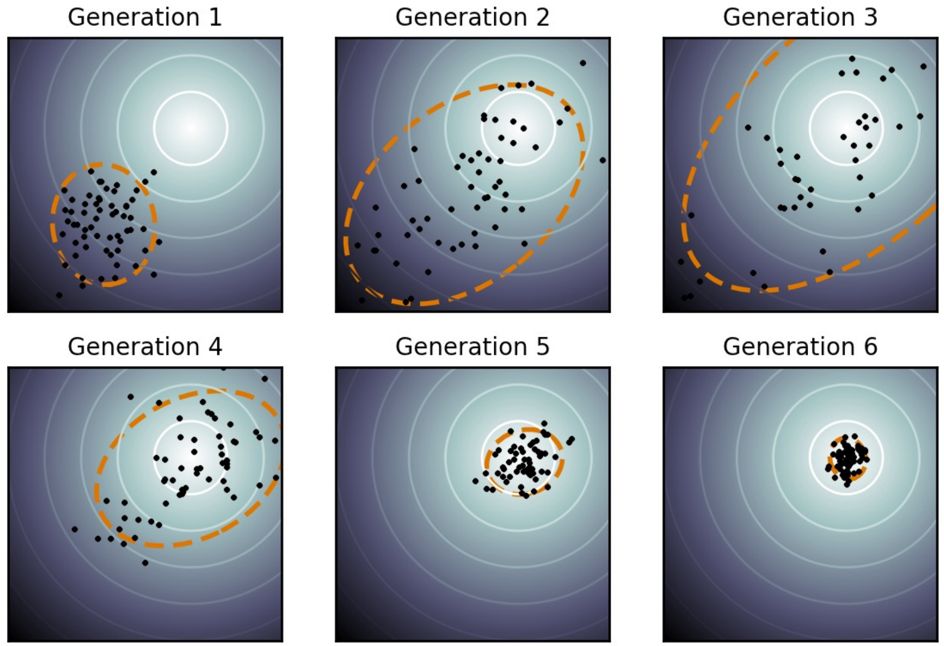
MCR

	φ_1^{AT} (objective)	φ_2^{AT}	φ_3^{AT}	F_X
u_1	1400	59.9	-3	7
u_2	-9	2	0	**5**
u_3	-180	2	-1	8

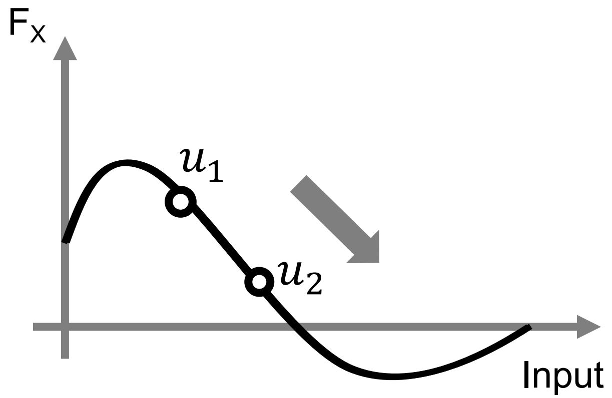
MCR fits our intuition

MCR for falsification

- Optimization algorithm should be population-based
- We adopt **CMA-ES** [Hansen & Ostermeier, International Conference on Evolutionary Computation 1996]
- CMA-ES is commonly used in optimization-based falsification



https://en.wikipedia.org/wiki/CMA-ES



Experimental setting

Model

- Automatic transmission [Hoxha et al., ARCH'15]
- Abstract fuel Control [Jin et al., HSCC'14]
- Wind Turbine [Schuler et al., ARCH'16]

Solver

- Breach (state-of-the-art falsification solver) [Donze, CAV'10]
- MCR (Breach + MCR calculator implemented in Python)
  - Choose each conjunct as **the optimization target** and report **best and worst results**

Metrics

- Success rate (per 60 trials)
- Average elapsed time of successful trials

Particularly exhibits the scale problem

Spec. ID	φ_1	φ_2	φ_3	φ_4
$\mathrm{AT1}_p$	$\Box_{[0,30]}(\mathsf{rpm} \leq p)$	$\Box_{[0,30]}(\mathsf{speed} \leq 60)$	$\Diamond_{[0,30]}(\mathsf{gear} \geq 3)$	
AT2	$\Diamond_{[0,29]}(\mathsf{speed} \geq 100)$	$\Diamond_{[29,30]}(\mathsf{speed} \leq 65)$		
$\mathrm{AT3}_{p1,p2}$	$\Diamond_{[0,10]}(\mathsf{speed} \geq p_1)$	$\Box_{[0,30]}(\mathsf{rpm} \leq p_2)$		
AFC	$\Box_{[31,50]}(\mathsf{mode} = 0)$	$\Diamond_{[11,20]}(\mathsf{mode} = 1)$	$\Box_{[0,30]}(\mathsf{throttle} > 40 \Rightarrow \mathsf{engine} < 1000)$	$\Diamond_{[0,50]}\Box_{[0,25]}(\mathsf{engine} > 1000)$
WT	$\Diamond_{[0,90]}\Box_{[0,5]}(\theta < 12 \land 15.5 \leq v \leq 15.95)$	$\Diamond_{[0,90]}(M_{g,d} \geq 47000)$	$\Diamond_{[0,90]}(\Omega < 9)$	

Experimental results

Our approach

The choice of optimization target

Model	Spec. φ	Breach		MCR (best)		MCR (worst)	
		SR	time [s]	SR	time	SR	time
AT	$AT1_{2500}$	58	34.3	**60**	33.9	**60**	38.9
	$AT1_{2400}$	18	72.7	**55**	147.0	28	87.3
	$AT1_{2300}$	0	—	**37**	326.4	0	—
	AT2	51	245.1	**54**	307.9	43	233.1
	$AT3_{80,4500}$	**60**	31.3	**60**	24.4	**60**	31.0
	$AT3_{50,2700}$	**60**	108.8	59	127.7	56	157.0
AFC	AFC	43	272.4	**54**	288.2	48	248.3
WT	WT	**60**	175.7	**60**	174.0	59	180.1

- Largerst success rates are show in blue
- Best combination of (SR, time) is highlighted

RQ1: Does MCR address the scale problem?

Model	Spec. φ	Breach		MCR (best)		MCR (worst)	
		SR	time [s]	SR	time	SR	time
AT	$AT1_{2500}$	58	34.3	**60**	33.9	**60**	[illegible]
	$AT1_{2400}$	18	72.7	**55**	147.0	28	[illegible]
	$AT1_{2300}$	0	—	**37**	326.4	0	—
	$AT2$	51	245.1	**54**	307.9	43	233.1
	$AT3_{80,4500}$	**60**	31.3	**60**	24.4	**60**	31.0
	$AT3_{50,2700}$	**60**	108.8	59	127.7	56	157.0
AFC	AFC	43	272.4	**54**	288.2	48	248.3
WT	WT	**60**	175.7	**60**	174.0	59	180.1

Breach always failed but MCR **succeeded 37 times** (/60)

- Yes. Our approach resulted higher SR in most cases (blue)
- Specifically, the advantage is obvious where the scale problem is more eminent

RQ2: How important is the choice of the objective conjunct in MCR?

The performance of MCR (worst) is **comparable or better** compared to Breach in every benchmarks.

Model	Spec. φ	Breach		MCR (best)			
		SR	time [s]	SR	time	SR	
AT	$AT1_{2500}$	58	34.3	**60**	33.9	**60**	38.9
	$AT1_{2400}$	18	72.7	**55**	147.0	28	87.3
	$AT1_{2300}$	0	—	**37**	326.4	0	—
	AT2	51	245.1	**54**	307.9	43	233.1
	$AT3_{80,4500}$	**60**	31.3	**60**	24.4	**60**	31.0
	$AT3_{50,2700}$	**60**	108.8	59	127.7	56	157.0
AFC	AFC	43	272.4	**54**	288.2	48	248.3
WT	WT	**60**	175.7	**60**	174.0	59	180.1

- A **bad choice** had **a negative effect** on the performance of MCR
- The effect is not so critical

Future work and Conclusion

Future work

- A method to choose the good objective conjunct
- Extension to more general form of specifications

Conclusion

- A method solving conjunctive synthesis via constrained optimization
- MCR and CMA-ES for effective optimization
- Our approach addresses the scale problem