Constrained Optimization for Hybrid System Falsification and Application to Conjunctive Synthesis

Sota Sato*†, Masaki Waga*‡, Ichiro Hasuo*†
*National Institute of Informatics, Tokyo, Japan (e-mail: {sotasato,hasuo}@nii.ac.jp)
†The Graduate University for Advanced Studies, Tokyo, Japan
‡Graduate School of Informatics, Kyoto University, Japan (e-mail: mwaga@fos.kuis.kyoto-u.ac.jp)

***Index Terms*—control system synthesis, cyber-physical system, constrained optimization, evolutionary algorithm, temporal logic, hybrid system falsification, search-based testing**

I. Motivation and Problem Formulation

Optimization-based falsification [1], is an established approach to the falsification problem. The goal of the falsification problem is to find an input signal u such that the output $\mathcal{M}(u)$ violates the specification φ. Optimization-based falsification translates the falsification problem into minimization of the *robustness*, an (extended) real number $[\![\mathcal{M}(u), \varphi]\!]$ defined in the robust semantics [2], in which negative values mean the violation. This allows us to utilize existing optimization algorithms to find a falsifying input.

One easily figures out that falsification of $\neg\varphi$ (i.e., to find a falsifying input for $\neg\varphi$) is equivalent to *synthesis* for φ (i.e., to find an input that satisfies φ). We aim to exploit and extend the techniques for optimization-based falsification with the aim of solving the following *conjunctive synthesis problem*.

Problem 1 (Conjunctive Synthesis)**. Given:** a *model* $\mathcal{M}$ that takes an input signal u and yields an output signal $\mathcal{M}(u)$, and a *conjunctive specification* $\varphi \equiv \varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_m$ given by *signal temporal logic* (STL) formula.

Find: a *satisfying input*, that is, an input signal u such that the corresponding output $\mathcal{M}(u)$ satisfies φ.

Example 2. Here is our leading example. The system model $\mathcal{M}$ is given by a Simulink model for automatic transmission system [3]. The model $\mathcal{M}$ has two inputs ($\mathsf{throttle}, \mathsf{brake}$) and three outputs ($\mathsf{rpm}, \mathsf{speed}, \mathsf{gear}$). The specification is given by

$$\varphi :\equiv \varphi_1 \wedge \varphi_2 \wedge \varphi_3, \text{ where } \varphi_1 :\equiv \Box_{[0,30]}(\mathsf{rpm} \leq 2400),$$
$$\varphi_2 :\equiv \Box_{[0,30]}(\mathsf{speed} \leq 60), \varphi_3 :\equiv \Diamond_{[0,30]}(\mathsf{gear} \geq 3);$$

it means the gear should reach the third without any of RPM and speed getting too large, a requirement common in the break-in procedure. This conjunctive synthesis asks for a careful trade-off because it contains conflicting requirements; gear gets larger typically when RPM and/or speed is larger.

Existing falsification solvers can struggle with some problem instances due to the *scale problem*, a general difficulty in falsification that is identified and tackled in [4]. The recent paper [4] proposed a solution concerning *multi-armed bandit problem* (MAB); however, it is dedicated to satisfying the specifications of the form $\Box_I(\varphi_1 \vee \cdots \vee \varphi_m)$ and $\Diamond_I(\varphi_1 \wedge \cdots \wedge \varphi_m)$; therefore it does not apply to our current problem of conjunctive synthesis (satisfying $\varphi_1 \wedge \cdots \wedge \varphi_m$).

To handle the scale problem, our proposed method for solving conjunctive synthesis combines optimization-based falsification and *constrained optimization*.

II. Conjunctive Synthesis by Constrained Optimization

In the light of optimization-based falsification, conjunctive synthesis problem can be turned into the following optimization problem:

$$\underset{u}{\text{maximize}} \quad [\![\mathcal{M}(u), \varphi_1]\!] \sqcap \cdots \sqcap [\![\mathcal{M}(u), \varphi_m]\!]. \tag{1}$$

Note that the robust semantics interprets conjunction $\wedge$ by the infimum $\sqcap$ of real numbers.

However, the issue here is that some specific component can dominate the robustness of a Boolean combination and masks away the other components and prevent hill-climbing optimization algorithms from effectively making all the components positive—this is the scale problem.

Our main idea is to regard conjuncts not as objectives but as constraints.

Problem 3 (Conjunctive Synthesis by Constrained Optim.)**.**

$$\begin{aligned} &\underset{u}{\text{maximize}} && [\![\mathcal{M}(u), \varphi_1]\!] \\ &\text{subject to} && [\![\mathcal{M}(u), \varphi_i]\!] > 0, \quad i = 2, \ldots, m. \end{aligned} \tag{2}$$

If the discovered maximum is positive, then the corresponding value of the optimization variable u is a solution to conjunctive synthesis (Problem 1).

The conflict between different conjuncts $\varphi_1, \ldots, \varphi_m$ is buried away in a single objective function in (1); it is made explicit in (2) via the translation of Problem 1 to Problem 3. This translation would lead to an efficient solution only if there exists an algorithm that successfully exploits the structure that is now made explicit. This is the topic of the next section.

III. Our Algorithm: Combining MCR and CMA-ES

For an optimization problem such as (1), we adopt CMA-ES, an evolutionary optimization algorithm introduced by [5], whose efficiency in the context of optimization-based falsification is well-established [4].

The *multiple constrained ranking* algorithm (MCR) [6] is a constraint handling technique (CHT) for general evolutionary

optimization algorithms, hence also for CMA-ES. MCR address the scale problem in the constraints and/or the objective function, using suitable *rankings*—instead of robustness values of constraints themselves—in prioritizing candidate solutions.

Let us write $f(u) = [\![\mathcal{M}(u), \varphi_1]\!]$ for the optimization objective (the fitness function). MCR in CMA-ES consists of replacing the use of the fitness function f, in the *selection* step of CMA-ES, with the *scoring function* F_X, relies on the current population X. The value $F_X(u)$ is a natural number, and those u with smaller $F_X(u)$ are deemed fitter.

The scoring function F_X employs three kinds of functions $\mathsf{RObj}_X, \mathsf{RVNum}_X, \mathsf{RCon}^j_X$; all return a suitable "rank" of the input. RObj_X compares the value of the objective function f, namely the value of $[\![\mathcal{M}(v), \varphi_1]\!]$. RCon^j_X $(j = 2, \dots, m)$ compares the violation of φ_j, namely $0 \vee [\![\mathcal{M}(v), \varphi_j]\!]$. RVNum_X compares the number of violated constraints.

TABLE I
EXAMPLE; USUAL ROBUST SEMANTICS (TOP) AND MCR SCORING (BOTTOM) FOR INDIVIDUALS

Individual	φ_1	φ_2	φ_3	infimum
u_1	1400	59.9	-2	-2
u_2	-9	2	1	-9
u_3	-180	2	-1	-180

Individual	RObj_X	RCon^2_X	RCon^3_X	RVNum_X	F_X
u_1	1	1	3	2	7
u_2	2	1	1	1	5
u_3	3	1	2	2	8

Example 4. In the setting of Example 2, for certain individuals in $X = \langle u_1, u_2, u_3 \rangle$, their robustness values $[\![\mathcal{M}(u_i), \varphi_j]\!]$ with respect to $\varphi_1, \varphi_2, \varphi_3$ are shown in the top part of Table I.

The usual robust semantics indicates the input u_1 is the best individual among X, of which the infimum is the largest. However, once we inspect the input signals u_1, u_2, u_3, it becomes obvious that u_1 is the farthest from desired—it is in fact the signal in which brake is constantly the maximum and throttle is constantly 0.

This mismatch between the robustness-based preference and human intuition comes from the scale problem. The robustness of φ_3 (namely gear) tends to mask that of others.

In contrast, the MCR scoring function gives different preference, as shown in the bottom part of Table I. Here we pick the formula $\varphi_1 \equiv \Box_{[0,30]}(\mathsf{rpm} \leq 2400)$ as the objective; the others φ_2, φ_3 are deemed to be as constraints.

The scoring function F_X indicates the best input is u_2. This matches human intuition: the input signal u_2 is one with moderate throttle and no braking. The signal u_2 satisfies φ_2, φ_3 and almost satisfies φ_1, violating the RPM limit 2400 only by 9.

IV. EXPERIMENTS

We implemented our conjunctive synthesis algorithm (henceforth denoted by "MCR") by combining Breach [7] with MCR. In our implementation, we replaced the MATLAB implementation of CMA-ES with *pycma* (a standard Python implementation of CMA-ES by [5]) and combined with MCR (also implemented in Python).

TABLE II
EXPERIMENTAL RESULTS. FOR EACH PROBLEM INSTANCE, THE BEST RESULT IS HIGHLIGHTED AND THE LARGEST SR IS SHOWN IN BLUE.

Model	Spec. φ	Breach		MCR (best)		MCR (worst)	
		SR	time [s]	SR	time	SR	time
AT	$\mathrm{AT1}_{2500}$	58	34.3	**60**	33.9	**60**	38.9
	$\mathrm{AT1}_{2400}$	18	72.7	**55**	147.0	28	87.3
	$\mathrm{AT1}_{2300}$	0	—	**37**	326.4	0	—
	AT2	51	245.1	**54**	307.9	43	233.1
	$\mathrm{AT3}_{80,4500}$	**60**	31.3	**60**	24.4	**60**	31.0
	$\mathrm{AT3}_{50,2700}$	**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

In our experiments, we used the benchmark models from [8] and specifications. We set a timeout in 600 seconds; and measured the *success rate* (out of 60 trials) and the *average elapsed time* of the successful trials. See [9] for the details of the models, the specifications, and other experiment setups. Table II summarizes the experiments results.

When one translates optimization-based falsification into constrained optimization, there is freedom in the choice of the objective conjunct. In our experiments, we tried each conjunct in a specification as the optimization target, and we report the performance of the best and the worst choices.

The experiment results suggest that MCR successfully addresses the scale problem. The advantage of MCR is more obvious in challenging problem instances such as $\mathrm{AT1}_{2400}$, $\mathrm{AT1}_{2300}$ and AFC. AT2 and AT3 are less challenging ones where the scale problem is less eminent; for these problem instances, too, MCR's performance is comparable or better compared to plain Breach.

The hardest instance $\mathrm{AT1}_{2300}$, in which the performance gap between MCR (best) and MCR (worst) is largest, indicates that a bad choice of the objective may have a negative effect on the performance of MCR. However, the effect is not so critical, observing that the performance of MCR (worst) is comparable or better compared to Breach without MCR in every benchmarks.

V. FUTURE WORK

One future work is to extend our idea of using the constrained optimization problem to a more general form of specifications than the conjunctive specifications in the synthesis problem. Investigating a method to choose a good objective conjunct is another future work.

REFERENCES

[1] G. E. Fainekos and G. J. Pappas, "Robustness of temporal logic specifications for continuous-time signals," *Theor. Comput. Sci.*, vol. 410, no. 42, pp. 4262–4291, 2009.

[2] A. Donzé and O. Maler, "Robust satisfaction of temporal logic over real-valued signals," in *Formal Modeling and Analysis of Timed Systems - 8th Int. Conf., FORMATS 2010*, 2010, pp. 92–106.

[3] B. Hoxha, H. Abbas, and G. Fainekos, "Benchmarks for temporal logic requirements for automotive systems," in *ARCH14-15*, ser. EPiC Series in Computing, vol. 34. EasyChair, 2015, pp. 25–30.

[4] Z. Zhang, I. Hasuo, and P. Arcaini, "Multi-armed bandits for boolean connectives in hybrid system falsification," in *Proc. CAV 2019, Part I*, ser. LNCS, vol. 11561. Springer, 2019, pp. 401–420.
[5] N. Hansen, "The CMA evolution strategy: A tutorial," *CoRR*, vol. abs/1604.00772, 2016.
[6] R. de Paula Garcia, B. S. L. P. de Lima, A. C. de Castro Lemonge, and B. P. Jacob, "A rank-based constraint handling technique for engineering design optimization problems solved by genetic algorithms," *Computers and Structures*, vol. 187, pp. 77–87, 7 2017.
[7] A. Donzé, "Breach, A toolbox for verification and parameter synthesis of hybrid systems," in *Proc. CAV 2010*, 2010, pp. 167–170.
[8] G. Ernst, P. Arcaini, I. Bennani, A. Donze, G. Fainekos, G. Frehse, L. Mathesen, C. Menghi, G. Pedrielli, M. Pouzet, S. Yaghoubi, Y. Yamagata, and Z. Zhang, "Arch-comp 2020 category report: Falsification," in *Proc. ARCH 2020*, ser. EPiC Series in Computing, vol. 74. EasyChair, 2020, pp. 140–152.
[9] S. Sato, M. Waga, and I. Hasuo, "Constrained optimization for falsification and conjunctive synthesis," *CoRR*, vol. abs/2012.00319, 2020, preprint, to appear in 7th IFAC Conference on Analysis and Design of Hybrid Systems, ADHS 2021, July 7-9, 2021, Brussels, Belgium.