October 20, 2021

New method for automatic and efficient discovery of reliable gas turbine system designs

-- Exploiting the logical specification in black box optimization and applying it to the design process of real commercial products --

A research team consisting mainly of SATO Sota and HASUO Ichiro at the National Institute of Informatics (NII, Japan) and the Graduate University for Advanced Studies (SOKENDAI, Japan), developed a method for automatically finding gas turbine control system designs that satisfy multiple requirements, with collaboration of Mitsubishi Heavy Industries, Ltd.

Automatic control system design methods have not hitherto been able to discover controllers of comparable quality to those designed by human experts. But with the new method developed by this research team, it is now possible to find controllers with comparable quality to the results obtained manually by human experts, based on fully automatic computation. This method is generally applicable to “black box” control systems whose internal behavior cannot be described by models such as mathematical formulas. The method is expected to be useful in design processes in various fields such as autonomous driving.

This research was conducted under the ERATO MMSD Project (*1) funded by the Japan Science and Technology Agency (JST, Japan). The results of this research will be presented online on November 24, 2021 (Chinese Standard Time) at the 24th International Formal Methods Symposium (FM’21).

Background

When designing control system for mechanical products, quality assurance should be performed to ensure that the system meets the required specification targets for attributes such as efficiency and safety. The adjustment of systems to improve the efficiency and reliability of products is called optimization, and is routinely performed in industrial product development. In this research, we collaborated with Mitsubishi Heavy Industries on the safety validation and optimization of a gas turbine for power generation. For the safety validation and optimization of such a large-scale control system, it is impractical to conduct repeated experiments with an actual equipment, so the use of computer simulations is an effective approach.

The design of efficient gas turbine systems realizes a power generation system that is efficient in control. For example, if the output is suddenly suppressed due to a drop in electricity demand, then the internal temperature may drop below the minimum limit, resulting in a flame loss that causes the engine to stop. In the event of a flame loss, it will take a lot of time and effort to restart the engine. On the other hand, if the output is reduced too slowly, the turbine speed could become too high, leading to failure. In other

Japan Science and Technology Agency（JST）

Public Relations Division
5-3 Yonban-cho Chiyoda-ku, Tokyo
102-8666 JAPAN
TEL：+81(0)3-5214-8404　FAX：+81(0)3-5214-8432
E-Mail：jstkoho@jst.go.jp

Research Organization of Information and Systems
National Institute of Informatics
Publicity Team
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo
101-8430 JAPAN
Direct: +81(0)3-4212-2164　FAX：+81(0)3-4212-2150
E-Mail: media@nii.ac.jp

words, to design a reliable gas turbine, it is necessary to provide a smart and precise controller that meets all the requirements of multiple factors such as temperature and speed (Fig. 1). In many cases, the optimization of controllers is a complex problem that involves the adjustment of multiple parameters (possibly hundreds of them). Therefore, designing reliable control systems entails efficiently finding better parameter values from a myriad of possibilities.

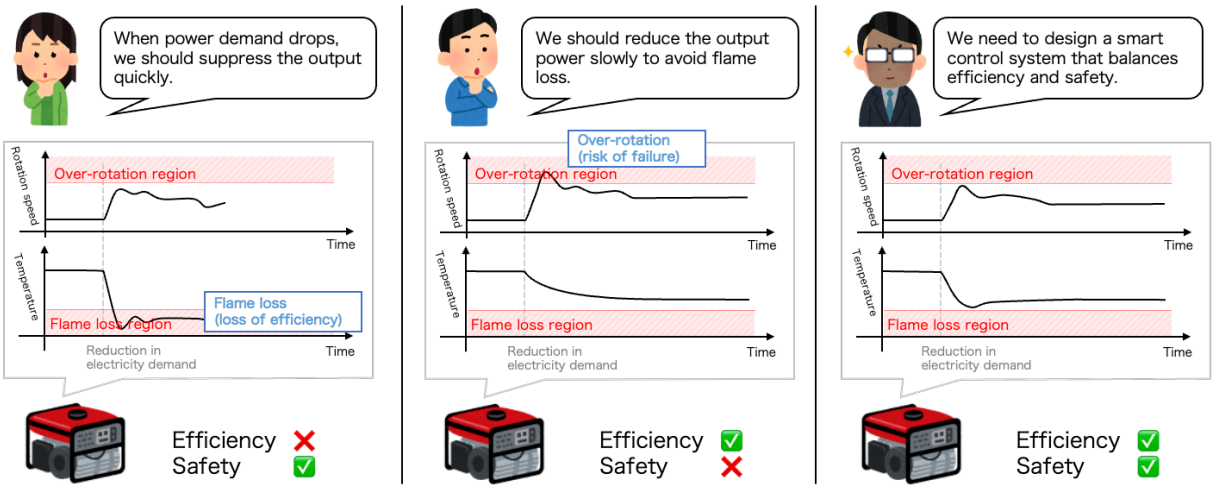

Fig. 1: **A gas turbine controller should be designed to prevent the causes of failure such as excessive rotation speed while preventing the turbine from entering the flame-loss region as a result of temperature changes. Smart controllers must be designed to satisfy these multiple requirements at the same time.**

Parameter optimization is conventionally conducted by human experts based on their expertise and a process of trial and error. If it can be done automatically by a computer, this would significantly reduce the design costs. For example, existing solvers can be used to search automatically for optimal parameters in a so-called “white box” system whose internal behavior is clearly understood and can be described using mathematical formulas such as differential equations that express this behavior precisely. But in real industrial products whose behavior depends on combinations of complex problems, it is seldom possible to obtain practical optimization results by modeling the system as a white box because the behavior of complex systems is difficult to express in mathematical terms. This study was targeted at gas turbine products manufactured by Mitsubishi Heavy Industries. Since the software that controls them is mostly written in machine code, it is difficult for humans to decipher. As a result, these products are “black box” systems that cannot be modelled by methods such as mathematical formulas.

Algorithms that have hitherto been used for the optimization of black-box systems include stochastic optimization and evolutionary computation. Since these algorithms search for numerical parameter values that optimize a system using only the correspondence between the input parameters and the system’s outputs, they can also be applied to the design of control systems for black boxes including not only the gas turbine systems targeted by this study, but also automobiles and airplanes. However, as systems become more complex and their requirements become more stringent, it has become more difficult to find parameters that realize safety and practical performance. For the target system in this study, these existing black-box optimization methods did not produce results comparable to those of a system designed by humans. As a result, most practical systems are still designed by human experts

through a combination of persistent trial and error, coupled with parameter optimization based on expert knowledge that is not clearly documented.

Methods and Results

By improving a black-box optimization method called hybrid falsification, we sought to develop a practical method that can produce optimal results in real systems. As a result, we overcame the drawback of existing black box optimization methods in that they are unable to find parameters that satisfy safety requirements, and at the same time we succeeded in finding parameters of comparable quality to the results obtained manually by experts.

Moreover, while manual optimization by human experts required seven days of trial and error, our new method provides results after just three hours of automatic computation, which significantly reduces the design cost. In addition, this new method does not require large-scale computer facilities and can run on an ordinary computer such as a laptop.

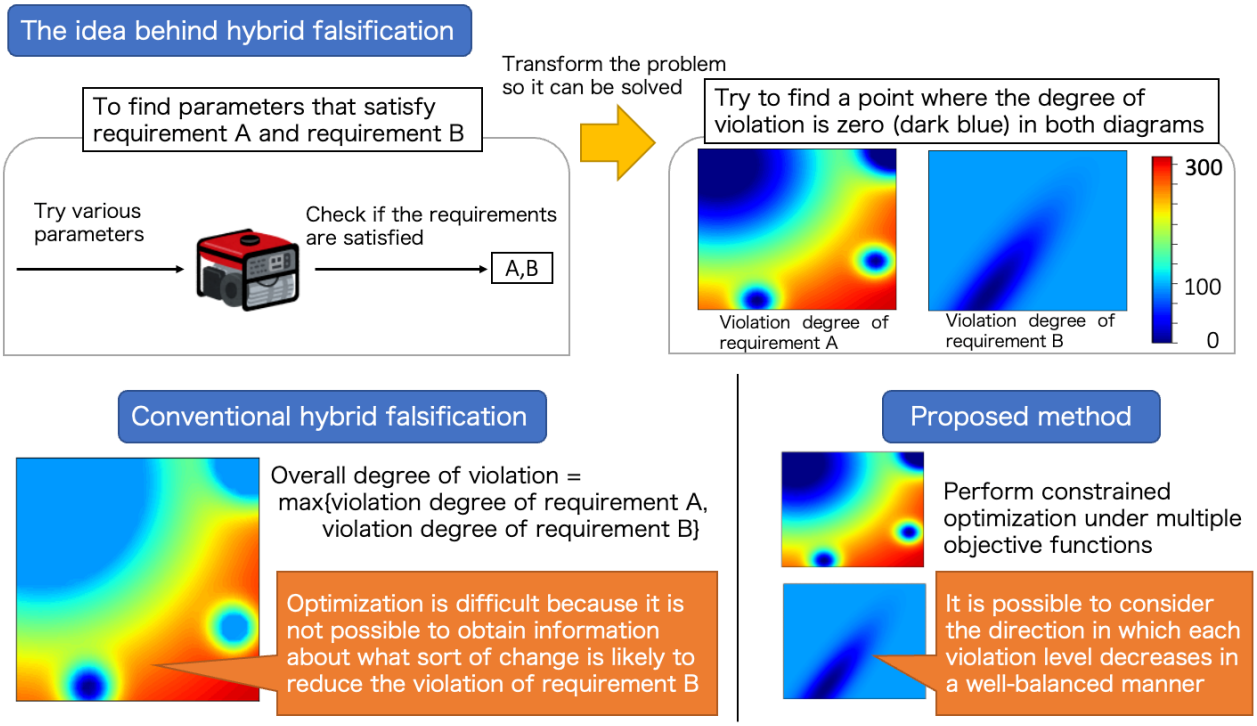

Fig. 2: When provided with multiple formal specifications, the conventional hybrid falsification method has a so-called masking problem whereby it hides information about the degree to which these specifications are violated (left). On the other hand, since the proposed method uses multiple objective functions, it enables a balanced assessment of each violation (right).

In general, hybrid falsification solves the quality assurance problem of finding parameters that satisfy certain requirements by implementing the following two steps: (1) create an objective function that generates a real value expressing how much the system violates the requirements when given certain

parameters, and (2) repeatedly modify these parameters (by using a general-purpose algorithm such as gradient descent) in such a way that the value of this objective function decreases. The requirements in this process are provided as formal specifications described by a logical formula called temporal logic that handles time-related expressions. In the conventional hybrid falsification method, when a logical expression consists of a string of requirements that must be simultaneously satisfied (e.g., requirement A for safety, and requirement B for efficiency), the parameters were sometimes modified to reduce only one requirement specification instead of all of them at the same time. This problem (which is called “masking”) occurs because a single objective function must be used to optimize multiple requirement specifications (Fig. 2, left: conventional hybrid falsification). In this study, we expanded both parts of the two-step hybrid falsification procedure, and we developed a method that (1) uses multiple objective functions and (2) searches on multiple objective functions. This sort of optimization based on multiple objective functions is called “multi-objective optimization” and involves complicated calculations that are completely different from conventional optimization. If this method is applied directly to hybrid falsification, it will therefore be difficult to finish the calculations in a realistic amount of time. Instead, for this study we devised a method based on constrained optimization, which involves weaker conditions than multi-objective optimization, and we showed that it is effective in cases where the logical formula consists of multiple requirements that must be satisfied simultaneously. Furthermore, by using a ranking-based algorithm proposed by de Paula Garcia et al. in a recent work on constrained optimization, we were able to avoid the masking problem without having to perform complex computations (Fig. 2, right: proposed method).

As mentioned above, in this study, we made improvements in black-box optimization by exploiting formal specifications given by logical formulas. In conventional system optimization, calculations using logical specifications of this sort are only effective for discrete, tractable models where the behavior of the system can be mathematically described (i.e., white-box systems). However, in this study, we were able to demonstrate that a logic-focused approach is practical even in the absence of such a model (i.e., black-box systems).

Future outlook

In this study, using a black-box optimization method that takes advantage of a system’s logical specification, we were able to quickly produce results superior to those obtained manually by human experts. Black box optimization based on logical specifications has been mostly applied to the discovery of dangerous scenarios for automobiles and aircraft, but in this study we were able to show an example that it can be used for designing, performing safety checks, and optimizing a wider range of industrial products such as gas turbines.

The key point of this method is that the logical structure of the formal specification is well reflected in the optimization algorithm. Although logical methods have hitherto attracted attention only in limited situations, this study demonstrates that they have great potential for application to a wide range of real-world problems. On the other hand, there are some drawbacks to using this method. To use this method, requirements that were previously written in a natural language have to be converted into logical expressions. To do this, it is necessary to get familiar with formal specification, a skill that is comparable to using a new programming language. To make this method easier to use, further work is needed to develop an interactive formal specification description support tool that anyone can use.

Comment from SATO Sota

"Although logic is a mathematically rigorous framework, it is inflexible in dealing with the uncertainties of real-world systems. It has only been used in limited applications where while box models such as state transition diagrams are available. On the other hand, methods based on stochastic and continuous optimization, such as black-box optimization and machine learning, are applicable to many systems, but it is difficult to modify the algorithms and interpret the output results. In this study, we were able to broaden the range of applications by compounding the benefits of the two contradictory approaches, namely logical methods and black box optimization. It seems that more could be done to explore the interface between the two approaches. Furthermore, to get the best performance from this method, it is essential to make the logical framework easier for humans to understand. I am interested in studying techniques that support the connection between humans and logic, including the description of formal specifications."

Funding

This research has been made possible thanks to the support of the Japan Science and Technology Agency's ERATO-MMSD (JPMJER1603).

Information on Paper

Title: Hybrid System Falsification for Multiple-Constraint Parameter Synthesis: a Gas Turbine Case Study
Authors: Sota Sato, Atsuyoshi Saimen, Masaki Waga, Kenji Takao, Ichiro Hasuo
Conference: 24th International Symposium on Formal Methods
Date of Presentation: November 24, 2021 (Chinese Standard Time)

END

<Media Contact>
Research Organization of Information and Systems
National Institute for Informatics
Publicity Team
TEL: +81(0)3-4212-2164; E-mail: media@nii.ac.jp

<About JST>
Japan Science and Technology Agency (JST)
Department of Research Project UCHIDA Nobuhiro
TEL：+81(0)3-3512-3528 E-mail：eratowww@jst.go.jp

(*1) ERATO Hasuo Metamathematics for Systems Design Project (ERATO-MMSD): a project funded in the Exploratory Research for Advanced Technology (ERATO) scheme of the Japan Science and Technology Agency (JST). The project conducts academic research for quality assurance of cyber-physical systems as the core of Society 5.0. The project specifically focuses on automated driving systems and investigates reliability techniques for modeling, formal verification, testing, and holistic, practical V&V techniques including all of them. This challenge requires tight collaboration of different academic areas such as software science and engineering, control theory and engineering, and artificial intelligence. Therefore, the project also focuses on (meta)mathematical theories. https://www.jst.go.jp/erato/hasuo/en/