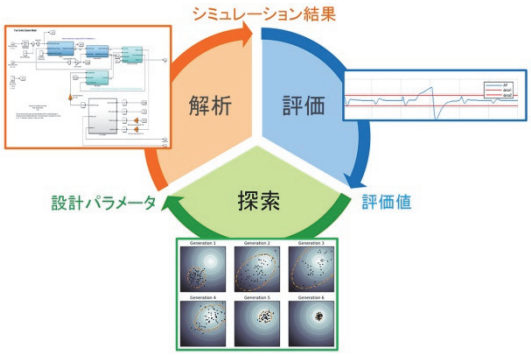
自動検証技術を応用したパラメータ探索技術の開発

Automated Parameter Synthesis by Falsification Technique



西面 敦義*1
Atsuyoshi Saimen

高尾 健司*2
Kenji Takao

蓮尾 一郎*3
Ichiro Hasuo

自動検証技術は，複雑な要件を時相論理式で表現した上で，要件を満足しない入力パターンや運転条件をシミュレータと最適化ソルバーにより探索する技術である。その技術の応用として，複数の要件を同時に満たす設計パラメータを探索できない，“しきい値を超える量も時間も短い方がよい”といったように量と時間の両方に関する要件を扱えないという課題があった。国立情報学研究所と当社の共同研究においてこれらの課題に取り組んだ結果，ガスタービンの負荷遮断時における燃料制御パラメータ設計を例に，人の設計に匹敵する設計パラメータを短時間で探索可能な技術を開発したので本報で紹介する。

1. はじめに

製品設計において，設計パラメータを設定する際，複数条件の下でシミュレーションを行い，性能等の要件を最も良く満たすパラメータを選定することがあるが，製品によっては，複数の相反する要件を満たすように多数の設計パラメータを決定する必要があり，熟練者の試行錯誤による調整により，多くの工数を要している。設計パラメータの自動調整技術として，確率的最適化や進化計算等の最適解探索アルゴリズムによる手法が提案されているが，“一度はしきい値を超えること”，“T秒間以上連続してしきい値を超過しないこと”，“変数Xがしきい値Aを超えた後，変数Yがつねにしきい値Bを上回ること”といった時間の概念を含む複雑な要件が含まれる場合，最適化計算における目的関数や制約条件を定式化することが難しかった。

一方，複雑な要件を扱えるパラメータ探索手法として，自動検証技術を用いる方法がある。自動検証技術は，複雑な要件を時相論理で表現し，要件を満足しない入力パターンや運転条件をシミュレータと最適化ソルバーにより探索する技術であり，要件を満たす設計パラメータの探索にも応用されている。しかし，従来の自動検証技術を応用したパラメータ探索技術は，①複数の要件を満たす設計パラメータを探索できない，②“しきい値を超える量も時間も短い方がよい”というように違反量と違反時間の両方に関する要件を扱えないといった課題があった。これらの課題に対する技術開発を行い，ガスタービンの負荷遮断時における燃料制御パラメータ設計に試行したところ，熟練者が設計した結果に匹敵する設計パラメータを短時間で自動的に抽出できることを確認できた。

以降では，2章で自動検証技術の概要，3章で従来技術の課題，4章で開発した技術，5章で開発技術を用いた数値例，6章でまとめを述べる。

*1 ICT ソリューション本部 CIS 部
*2 ICT ソリューション本部 CIS 部 主席技師 工博
*3 国立情報学研究所 准教授

2. 自動検証技術

2.1 概要

自動検証技術は，図1に示す通り，まず要件を定式化し，①シミュレーションの実行，②要件をどれだけ余裕を持って満たしているかという観点でのシミュレーション結果の定量評価，③要件に対する余裕を小さくするシミュレーション条件の選定，のフローを繰り返し，評価値（余裕）が負となる，すなわち要件を満足しない入力パターンや運転条件を探索する技術である。シミュレーション対象はブラックボックスとして扱われるため，モデルが大規模・複雑な場合でも適用可能であり，シミュレータは入力と出力が取得できるものであればどのようなものでも構わない。要件に対する余裕を小さくするシミュレーション条件の選定は，従来手法では焼きなまし法等の最適解探索アルゴリズムが適用されている。

また，自動検証技術では，信号時相論理と呼ばれる論理体系に従って要件を記述する。信号時相論理を用いることで，前章で例示したような時間の概念を含む要件を扱うことができる。さらに，Robust Semantics と呼ばれる，シミュレーション結果が信号時相論理で記述した要件をどれだけ余裕を持って満たしているか定量評価する手法が提案されており，これにより，要件を満足しない条件の探索を効率的に実行できる。

自動検証技術は既にツール化されたものが普及しており，自動車業界や航空機業界では設計段階における不具合発生ケースの検出に利用された事例が複数報告されている。

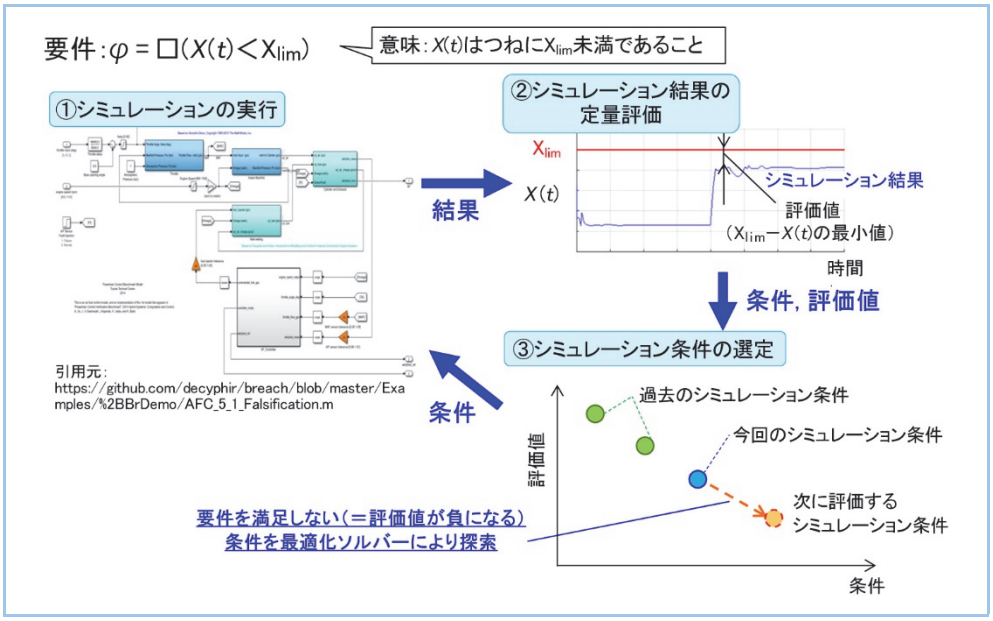


図1 自動検証技術の概要

2.2 パラメータ探索への応用

図1において，入力パターンや運転条件はシミュレーションモデルの設計パラメータでもよい。ここで，要件φの否定（$\neg\varphi$）を要件として設定し，自動検証を行うことで，$\neg\varphi$を満たさない設計パラメータ，つまりφを満たす設計パラメータを探索することができる。

3. 従来技術の課題

自動検証技術によるパラメータ探索の適用にあたり，下記2つの課題があった。

3.1 複数の要件を同時に満たす設計パラメータの探索

複数の要件$\varphi_1,\cdots,\varphi_n$を同時に満たすことを求める場合，要件$\varphi$は$\varphi = \varphi_1 \wedge \cdots \wedge \varphi_n$と記述される。設計パラメータ探索の場合，2.2 節で述べたとおり，φの否定である$\neg\varphi = \neg\varphi_1 \vee \cdots \vee \neg\varphi_n$を満たさない設計パラメータを探索することになる。ここで，$\wedge$は AND 条件，$\vee$は OR 条件を意味する。$\neg\varphi$に対するシミュレーション結果の定量評価結果（以降，評価値と称する）は，$\neg\varphi_1,\cdots,\neg\varphi_n$

の各々に対する評価値のうち，最大のものとして定義される。図2に示す様に複数の要件がVで連結されている場合，$\neg\varphi_2$に対する評価値をより小さくできるパラメータが見つかった場合でも全体の評価値は$\neg\varphi_1$の評価値に支配されてしまい，最適化ソルバーにとってどのようにパラメータを選べば$\neg\varphi_2$の評価値をより小さくできるのか判別できなくなり，探索が進まなくなる。このような問題はスケール問題と呼ばれる。

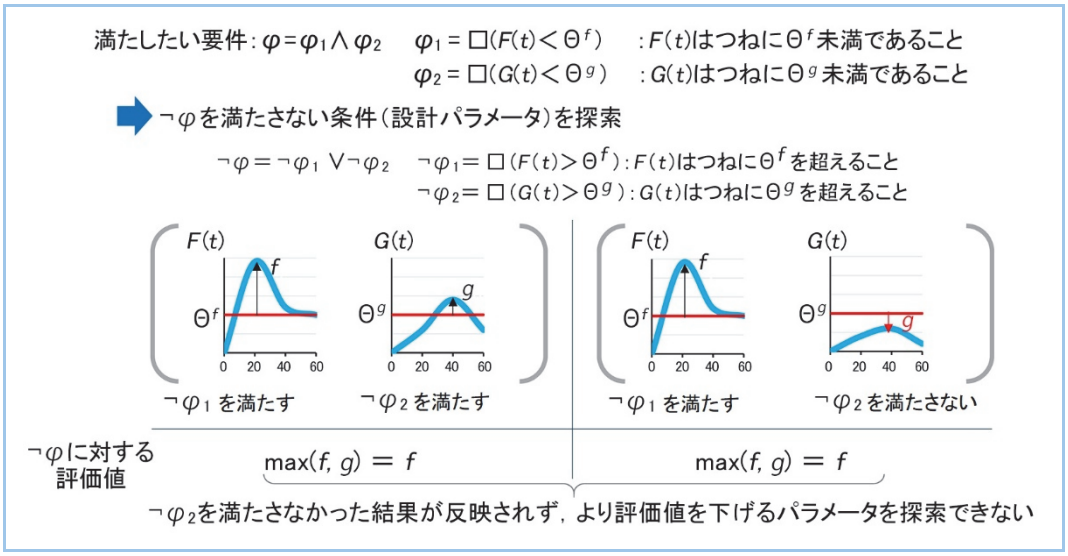


図2　スケール問題の例

3.2　量と時間に関する要件の考慮

自動検証技術において，要件は信号時相論理で記述できる必要がある。要件が，“出力値がしきい値を超過する量も，しきい値を超えている時間もともに短い方が望ましい”といった様ように量と時間の両方に関する場合，通常の信号時相論理では記述できず，信号時相論理を拡張する必要がある。

4. 開発技術

4.1　MCR(Multiple Constraint Ranking)を用いた制約付き最適解探索

3.1 に示した課題に対して，まず，全ての要件の評価値を最小化するのではなく，要件を目的関数と制約条件に分離し，制約付き最適化問題とすることでスケール問題を回避する。次に，制約付き最適化問題の解探索においてMCR(Multiple Constraint Ranking)[(1)] を適用する。MCRの概要を図3に示す。MCRは，PSO(Particle Swarm Optimization)やCMA-ES(Covariance Matrix Adaptation Evolutional Strategy)に代表される，多くの個体の中からより優れた個体を選出していく進化計算手法とともに用いられ，個体選出の指標となる適応度を個体間のランキングにより決定する。これにより，複数要件間のスケール問題が解消できる。制約条件をより多く満たしている個体ほど優れた個体と判断され，その個体の周辺で全ての制約条件を満たし，かつ目的関数を最小化する個体が探索される。

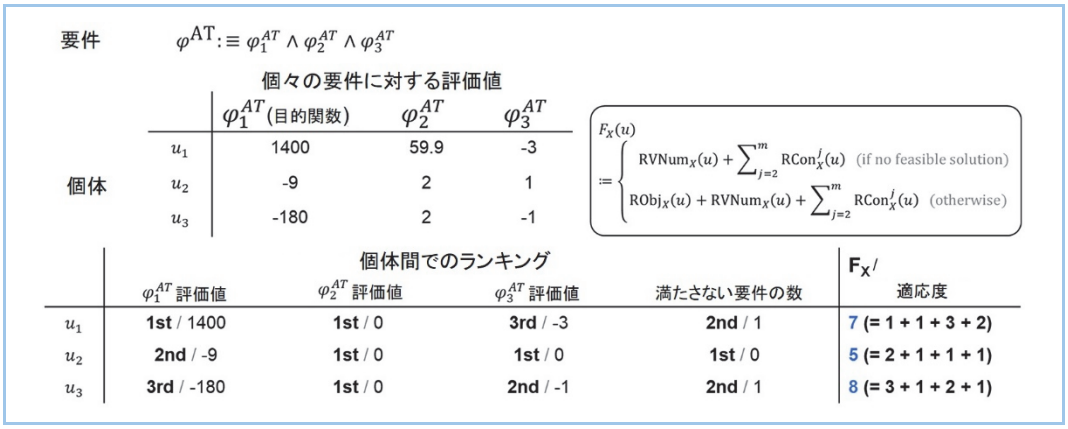


図3 MCR の概要

4.2 Area 関数の導入

3.2 に示した課題に対して，図4に示すように，シミュレーション結果がしきい値を超えている間，しきい値を超えている量を積分して面積を取り，この面積を評価値とする Area 関数を信号時相論理に導入した。Area 関数では，しきい値を超えている量と時間によって評価値に差がつくため，しきい値を超えている量も超えている時間も小さい解を探索することができる。

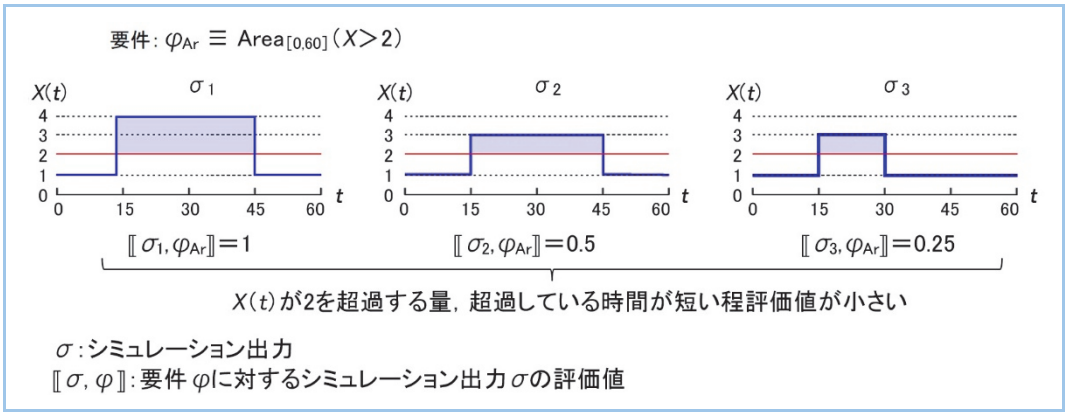


図4 Area 関数

5. 計算例

自動検証技術による設計パラメータ探索の適用例として，ガスタービンの負荷遮断時の燃料制御パラメータ設計を選定した。ガスタービンが電力系統から切り離された際，予め設計された時系列の燃料供給スケジュールに沿って燃料が制御されるが，失火現象や機器損傷を防ぐために，火炎温度やロータ回転数を時間によって適切に変更する必要がある。本設計における要件を図5に示す。要件は必ず満たすべきもの（必須要件 1，2）と可能な限り満たすことが望ましいもの（考慮要件 1，2，3）がある。H_1, H_2は火炎温度，Fはバルブ開度，Gはロータ回転数，θはしきい値を表す。

MATLAB/Simulink ベースの自動検証ツール Breach[(2)]において，MCR と Area 関数を適用できるように拡張し，上記の設計問題に適用した。熟練者が試行錯誤により設計したパラメータ，及び3時間（7000 回以上の探索）の計算により得られたパラメータでシミュレーションした結果を図6に示す。探索により得られたパラメータはH_1, H_2, Gに関する要件を満たし，Fがしきい値を僅かな時間超過するのみであり，熟練者の設計に匹敵する結果が熟練者のノウハウ無しに自動的に得ることができた。

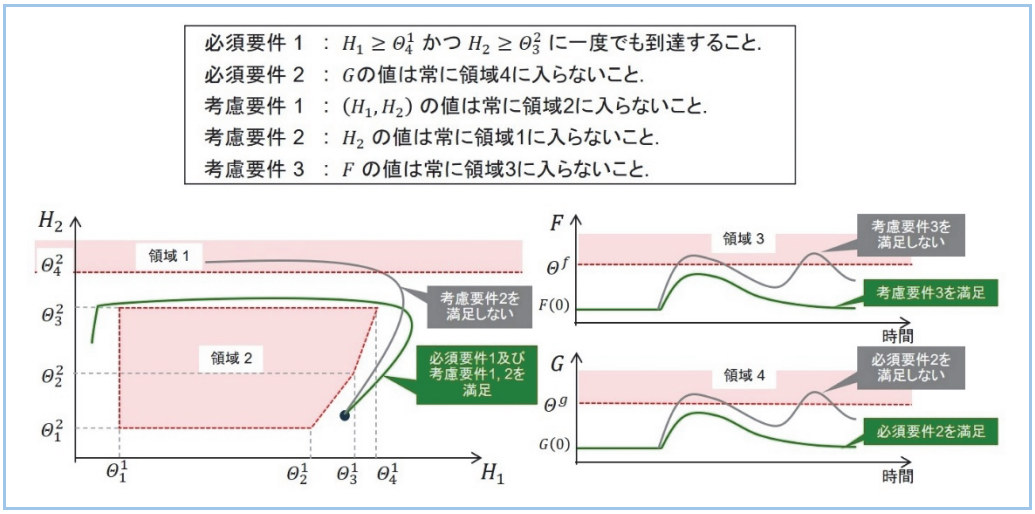


図5 パラメータ設計における要件

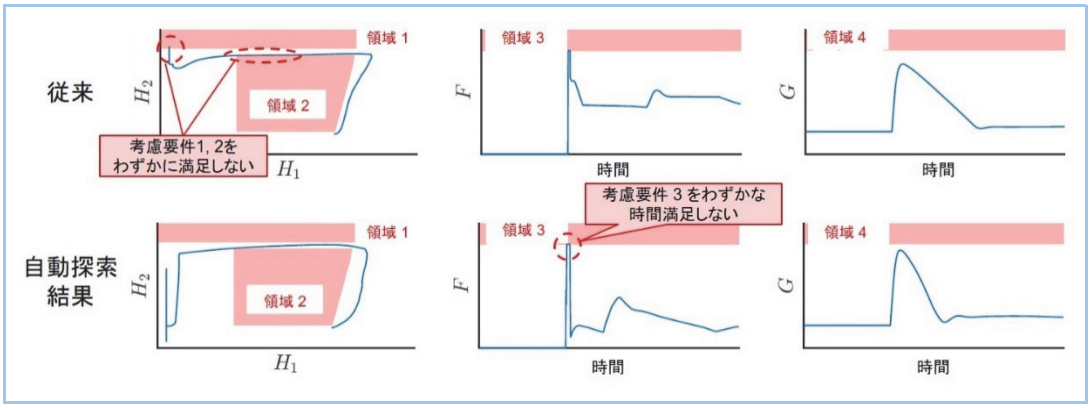


図6 探索結果

6. まとめ

本報では，自動検証技術を応用した設計パラメータ探索手法を，要件が複数ある場合や量と時間に関する要件を含む場合においても適用できるように改良し，ガスタービンの燃料制御パラメータ設計において，熟練者の設計に匹敵する設計パラメータを短時間で探索し，設計工数を大幅に短縮できることを示した。

自動検証技術の当社他製品への展開として，輸送冷凍機の設計検証への適用を進めている。設計段階で要件を満たさないケースが無いか検証することは，開発コスト削減や品質保証の点で重要であり，今後も適用製品を拡げていく。

参考文献

(1) de Paula Garcia et al., A rank-based constraint handling technique for engineering design optimization problems solved by genetic algorithms, Computers and Structures 187 (2017) p77-87
(2) Donzé, A., Breach, A toolbox for verification and parameter synthesis of hybrid systems, Proc. CAV 2010 (2010) p.167-170
(3) Sato S. et al., Hybrid System Falsification for Multiple-Constraint Parameter Synthesis: A Gas Turbine Case Study, Proc. Formal Methods. FM2021 (2021) p.313-329