氏　　名	Zhenya Zhang
学位(専攻分野)	博士(情報学)
学 位 記 番 号	総研大甲第 2197 号
学位授与の日付	2020 年 9 月 28日
学位授与の要件	複合科学研究科　情報学専攻 学位規則第6条第1項該当
学 位 論 文 題 目	Hierarchical Optimization for Hybrid System Falsification
論 文 審 査 委 員	主　査　准教授　蓮尾　一郎
	准教授　岸田　昌子
	助教　関山　太朗
	准教授　石川　冬樹 国立情報学研究所　アーキテクチャ科学研究系
	准教授　海野　広志 筑波大学　大学院システム情報工学研究群

(Form 3)

Summary of Doctoral Thesis

Name in full Zhenya Zhang

Title Hierarchical Optimization for Hybrid System Falsification

Cyber-Physical Systems (CPS) are physical systems integrated with digital control. Quality assurance of CPS is a problem of great importance, but it is also challenging due to the hybrid nature of CPS in which both discrete and continuous dynamics exist. While formal verification approaches suffer from a severe scalability issue, stochastic optimization-based falsification, which aims to find a counterexample input to refute the system specification, is a viable approach to solving the problem. This method turns the problem into an optimization one based on the robust semantics of the specification language, namely Signal Temporal Logic (STL), and employs stochastic optimization algorithms to search for an answer.

Although falsification has proved to be an effective approach, many methodological weaknesses are still there, limiting its usage in practice. In this work, we address three important ones, namely, improper balance between exploration and exploitation during search, superposing robustness values from signals of different scales in STL robust semantics, and inability of handling input constraints.

In order to tackle those problems, we propose a general two-layered hierarchical optimization framework, in which a problem is firstly decomposed into a set of sub-problems, and then solved via a two-layered methodology: the top layer selects a sub-problem as the next step to proceed based on the information given by the bottom layer; the bottom layer performs numerical optimization with the selected sub-problem and returns feedback to the top layer. In this way, the two layers collaborate with each other and work together to solve the problem.

This framework is instantiated to three techniques, each addressing one specific weakness in the existing falsification workflow. In summary, these techniques are:

- A Monte Carlo Tree Search (MCTS)-based technique for balancing exploration and exploitation during search. Hill-climbing optimization used in the existing falsification technique is a greedy search strategy, and thus can easily fall into the local optimum. In our method, we discretize the search space and structure them as a search tree, and then we propose a two-layered optimization framework to perform search: on the top layer, MCTS decides the sub-spaces (identified by branches) that should be further looked into based on the rewards computed by the bottom layer; on the bottom layer, hill-climbing optimization is run in a local space suggested by the top layer to give feedback or find a concrete solution. These two layers collaborate together to improve the effectiveness and efficiency of the search.

- Application of Multi-Armed Bandit (MAB) model to handling safety properties with Boolean connectives. The existing definition of STL robust semantics for Boolean connectives superposes the robustness values from different signals. As signals may have different scales, the global robustness will be biased, and this can affect the falsification performance. We propose a novel technique that treats different sub-formulas as different bandit machines, and applies the MAB algorithms (UCB1 and ε-Greedy) to govern the hill-climbing processes running on different machines. We then define hill-climbing gain rewards to embody the running status of each machine. It forms such a framework: the MAB algorithms on the top layer select one of the machines according to the rewards of them; the selected machine on the bottom layer runs hill-climbing optimization and returns the running status information for computing rewards. These two layers work together to handle the problem of falsifying safety properties with Boolean connectives.
- Handling input constraints via search space transformation technique integrated with the Multi-Armed Bandit (MAB) model. The existing falsification framework ignores logical constraints on input signals, and thus produces falsifying inputs that are meaningless. We propose a search space transformation approach, in which the search is allowed to sample in an unconstrained search space, guided by fitness coming from the constrained input space. This is implemented by a surjection that maps points from the unconstrained space to the constrained space. Once a negative fitness is observed, we return the point in the constrained space as the counterexample for falsification, so that its satisfaction to the input constraints is guaranteed. The performance of this approach is subject to a parameter, namely, a total order over the dimensions of the search space. In order to achieve the best performance, we introduce the MAB model in this context again, and construct the hierarchical framework: the MAB algorithm on the top layer selects the best order and sends it to the bottom layer; the search space transformation-based optimization on the bottom layer runs following that order and gives feedback to the top layer. Again, they solve the problem through collaboration.

We run experiments on real Simulink models, and the experimental results show the effectiveness of our approaches. Together, these approaches enhanced the existing falsification technique.

Moreover, these approaches also exemplify our hierarchical optimization framework, which is potentially applicable in other contexts.

Form8・Separate Sheet
(様式８・別紙１)

Results of the doctoral thesis screening

博士論文審査結果

Name in Full
氏 名　Zhenya Zhang

Title
論文題目　Hierarchical Optimization for Hybrid System Falsification

本論文は，反例生成 falsification と呼ばれる物理情報システムのテスト手法について，出願者が行った研究内容をまとめたものである．応用対象である物理情報システムとは，連続的に動作する物理システムをソフトウェアによってデジタル制御するようなシステムのことを指し，自動車や航空機，医療機器，発電システムなどの例を通じて，現代社会の多くの分野に進出している．物理情報システムのバグは人命の損失やその他の大きな経済的損失につながることが多く，物理情報システムの品質保証は社会的に重要な問題である．一方で，物理情報システムにおいては物理的連続ダイナミクスとソフトウェア的離散ダイナミクスが共存するため（物理情報システムのこの側面を指して特にハイブリッドシステム hybrid system と呼ぶ），従来ソフトウェアの離散的ダイナミクスを対象に研究が行われてきた形式検証の諸手法の実効性は限定的とならざるを得ない．この困難な状況の中で，実効的かつ実システムへの応用が容易な品質保証手法として学術界のみならず産業界からも注目を集めているのが反例生成と呼ばれる手法群である．反例生成はテスト手法の一種であり，バグ探しの問題を適当な目的関数の最適化問題として定式化することで，さまざまな確率的最適化アルゴリズムを用いて物理情報システムのバグを発見することを可能にする．

出願者は，反例生成手法の実効性，特にバグの発見能力を改善することを目指し，既存の反例生成手法の持つ諸課題に対処するような最適化フレームワークを３つ提案した(３，４，５章)．これら３つの最適化手法に共通する特質として，連続最適化と離散最適化を組み合わせた階層的構成を持つことがあげられる．すなわち，既存手法において用いられる勾配降下法による連続的最適化アルゴリズムに加えて，反例生成問題に内在する離散的構造を利用するような離散的最適化アルゴリズムを組み合わせ，後者の離散最適化をハイレベルの最適化レイヤーとして用いて前者の連続最適化をガイドすることにより，バグ発見のための最適化問題をより効率よく解こうというわけである．本論文では，提案される３つの階層的最適化手法のそれぞれに対して，解決を目指す実用上の課題によって動機づけがなされたあと，実験評価によって反例生成の実効性が実際に向上したことが示されている．

論文は６つの章から構成され英語で書かれている．第１章では物理情報システムの品質保証の重要性および困難について導入がなされたあと，本論文の研究の背景として，反例生成の既存手法の学術的な概要および応用の現状の紹介が述べられる．さらに，反例生成の既存手法の持つ課題として，(1) 確率的最適化における活用と探索のバランス，(2) 最適化の目的関数の定義における命題演算子の解釈，(3) バグ探しの探索空間に制約を課すことの困難さ，以上の３つの課題が述べられる．

第２章では，本論文の研究の背景たる確率的最適化による反例生成について，技術的詳細に踏み込んだ導入がなされている．ここでの主題は，仕様記述言語としての時相論理に対して定量的なロバスト意味論を導入した Fainekos や Donze らの成果によりバグ探しの問題が数値最適化問題に帰着できること，ならびに，この帰着を通じていくつかの既存手法・ツールが大きな成功を収めてきたこと，以上の２つである．

第３章では上述の３つの課題の一つ目，すなわち確率的最適化における活用と探索のバランスの課題について，これを解決する階層的最適化手法が導入されている．この手法はハイレベルの離散的最適化レイヤーとしてモンテカルロ木探索を用いるものであり，より具体的には探索木の深さがシステム実行における時間経過に対応し，また探索木の分岐が探索空間の分割に対応する．モンテカルロ木探索をハイレベルの最適化レイヤーとして用いて，ロウレベルの最適化レイヤーたる勾配降下法による連続的最適化をガイドすることにより，探索空間の異なる領域をバランス良く試しながら（探索），有望とみられる領域には連続的最適化のリソースを集中してバグを探索するという（活用），探索と活用のバランスのよい最適化手法を実現したのが本章の貢献である．自動車のオートマティックトランスミッションなどの例を用いた実験によって，提案手法の既存手法に対するバグ発見能力における優位性が示されている．

第４章では上述の３つの課題の二つ目，すなわち最適化の目的関数の定義における命題演算子の解釈の課題について，これを解決する階層的最適化手法が導入されている．本章で対処する上記の課題はより具体的に，スケールの異なる物理量の間で安全マージンを比較することにより片方の寄与分が打ち消されてしまうという，もともとのロバスト意味論の持つ「スケール問題」として説明されている．この課題を解決するための階層的最適化手法は，ハイレベルの離散的最適化レイヤーとして多腕バンディット問題を持つものであり，ここでの「腕」は命題演算子によって結合された各論理式に対応する．提案手法の実験による評価においては，既存手法に比較してのバグ発見能力の優位性が示されているのみならず，人工的に物理量のスケールを変更してスケール問題を発生させても提案手法の性能には影響しないことも示されている．

第５章では上述の３つの課題の三つ目，すなわちバグ探しの探索空間に制約を課すことについて，これを実現する階層的最適化手法が導入されている．探索空間に制約がある最適化問題を解くにあたっては，制約に違反することによるペナルティを目的関数に含めるというアプローチが一般的である．しかしこのペナルティアプローチには，制約を満たさないサンプルが無駄になってしまったり，ペナルティにより目的関数が変わることでもともとの目的関数の最適化に悪影響を及ぼしたりという問題がある．よって本章では，制約付き探索空間を制約のない探索空間に引き延ばすような探索空間変換によるアプローチを提案している．具体的な探索空間変換を与えるため本章では比例変換と呼ぶ関数を導入しているが，比例変換の定義においては，引き延ばす軸の優先度というパラメータが最適化の性能に影響を及ぼす．このパラメータの選び方を多腕バンディット問題として定式化して UCB などのアルゴリズムで最適化するのをハイレベルの離散的最適化レイヤーとし，（ロウレベルの最適化レイヤーとしての）比例変換を介した制約付き連続最適化をガイドするのが，本章で導入されている階層的最適化手法である．実験による性能評価においては，多腕バンディットを用いた提案手法が多くの例において優位性を持つことが示されて

いる.

最後に，第６章では本論文の貢献をまとめ，今後の研究課題と展望を示している.

本論文にまとめられた研究の成果は学術誌 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems の論文２篇（１篇は出版済み，１篇は採択決定済み），および査読付き国際会議予稿集のフルペーパー１篇として発表されている.

公開発表会では博士論文の章立てに従って発表が行われ，その後に行われた論文審査会及び口述試験では，審査委員からの質疑に対して適切に回答がなされた.

以上を要するに本論文は，反例生成という物理情報システムの実効的品質保証手法の研究において,階層的最適化手法という統一的フレームワークによって様々な課題を解決し，反例生成手法の実効性をさらに向上されるものである．この貢献は物理情報システム・論理・最適化などの多様な分野を融合するものであり，離散的構造と連続的構造の両方を階層的手法によって最適化に利用するという方法論も含め，その学術的価値及び実用上の価値は高いと認められる.

以上の理由により審査委員会は，本学位論文が学位の授与に値すると判断した.