氏　　名　和賀 正樹

学位(専攻分野)　博士(情報学)

学 位 記 番 号　総研大甲第 2198 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　Empowering Runtime Verification with Polyhedra

論 文 審 査 委 員　主　査　准教授　蓮尾　一郎

教授　米田　友洋

准教授　福田　健介

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

教授　Jaco van de Pol
オーフス大学

（様式３）

博士論文の要旨

氏　　名 和賀 正樹

論文題目 Empowering Runtime Verification with Polyhedra

This thesis aims to improve the practical effectivity of *runtime verification*, monitoring with logics. Our main application is the safety monitoring of cyber-physical systems (CPSs), e.g., cars and robots. Our technical gadget is the symbolic analysis with *convex polyhedra*. The high-level contribution of this thesis is to show that the polyhedra-based symbolic analysis plays an essential role in various advanced runtime verification algorithms.

Monitoring is, in general, an activity to observe system behavior. In the development and maintenance of systems, it is essential to monitor the system behavior. For example, in development, engineers have to monitor the system behavior to identify the necessary modification to the system under development. In maintenance, for example, engineers have to monitor the running system so that they can replace the system's worn-out components as soon as possible.

Runtime verification (or *specification-based* monitoring) is an automated monitoring technique using logic. Given a formal specification of an unsafe behavior expressed by some logical formalism, runtime verification observes a system execution and evaluates if the observation satisfies the specification.

Although quite a lot of research and engineering efforts have been devoted to runtime verification of CPSs, there are remaining challenges. We identify the following important but often missing features of runtime verification.

- *Generic* algorithms that are applicable to a wide class of runtime verification problems rather than one problem setting
- *Flexible* runtime verification algorithm that does not require complete knowledge of the specifications or behaviors
- *Informative* results such as quantitative satisfaction rather than Boolean satisfaction

In this thesis, we present enhanced runtime verification algorithms focusing on the three features above. In our improvements, the use of polyhedra for symbolic analysis plays an essential role. In the symbolic analysis, we utilize discrete abstraction of the continuous value domains represented by polyhedra: each of which stands for infinitely many concrete values; and thus, we can analyze infinitely many values. This is in contrast to the

analysis of each value, where only finitely many values can be analyzed in finite time.

Such a polyhedra-based analysis is useful, for example, in the runtime verification with an ambiguous specification. Consider the following specification: "whenever the gear of a car becomes low, the gear should remain low for a while," where the definition of "for a while" is unclear. Moreover, the threshold defining "for a while" may depend on the context. When the specification contains such an unspecified threshold, we have to monitor the log considering all the possible thresholds. Since there are infinitely many possibilities, we cannot try each threshold in a one-by-one manner, and we need a polyhedra-based symbolic analysis.

This thesis's high-level contribution is to show the usefulness of the polyhedra-based analysis in runtime verification. To show the usefulness, we conducted three concrete improvements. The following summarizes the usages of polyhedra and the enhanced features in this thesis.

Firstly, in Chapters 3 and 4, we study runtime verification with ambiguous specifications containing unknown thresholds in the constraints. Such a runtime verification algorithm does not require complete knowledge of the monitored specification and is flexible. We use polyhedra for symbolic analysis of infinitely many possible thresholds. In Chapter 3, we introduce and solve the parametric timed pattern matching problem, where we can use a specification with timing parameters to leave some thresholds in the timing constraints unspecified. For example, in the example above, we can represent the timing constraint "for a while" by "for p seconds" using a timing parameter p. In Chapter 4, we generalize the parametric timed pattern matching problem to allow the parameters also in data values. For example, consider the following specification: "whenever the temperature becomes high, the air conditioner must be turned on within 5 seconds", where the high-temperature threshold is unspecified. In this example, we can represent the condition on high-temperature by "more than T degree," where T is a data parameter representing the high-temperature threshold. Moreover, our algorithm is *generic* because it allows any data with a suitable data structure for symbolic analysis such as polyhedra for rationals and an ad hoc data structure for strings.

Secondly, in Chapter 5, we study quantitative timed pattern matching that is a mathematical formulation of quantitative runtime verification of real-valued signals. Quantitative timed pattern matching returns the degree of unsafety and is more *informative* than returning Boolean results. We propose an online algorithm for quantitative timed pattern matching that can monitor a running system. Our notion of unsafe degree and our proposed algorithm are based on

semiring valued weighted automata. Thanks to the algebraic genericity of semirings, our algorithm works for various quantitative semantics capturing different safety criteria such as the worst deviation from the specification and the accumulated deviation from the threshold over time. We use polyhedra to obtain discrete abstraction of the continuous possibility of switching in a temporal specification. Consider the specification "in the beginning, the acceleration of the car is high, and later, the velocity becomes high." When monitoring such a temporal specification, we have to consider all the possible timing of the switching from the "beginning" to the "later." Since there are continuously many possibilities, we utilize polyhedra-based symbolic analysis to consider all such switching.

Thirdly, in Chapter 6, we study runtime verification, where we only have intermittent samples of the signal values. We introduce and solve the model-bounded monitoring problem, where we interpolate the signal values between the samples considering the bounding model. Thanks to the bounding model, model-bounded monitoring is precise even if we reduce the sampling frequency, and thus it is flexible. More precisely, if the bounding model overapproximates the actual system behavior, model-bounded monitoring is guaranteed to detect every unsafe behavior independent of the sampling frequency. Although we may have false alarms, we have fewer false alarms for a more precise bounding model. We use polyhedra to consider all the possible interpolation.

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　　和賀 正樹

Title
論文題目　　Empowering Runtime Verification with Polyhedra

本論文は，実行時検証 runtime verification と呼ばれる物理情報システムの品質保証手法について，その実用性および実効性をさらに向上させるために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．これら物理情報システムの品質保証は，人命の損失やその他の大きな経済的損失に直結する重要な問題である．システムの振る舞いを監視すること（モニタリング monitoring）は，システムの設計上の問題を発見したり，システム実行に介入して危険を回避したりするために不可欠な営為であるが，モニタリングを論理学またはオートマトンを用いた形式的仕様のもとで行うことを実行時検証と呼ぶ．既存研究では，特に時間オートマトン timed automaton および連続時間時相論理の理論に立脚した実行時検証手法が多数提案され，産業界での実用に供されている．

既存研究の実行時検証アルゴリズムの多くの数学的基礎を与えているのが連続空間の多面体 polyhedra による抽象であり，この数学的テクニックにより時間オートマトンの自動解析が可能になっている．出願者は多面体抽象の持つさらなるポテンシャルに注目し，これを利用して時間オートマトンの理論を拡張した上で，その理論的成果を用いて新しい実行時検証手法を導入する研究を行った．同時に，こうして導入された実行時検証手法は，実応用において現れるさまざまな課題を解決するものになっており，実行時検証の実効性を実用的視点から向上されるものである．本論文では特に，実行時検証の実効性の向上を「汎用性 genericity」「柔軟性 flexibility」「表現能力 informativity」の３つの視点で整理して追求している．

本論文は６つの章から構成され英語で書かれている．第１章ではモニタリングおよび実行時検証について研究の背景が述べられたあと，多面体抽象による実行時検証の実用性の向上という本論文の貢献の全体像と，本論文で提案する４つの実行時検証手法それぞれの概要が述べられている．各手法の概要においては，実用上の動機づけ，利用シナリオおよび当該手法の出力例を具体的に述べることにより，実務家の興味にも応えるような記述となっている．

第２章では，時間オートマトンの理論的背景を説明することで，後に続く章の理論的準備を与えている．

第３章では本論文の４つの提案手法の１つ目として，仕様に時間的パラメタを含む実行時検証の問題と，この問題を解く実効的アルゴリズムが述べられている．ユーザーが実行時検証のための形式的仕様を書き下す際に，異常と判断するためのしきい値を具体的にい

くつに設定するかという問題は，実行時検証の実応用においてユーザーがしばしば直面する実用上の問題である.本章では,パラメタ付き時間オートマトンの理論を踏まえた上で，その上のパターンマッチ問題を多面体抽象によって高速に解くアルゴリズムを提案している．このアルゴリズムの実効性は実験により示されている．本章の貢献は，仕様に時間的パラメタを許すことで実行時検証の柔軟性を向上させるとともに，パラメタを用いて時間的余裕を表現することで実行時検証の表現能力をも向上させるものとなっている.

第４章は本論文の４つの提案手法の２つ目として，第３章の手法を（時間的パラメタだけでなく）データ的パラメタをも許容するように拡張した手法を提案している．データ的パラメタの対象となるデータとしては（たとえば口座振り込みの金額などの）有理数値データと（口座振込の宛先などの）文字列データをサポートしており，実行時検証の応用範囲を大きく広げる成果となっている．出願者は，多面体抽象という数学的テクニックのポテンシャルを追求してパラメタ付き時間オートマトンの理論を拡張することにより，このようなパラメタ付き実行時検証を実現している．本章の貢献は，さまざまなデータ型におけるパラメタを許容する汎用性を実現しており，またこれらのパラメタによって第３章と同様に柔軟性と表現能力の向上を実現している.

第５章は本論文の４つの提案手法の３つ目として，形式的仕様の充足度合いを（yes/noの２値でなく）実数を代表例とする半環の元を用いて定量的に表現する実行時検証手法が提案されている．この定量的な実行時検証の問題を効率的に解くために，時間オートマトンの理論を重み付きに拡張し，実行時検証の問題が最短路問題に対応するような理論的枠組みを導入して，その結果として実効的アルゴリズムが得られている．本章の貢献は，形式仕様の定性的な真偽値を定量的な充足度合いに拡張することで表現能力の向上を実現している.また同時に,さまざまな半環に対して適用可能なアルゴリズムを示すことにより，実行時検証の汎用性の向上も実現している.

第６章は本論文の４つの提案手法の４つ目として，過大近似モデルを用いてサンプル間の補完を行う実行時検証手法が提案されている．連続時間シグナルに対する実行時検証においては，実行時検証アルゴリズムへの離散時間入力を生成するためのサンプリングのステップにおいて情報ロスが不可避であるため，もともとの連続時間シグナルに対する解析結果の正当性が保証できない．この方法論的困難に対処するため提案手法では，所与の過大近似モデルを用いてサンプル間の連続時間補完の可能性を限定することで，離散時間サンプルの解析結果を連続時間シグナルに敷衍することを可能にするような実行時検証手法を実現している．この実行時検証手法を可能にする理論的基盤は，線形ハイブリッドオートマトンの理論および，新たに導入する線形ハイブリッドオートマトンの受理言語の概念であり，当該受理言語を計算するアルゴリズムにおいて多面体抽象化が活用されている．本章の貢献は，モデルを用いた精度の良いサンプル間補完を行うことで，疎なサンプリングからも意味のある結論を導出することを可能にするものであり，サンプリング頻度の選び方の柔軟性を実現している．また，仕様にパラメタを含むことも可能であり，このパラメタによって表現能力の向上を実現する.

最後に，第７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査読付き国際会議予稿集のフルペーパー4 篇として発表されている.これらの論文を含めた出願者の出版業績は以下の通りである： 主著者と

なる査読付きジャーナル論文１件，主著者となる査読付きトップ国際会議予稿集フルペーパー3 件（うち１件は前記ジャーナル論文と同一），その他の主著者となる査読付き国際会議予稿集フルペーパー5 件，以上の他に共著者となるトップ国際会議予稿集フルペーパー2 件．

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，実行時検証という物理情報システムの品質保証手法の研究において，多面体抽象化という数学的テクニックの理論的ポテンシャルを時間オートマトンの理論の文脈でさらに深く追求し活用することで，実行時検証手法の実用性・実効性のさらなる向上を図るものである．実際，本論文の４つの貢献は汎用性・柔軟性・表現能力という３つの視点において実行時検証の実効性を大きく向上させるものであり，その学術的価値及び実用上の価値は高いと認められる．審査委員は上記の博士論文の内容および出版業績をもって，出願者が博士課程学生として特に優れた業績を持つと判断した．

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．