様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月 ２０ 日現在

機関番号：１４３０１
研究種目：若手研究(B)
研究期間：2013～2015
課題番号：２５７３００４０

研究課題名（和文）無限小プログラミングによるハイブリッドシステムの形式検証手法

研究課題名（英文）Forma verification of hybrid systems based on the infinitesimal programming

研究代表者
末永　幸平（Suenaga, Kohei）

京都大学・情報学研究科・准教授

研究者番号：７０６３３６９２

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

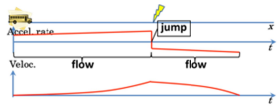
研究成果の概要（和文）：無限小プログラミングに基づくハイブリッドシステム検証手法について研究を行った．ハイブリッドシステム検証手法としては未だ発展途上であるものの，その過程で非線形な不変条件の高速な生成手法という重要な知見が得られた．不変条件生成手法はプログラム検証において検証の成否を握る重要な要素技術であるが，既存の手法は非線形な不変条件を効率よく生成することが難しいことが多く，複雑なシステムの検証に困難が生じていた．本手法では次元解析の手法を用いることで，既存の非線形不変条件生成手法を高速化することが可能となった．研究期間終了後は本手法をさらに発展させ，より複雑なハイブリッドシステム検証手法につなげる予定である．

研究成果の概要（英文）：We investigated a method for verifying hybrid systems based on the idea of the infinitesimal programming. Although the obtained result is yet to scale to practical hybrid systems, as a byproduct, we obtained an efficient nonlinear invariant synthesis algorithm. Invariant synthesis algorithms, which is an important technology in program verification, often cannot be applied to a complex system due to their complexity. Our method makes these algorithms fast using the idea of dimension analysis used in the are of physics. We plan to investigate this idea to an algorithm that can deal with more complex hybrid systems.

研究分野：プログラム検証

キーワード：ハイブリッドシステム　プログラム検証　不変条件　無限小プログラミング　超準解析　次元解析　非線形不変条件　システム検証

１．研究開始当初の背景



自動車や航空機など，以前は力学的・電気的な制御が行われていたシステムにソフトウェアが関わるようになっている．これらのシステムは速度や温度のような物理量を表す連続値の変化（フロー）と，レジスタの値やメモリアドレスのようなソフトウェアの動作に関わる離散値の変化（ジャンプ）とが相互に影響を及ぼしあって動作するハイブリッドシステムとなっており，その点で連続値のみからなる力学・電気系や離散値のみを扱うソフトウェア系とは異なった複雑さを持っている．例えば自動車においては，ブレーキオイルの圧力等の連続値と，カーナビゲーションシステム等のソフトウェアの振る舞いを決定する離散値が時々刻々と変化しながら，自動車全体としての動作を実現している．ハイブリッドシステムの誤動作は人命や財産の莫大な損失に繋がる可能性があり．これらのシステムの安全性を保証することは，自動車産業が盛んな我が国においては特に国内経済や我が国の国際的地位にも関わる重大な問題である．ハイブリッドシステムの品質を向上させるために，現在産業界においてはシミュレーションによるテストが用いられている．これは，様々な入力をシステムに繰り返し与え，その動作が意図した通りであることを確認することでシステムの品質を担保しようとする手法である．しかしながら，テストに基づく品質チェックのみでは (1) 全ての入力を網羅することが不可能であること (2) 入力に対してシステムの振る舞いが一意に定まらない非決定的な振る舞いのチェックが難しいこと等の問題がある．

同様の問題は（ハイブリッドでない）ソフトウェアシステムの開発においても存在し，この問題を解決するためにソフトウェア科学の分野では数理的手法を用いてシステムの品質を「証明」する手法（形式検証手法）が数十年にわたって盛んに研究されている．これら先行研究の成果をハイブリッドシステムに適用できればハイブリッドシステム検証の研究を大きく前進させることが可能となる．しかしながら，これらの手法はジャンプのみによって状態遷移が起こるソフトウェアシステムを対象としており，フローとジャンプを両方とも含むハイブリッドシステムの形式検証にはそのまま適用することはできない．

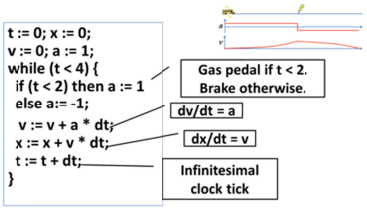
２．研究の目的

本研究の目標は，ハイブリッドシステムの形式検証にソフトウェアの形式検証手法を活用するための枠組みを提供することである．換言すれば，これまでに研究されてきたソフトウェア検証手法を，そのままの形でハイブリッドシステムに適用するための手法が本研究の目標である．

現在提案されているハイブリッドシステムの形式検証手法 [Alur et al. TCS ’95 等] では，フローとジャンプが微分方程式と状態間遷移という異なった方法で記述される．左図にその例を示す．この例では，各状態での x の値の変化が微分方程式を用いて表されている．そのため，ソフトウェアを対象とした既存の形式検証手法（モデル検査や定理証明に基づく手法等）をそのまま適用することができない．本研究では，無限小プログラミングを用いたアイディアで，フローをジャンプとして表現することが可能となる．この利点を生かし，従来ハイブリッドシステムへの適用が難しかったソフトウェア検証手法，特にホーア論理や型理論等の証明システムに基づく検証手法を適用することを目指す．証明システムに基づく検証手法は，検証のためにかかる時間が比較的短い等数々の利点があり，これによりハイブリッドシステムに対する形式検証がさらに有用なものとなると期待される．

３．研究の方法

研究代表者らは本研究以前に無限小プログラミングをハイブリッドシステム検証に健全（検証が成功すれば検証した性質が実行時に必ず成り立つこと）かつ相対完全（論理式として記述できる性質で実行時に成り立つ性質は，無限小で拡張された実数について成り立つ性質を証明する証明器を仮定すれば，必ず検証できること）な形で適用できることを理論的に示した．この結果を実際のハイブリッドシステム検証器につなげることを目指して，本研究ではループ不変条件生成手法の研究を行った．ループ不変条件生成手法は，プログラム検証において一般的に用いられる重要な要素技術であり，プログラム中で常に成り立つ条件で検証すべき性質を証明できる程度に強力な条件を求める手法である．

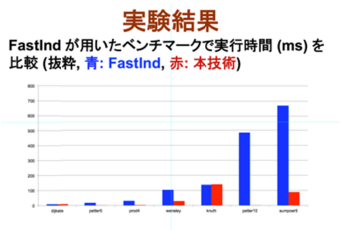


これまでにプログラムを対象としたループ不変条件生成手法はいくつか提案されてはいるものの，その多くはプログラム変数の線形結合で表現される条件のみが扱えるものであった．ハイブリッドシステムを扱うにあたっては非線形性の関わる条件を扱う必要があるために，これらの手法をそのまま適用することは難しいことが分かった．非線形性を含む不変条件を生成できる手法としては [Cachera et al. 2014, Müller-Olm et al. 2004, Rodríguez-Carbonell et al. 2007, Sankaranarayanan et al. 2004] があるが，これらの手法は計算コストが高く，複雑なシステムにスケールさせるのが難しい．そのため，本研究ではこれらの非線形条件が扱える不変条件生成手法を高速化させるための研

究を行った．

上述の非線形性を扱える不変条件生成手法はテンプレート法を用いている．この方法は，未定係数を含む不変条件のテンプレートを生成した上で，このテンプレートが実際に不変条件となるための未定係数上の制約を計算し，制約の解を求める方法である．この手法では，対象とするプログラムが複雑になると，用意すべきテンプレートが巨大となり，不変条件の生成にコストがかかるという問題点がある．

本研究では，プログラムを事前に解析することでテンプレートのサイズを削減する手法を研究した．ハイブリッドシステムはメカ・エレキと呼ばれる物理現象が関わる系を含むシステムである．そのため，生成すべき不変条件は物理的に意味のある量が関わる条件になるべきであると期待される．この直観に基づき本研究では，プログラムに対して次元解析を行う既存手法 [Kennedy 1994] を適用した上で，物理次元の合ったテンプレートのみを生成するように不変条件生成手法を改良した．これにより，物理的に意味のない巨大なテンプレートを生成することを防ぐことができる．



４．研究成果

本研究の手法を実装し，非線形不変条件生成手法のベンチマークで既存手法 [Cachera et al. 2014] と比較した（左図）．従来手法に比して現実的なプログラムにおいて最大 10 倍程度の高速化が達成された．この成果について 2 件の特許出願を行っている．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

[1] 蓮尾 一郎, 末永 幸平. “CPS の形式検証 - 超準解析によるアプローチ” 計測と制御 53-12, pp.1-6.（査読あり）

[2] Takumi Akazaki, Ichiro Hasuo, and Kohei Suenaga. “Input Synthesis for Sampled Data Systems by Program Logic”, EPTCS 174, 2015, pp.22-39.（査読あり）

〔学会発表〕（計 12 件）

[1] Yohei Miyamoto, Kohei Suenaga, and Koji Nakazawa. “A Denotational Semantics of a Probabilistic Stream-Processing Language” Workshop on Probabilistic Programming Semantics (PPS 2016), Jan. 23, 2016. 発表場所: セントピータースバーグ（アメリカ合衆国）（査読あり）

[2] Kohei Sueanga. “Formal Verification of Software, Continuous, and Hybrid Systems - Or: How Do We Verify Our Program is Correct?” Machine Learning Summer School 2015. Aug. 27, 2015. 発表場所:京都大学（京都府京都市）

[3] Kohei Suenaga. “Nonstandard Analysis Meets Programming Language Theory” The 12th International Conference on Computability and Complexity in Analysis (CCA 2015). Jul. 13, 2015. 発表場所: 明治大学（東京都千代田区）

[4] 五十嵐 淳, 中澤 巧爾, 馬谷 誠二, 関山 太朗, 花田 裕一郎, 大元 武, 宮本 洋平, 末永 幸平. “京都大学 Teen Racketeer 養成コース” 第 17 回プログラミングおよびプログラミング言語ワークショップ (PPL 2015), Mar. 4, 2015. 発表場所: 道後プリンスホテル（愛媛県松山市）

[5] 宮本 洋平, 末永 幸平. “確率的動作を含んだストリーム処理言語” 第 17 回プログラミングおよびプログラミング言語ワークショップ (PPL 2015), Mar. 4, 2015. 発表場所: 道後プリンスホテル（愛媛県松山市）

[6] Qi Tan, Kohei Suenaga, and Atsushi Igarashi “A Behavioral Type System for Memory-Leak Freedom” 第 17 回プログラミングおよびプログラミング言語ワークショップ (PPL 2015), Mar. 4, 2015. 発表場所: 道後プリンスホテル（愛媛県松山市）

[7] Tatsuya Sonobe, Kohei Suenaga, and Atsushi Igarashi “Automatic Memory Management Based on Program Transformation Using Ownership” Programming Languages and Systems 12th Asian Symposium (APLAS 2014), Nov. 17, 2014. LNCS 8858, pp.58-77. 発表場所: シンガポール国立大学（シンガポール）

[8] Takumi Akazaki, Ichiro Hasuo, and Kohei Suenaga. “Input Synthesis for Sampled Data Systems by Program Logic, The 4th Workshop on Hybrid Autonomous Systems (HAS 2014), Apr. 12, 2014. 発表場所: グルノーブル（フランス）

[9] Minoru Kinoshita, Kohei Suenaga, and Atsushi Igarashi. “Automatic Synthesis of Combiners in the MapReduce Framework”, 24th International Symposium on Logic-Based Program Synthesis and Transformation, Sep. 9, 2014. 発表場所: カンタベリー（英国）

[10] 樹下 稔, 末永 幸平, 五十嵐 淳. “MapReduce フレームワークにおける Combiner の自動生成” 第 16 回プログラミングおよびプログラミング言語ワークショップ (PPL 2014), Mar. 5, 2014. 発表場所: 阿蘇の司ビラパークホテル（熊本県阿蘇市）

[11] 末永幸平 “Type-Based Safe Resource Deallocation for Shared-Memory Concurrency” 日本ソフトウェア科学会第 30 回大会特別招待講演. 2013 年 9 月 12 日. 発

表場所：東京大学（東京都文京区）
[12] 末永幸平 “形式検証手法は無限小プログラミングを使えばハイブリッドシステムにもそのまま使える”日本ソフトウェア科学会第 30 回大会 Future Technology Design (FTD) 2013. 2013 年 9 月 11 日. 発表場所：東京大学（東京都文京区）

〔産業財産権〕
○出願状況（計 2 件）

[1]
名称：不変条件生成装置，コンピュータプログラム，不変条件精製方法，プログラムコード製造方法
発明者：末永 幸平，樹下 稔，小島 健介.
権利者：京都大学
種類：特許出願
番号：特願 2016-017441
出願年月日：2016 年 2 月 1 日
国内外の別： 国内

[2]
名称：不変条件生成装置，コンピュータプログラム，不変条件生成方法，プログラムコード製造方法
発明者：末永 幸平，樹下 稔，小島 健介.
権利者：京都大学
種類：特許出願
番号：特願 2016-017419
出願年月日：2016 年 2 月 1 日
国内外の別： 国内

○取得状況（計 1 件）

[1]
名称：ハイブリッドシステムの検証方法，検証装置，及び検証コンピュータプログラム，並びに，ハイブリッドシステムのモデル変換方法，変換装置，及び変換コンピュータプログラム
発明者：末永 幸平，蓮尾 一郎
権利者：京都大学
種類：特許権
番号：特許第 5843230 号
取得年月日：2015 年 11 月 27 日
国内外の別： 国内

〔その他〕
ホームページ等
http://www.fos.kuis.kyoto-u.ac.jp/~ksuenaga/

６．研究組織
(1)研究代表者：末永幸平（SUENAGA, Kohei）
京都大学・大学院情報学研究科
通信情報システム専攻・准教授
研究者番号：70633692

以上