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　２７　年　　６　月　　５　日現在

機関番号：　１２６０８
研究種目：　研究活動スタート支援
研究期間：　2013～2014
課題番号：　２５８８０００８

研究課題名（和文）区間制約プログラミングと演繹的推論に基づくハイブリッドシステムの検証技術

研究課題名（英文）Verification Techniques for Hybrid Systems based on Interval Constraint Programming and Deductive Reasoning

研究代表者

石井　大輔（Ishii, Daisuke）

東京工業大学・情報理工学（系）研究科・助教

研究者番号：００４５４０２５

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：連続変化と離散変化の振る舞いをするハイブリッドシステムに対する，安全性や安定性といった性質の検証を，区間制約プログラミングと演繹的推論を用いて実施するための技術を開発した．本研究は，制約概念を軸に，高信頼な数値計算と，数式処理や時相論理式検証などの記号計算とを統合した点を特色とする．非線形算術制約を高速に求解する並列区間制約ソルバーを構築するとともに，本ソルバーを利用したハイブリッドシステムの検証器を構築，既存ツールでは検証が難しかった複数の事例について，提案ツールにより検証可能であることを示した．

研究成果の概要（英文）：We have developed techniques for verifying various properties (e.g., safety and stability) about hybrid systems that involve continuous and discrete behaviors, using interval constraint programming and deductive reasoning. Development of this research is based on the notion of constraints that integrates reliable numerical computation and symbolic computation (e.g., formula manipulation and temporal logic verification). We have built (i) a parallel interval constraint solver that handles efficiently nonlinear arithmetic constraints, and (ii) a verifier for hybrid systems based on the constraint solver. In the experiments, we have shown that several models, which are difficult to handle with existing tools, can be verified with our tools.

研究分野：　ソフトウェア

キーワード：　ハイブリッドシステム　制約プログラミング　区間解析　探索・論理・推論アルゴリズム

１．研究開始当初の背景

(1) 区間制約プログラミング

算術制約プログラミングは，対象を実数変数を持つ等式・不等式制約として記述し，局所制約伝播と探索により効率よく充足解を計算する枠組みである．とくに区間解析に基づく区間制約プログラミングが 1990 年代中頃から仏・ナント大学を中心に発展してきた．区間制約プログラミングは数値計算の精度保証技術を包含する高信頼な非線形連続領域計算の枠組みである．最近の技術開発により，常微分方程式（ODE）制約を扱ったり，パラメタ付き制約のある区間内での妥当性を判定したりすることが可能になりつつある．研究代表者は連続システムおよびハイブリッドシステムの解析に対する区間制約プログラミングの有効性に着目し，平成 18 年度から技術開発に取り組んできた．たとえば，連続システムであるロボットを制約としてモデリングし，制約ソルバーによりロボットの稼働空間を区間計算するとともに，稼働空間中の特異解を同定し（特異性の条件も制約として記述），ロボットの安全な（特異解を含まない）稼働空間を連結した区間集合として計算するという事例がある．

(2) ハイブリッドシステム

時間経過とともに状態が連続変化したり，離散変化したりする系をハイブリッドシステムという．物理現象と計算機を強く結合するサイバーフィジカルシステムの根幹技術として注目を集めている．車載組み込みシステムや計算分子学のモデル等様々な問題がハイブリッドシステムの特徴を持ちつつあり，専用の検証技術が重要になっている．ハイブリッドシステム検証の 2 つのアプローチとして，モデル検査法と演繹的検証法が提案されている．モデル検査法は，対象を離散系からハイブリッドシステムへと拡張し，HyTech [Henzinger ら，1996] をはじめとする多くのツールを実現，実用的な問題に応用されてきた．演繹的検証法は，ハイブリッドシステムを論理式により記述し演繹的推論を行うことで解析する手法だが，近年，ツール KeYmaera [Platzer ら，2008] が提案され，対話的な検証作業が必要という欠点があるものの，モデル検査法では扱えなかったパラメタを含む系や非線形系等，広範なクラスの問題が検証可能であることを示した．研究代表者も演繹的検証法の開発に取り組み，区間制約プログラミングや数式処理による演繹的検証法の開発に貢献してきた．

２．研究の目的

本研究は，広範なクラス(例：非線形連続変化・大規模)の連続システムおよびハイブリッドシステムの高信頼な解析（例：安全性・安定性検証）を可能とすることを目標に，(1) 区間制約プログラミングと (2) 演繹的推論手法を用いた検証技術に，理論・実装の両面から取り組む．区間計算および探索による高信頼・効率的な制約求解技術と，解析学や計算科学の公理系に基づく演繹的推論技術とを統合し，検証可能な問題クラスの拡大と実用的ツールの提供を目指す．より具体的には下記項目に取り組む．

(1) 並列区間制約ソルバーの設計・実装

ハイブリッドシステム検証への応用を見据え，非線形算術制約を高信頼かつ効率よく求解する制約ソルバーの設計・実装を行う．最近の研究成果を踏まえ，下記機能のサポートを検討しながら基本設計を行った上で実装に取り組む:

- ODE 制約，不等式制約，パラメタ付き制約の求解
- 平行体計算に基づくラッピングエフェクト抑制
- 計算結果の区間集合中の連結成分の同定

また並列分散環境（例：東京工業大学 TSUBAME2.5）を想定し，効率的な並列求解アルゴリズム・ヒューリスティックを設計・実装する．

(2) 区間制約ソルバーと演繹的推論手法を連携したハイブリッドシステム検証器の開発

ハイブリッドシステムを逐次プログラムに変換，プログラム検証手法を適用して制約式を生成したり，検証したい性質から境界条件を制約式として抽出した後，区間制約ソルバーで制約式を求解することにより検証を実施するツールを開発する．とくに非線形算術制約で記述されるハイブリッドシステムを扱うことと，検証プロセスの全自動化を目指し，下記機能の研究に取り組む:

- ハイブリッドオートマトンの制約式へのエンコード
- ハイブリッドシステムの振る舞いに関する時相制約の検証
- 検証で必要となるループ不変条件の生成

また並行して，効率化のためのヒューリスティック蓄積，検証事例の蓄積，統合環境の開発等も行う．

３．研究の方法

(1) 2013 年度の実施内容

各要素技術の課題解決・確立を目指し，以下の研究を実施した．

① 区間制約プログラミングによるハイブリッドシステムのシミュレーション：非線形ハイブリッドオートマトンの到達領域を平行体により近似計算する方法を開発した．本方法では，連続変化の計算を区間 ODE 求解ライブラリ CAPD を用いて行い，離散変化を区間を拡張した平行体の計算に基づく独自の方法で行った．本方法によ

り,離散変化の計算におけるハイブリッドシステム特有のラッピングエフェクトを除去し,長いシミュレーション時間にわたる軌道を計算する方法を検討した.

② 区間制約ソルバーによる並列ロボットのアスペクト解析: 並列ロボットの機構をパラメタ付き算術制約で記述し,区間制約ソルバーを用いて,その到達範囲を計算,到達範囲中からアスペクトと呼ばれる部分集合を列挙する手法を開発してきた.本年度はこの手法を拡張し,アスペクトの数の下限を保証することを可能にした.

③ 区間制約ソルバーの並列化: 逐次ソルバーRealpaverを拡張し,並列処理を可能にした. Realpaver の主アルゴリズム部をX10 言語を用いて並列化することで実 施した. 実装にあたっては,求解ワーカ間の効率的・スケーラブルなワークスティーリング方法や求解処理の終了判定方法等を検討し,高速化を図った.並列ソルバーに関して,共有メモリマシンと大規模クラスタ(東京工業大学 TSUBAME2.5)の上でベンチマーク問題を解いて性能評価を行った.

④ 数式処理に基づくハイブリッドシステムの演繹的検証: ハイブリッドオートマトンの安全性検証問題を,擬似的なアノテーション付き逐次プログラムの検証問題に変換し,最強事後条件を求めることで算術制約式に変換する方法を検討した.変換した算術制約式を数式処理系 Mathematicaを用いて妥当性判定することにより,元の検証問題を判定する方法を検討した.

(2) 2014 年度の実施内容

区間制約ソルバーの保守・改良を行うとともに,区間制約プログラミングと記号処理を統合したハイブリッドオートマトンの検 証器の開発を行った.

① 区間制約プログラミングに基づくハイブリッドオートマトンに対する有界時相制約の検証: 前年度の区間シミュレーション手法を利用し,ハイブリッドオートマトンの有限長の軌道について有界時相論理式の充足性を判定する手法を開発した.さらに本手法を利用し,統計的モデル検査を実施する手法を検討した.

② 並列区間制約ソルバーの実装: 前年度の実装作業を継続し,平行体計算・パラメタ付き制約・微分方程式制約等をサポートする区間制約ソルバーの拡張実装を整備し,保守性を高めた.また並列ソルバー実装において, X10の大域負荷分散ライブラリを使用するように変更し,コードを簡略化するとともに負荷分散の効率化を図った.

４．研究成果

本研究では,(1) 区間制約プログラミングと,(2) 数式処理・演繹的推論とに基づき,連続システムおよびハイブリッドシステムの検証技術群を開発した.これらの検証技術群により,非線形算術制約で記述されるシステムやパラメタを含むシステム等,既存技術で扱えなかったシステムに対する検証が可能になった.また (1) に基づく検証技術では,時相論理式で記述される広範な性質を厳密に検証することを可能にした.

(1) 区間制約プログラミング

①区間制約プログラミングによるハイブリッドオートマトンのシミュレーション

非線形 ODE や非線形不等式で記述される非線形ハイブリッドオートマトンの振る舞い(軌道)をシミュレーションする方法を開発した.提案した方法は,軌道を計算誤差とともに平行体の集合で包む形で計算を行うため,高信頼である.また区間ベクトル (矩形) の代わりに平行体を用いたため,シミュレーションにともない矩形の大きさが増大するラッピングエフェクトを抑え,長いシミュレーション時間にわたって軌道を計算することを可能にした.

提案した方法を CAPD ライブラリを用いて C/C++と OCaml で実装した.あるモデルに対する実験では,矩形を用いたシミュレーションでは数十回の離散変化しか計算できないのに対し,平行体を用いることで 10,000 回以上の離散変化がシミュレーション可能になることを示した.

②区間に基づく有界時相制約の検証

①の方法を用いて計算した非線形ハイブリッドオートマトン有限長の軌道について,有界時相論理式の充足性を判定する手法を開発した.ただし,提案手法は区間解析の手法を用いて結果の正しさを検証するプロセスを含み,この検証プロセスがうまくいかない場合には充足性の判定をしない.この制限を設けたことにより,非線形ハイブリッドオートマトン一般について効率よく(部分的な)検証を実施することを可能にした.

さらに本手法を用いて統計的モデル検査を実施する実験を行い,数値シミュレーションを用いる場合に較べて高信頼な結果が得られることを示した.

③区間制約ソルバーの大規模並列化

連続システムの検証のための要素技術となる区間制約ソルバーRealpaver をプロセスレベルで並列化する手法を開発した.提案手法ではマルチコアマシンの各コアに求解ワーカを配置し,ワーカ同士が自律的に探索木を分散しながら,求解を行う.並列ソルバーを X10 言語と GLB ライブラリを用いて実装し,スーパーコンピュータ TSUBAME2.5 の 50 ノード・600 コア上で実験したところ,最大 516

倍の実行速度向上が得られた.

④区間制約ソルバーによる並列ロボットのアスペクト解析
並列ロボットの稼働空間中のアスペクトを列挙する区間手法において，アスペクトの数の下限を証明する方法を開発した．提案方法では，アスペクトの内部近似であることが保証された矩形集合を同定し，内部近似の数に基づき証明を行う．実験では，既存手法では解析できなったモデルのアスペクト数の下限値を証明することができた.

(2) 数式処理に基づくハイブリッドオートマトンの演繹的検証
パラメタ化されたハイブリッドオートマトンの安全性を算術制約にエンコードし，数式処理系 (Mathematica) を用いて検証する手法を開発した．提案したエンコード手法ではハイブリッドオートマトンの振る舞いがループ構造を持つことを想定しており，ループ長や不変条件を一部手動で設定する必要があるものの，既存ツールでは扱えなかった問題が検証可能であることを実験により示した.

(3) 研究の特色
本研究は，算術・区間制約プログラミングを軸として推進する点を特色とする.
ハイブリッドシステム検証において，連続状態をとる振る舞いを高信頼に計算する方法が重要となるが，既存技術は，(a) 数値的に変数領域を保守的近似する手法 (例: 既存ツール Flow*, SpaceEx) と，(b) 記号的に変数領域を簡略化・抽象化する手法 (例: 既存ツール KeYmaera) との 2 つに分類できる．これまで既存ツールにおいて (a) と (b) は別々に用いられていた.
これに対し，本研究では制約概念を介し，両者を統一的に扱うことを目指した．本研究の (1) 区間制約プログラミングに基づく検証技術では，計算結果が区間 (あるいは平行体) で表されるが，これは単なる保守的近似ではなく，区間解析による検証プロセスの結果を属性として付与することができる．たとえば，区間中にパラメタ変数がとる各値に関する解が唯一含まれる，といった付加的な属性を付与することができる．②の時相論理式の検証方法では，このような属性を利用している．また将来的には，(2) の演繹的推論の枠組みにおける付加的属性の利用を促進し，より発展的なハイブリッドシステム検証が可能になると考えている.
ハイブリッドシステムの自動検証は困難な問題である．本研究における実験では，検証の網羅性や検証プロセスの自動化を一部犠牲にすることで，複雑な算術制約で記述されたり，不定なパラメタを含んでいたりするシステムに対する (部分的な) 検証が可能になり，形式手法の成果が現実的な問題に応用可能であることを示した.

(4) 研究の意義
本研究は区間計算，探索アルゴリズム，制約プログラミング，並列プログラミング，プログラム検証といった複数分野の境界領域に位置付けられる問題の定式化および求 解ツールを提案し,各分野の相互交流を 促進するという意義を持つ.また応用分野である制御工学,生物学,ロボティクス等の各分野に対して情報科学に基づく最新のツールや知見を提供するという意義を持つ.

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 石井大輔，上田和紀．非線形ハイブリッドシステムの可到達集合の精度保証．計測と制御，Vol.53，No.12，pp.1086-1092，2014．(査読有，解説論文)
http://www.sice.or.jp/org/journal/moku53-12.html
② S. Caro, D. Chablat, A. Goldsztejn, D. Ishii, C. Jermann. A branch and prune algorithm for the computation of generalized aspects of parallel robots. Artificial Intelligence, Vol.211, pp.34-50, 2014. (査読有)
DOI: 10.1016/j.artint.2014.02.001

〔学会発表〕（計 6 件）

① 石井大輔，米崎直樹．区間解析を用いたハイブリッドシステムの統計的モデル検査．電子情報通信学会 ソフトウェアサイエンス研究会 (SS2014-44), Vol. 114, pp.67-71, 2015 年 1 月 27 日，ブランナールみささ (鳥取県・三朝温泉).
② D. Ishii, K. Yoshizoe, T. Suzumura. Scalable Parallel Numerical CSP Solver. In 20th International Conference on Principles and Practice of Constraint Programming (CP), LNCS 8656, pp.398-406, 2014 年 9 月 11 日，リヨン (フランス). (査読有)
DOI: 10.1007/978-3-319-10428-7_30
③ 石井大輔，A. Goldsztejn. 平行体計算を用いた非線形ハイブリッドシステムのシミュレーション．電子情報通信学会 システム数理と応用研究会 (MSS2013-74), pp.135-139, 2014 年 1 月 31 日，豊田中央研究所 (愛知県・長久手市). (MSS 優秀論文賞)
④ 石井大輔，鈴村豊太郎．PGAS 言語 X10 による数値制約充足問題ソルバー Realpaver の並列化．第 141 回ハイパフォーマンスコンピューティング研究発

表会，No. 10，2013 年 10 月 1 日，沖縄産業支援センター（沖縄県・那覇）.

⑤ 石井大輔，G. Melquiond，中島 震．最強事後条件の計算を用いたハイブリッドオートマトンの帰納的検証．日本ソフトウェア科学会第 30 回大会，2013 年 9 月 12 日，東京大学（東京都・本郷）.（高橋奨励賞）

⑥ D. Ishii，G. Melquiond，S. Nakajima. Inductive Verification of Hybrid Automata with Strongest Postcondition Calculus. In 10th International Conference on integrated Formal Methods (iFM)，LNCS 7940，pp. 139-153，2013 年 6 月 12 日，トゥルク（フィンランド）.（査読有）
DOI: 10.1007/978-3-642-38613-8_10

６．研究組織

(1)研究代表者

石井 大輔（ISHII，Daisuke）
東京工業大学，大学院理工学研究科，助教
研究者番号：000454025

(2)研究分担者

なし

(3)連携研究者

なし