様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ５ 月 ２９ 日現在

機関番号：１３３０２
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ１１２４０

研究課題名（和文）大規模・複雑なハイブリッドシステムのための区間制約プログラミング技術

研究課題名（英文）Interval constraint programming techniques for large and complex hybrid systems

研究代表者
石井　大輔（Ishii, Daisuke）

北陸先端科学技術大学院大学・先端科学技術研究科・准教授

研究者番号：００４５４０２５

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：連続離散ハイブリッドシステム（HS）のための制約プログラミング技術を開発することを目指し，大規模・複雑な組込みシステムをモデリングしたHSに対し，高信頼かつ有用な解析を実施する手法・ツールに関する研究を実施した．制約プログラミング技術に基づき，安全性のモデル検査や目的関数の最適化をする手法・ツールを提案した．提案手法は，SimulinkおよびAcumenで記述したHSを，実数，浮動小数点数，区間等の領域の変数をもつ制約へと符号化し，ソルバーによる解析を行う．産業界由来のモデルによる実験により，提案手法の性能と有用性を確認するとともに，基本手法・実装については正しさの形式的検証を実施した．

研究成果の学術的意義や社会的意義
学術的意義として，一般的には扱うのが難しい大規模複雑なハイブリッドシステムを解析する手法の開発に取り組み，その効果を示す実験結果を得たことが挙げられる．有用な実例を検査するため，制約への符号化法，部品や繰り返しを考慮した検査法，モンテカルロ法との連携，大規模並列化，提案手法の実装技術等，複数の面について研究した．また，手法・実装自体の検証に取り組み，形式手法の研究過程の機械化・高信頼化を進めた意義がある．
社会的意義として，提案手法を実世界で稼働するシステムに対して適用し，そのモデルの安全性検査等に役立てられることが挙げられる．

研究成果の概要（英文）：To develop constraint programming techniques for discrete/continuous hybrid systems (HS), we have conducted a research on methods and tools for reliable and practical analyses on HS that models large-scale and complex embedded systems. The proposed methods include a safety model checker and an optimizer of objective functions based on constraint programming techniques. The proposed methods encode HS described with Simulink and Acumen into constraints involving variables in the domains of reals, floating-point numbers, intervals, etc., and then analyze them using solvers. We have confirmed the performance and effectiveness of the proposed methods by the experiment with industrial model examples. We have also performed a formal verification of the correctness of the basic methods and implementations.

研究分野：計算機ソフトウェア

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

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

１．研究開始当初の背景

車載組込みシステム等，物理系と情報系が結合したサイバーフィジカルシステム （cyber-physical systems, CPS）が普及し，その安全性保証が重要になっている．CPS の開発では，計算機上でシミュレーション可能なモデルを用意し，プロトタイピング等の効率化を図りながら進めることが多い.検証の工程では,モデル･実装両方について安全性を確認するのが望ましい.

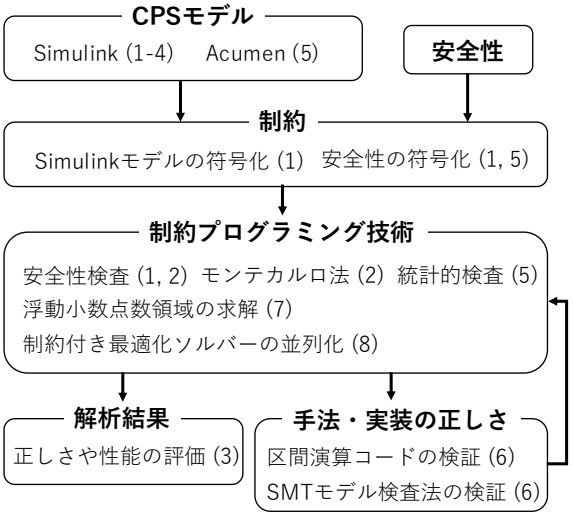
連続離散ハイブリッドシステム （hybrid systems, HS）は，時間とともに状態が連続変化したり，離散変化したりする系である．CPS を HS としてモデリングし，安全性を解析 （モデル検査）するための形式手法が多数研究されてきた．しかし，既存手法が扱える対象は部分的なものであり，モデルが非線形制約で記述されたり，階層的な部品で構成されたりするような，大規模複雑なシステムを扱う方法は自明でない.一般の HS を自動検証することは原理的に難しいため，複数の手法を部分的に適用し，現実的なシステムを検証する手法が求められている．

制約プログラミングは，ある領域の変数に関する制約を記述し，ソルバーと呼ばれるソフトウェアによりその充足解や最適解を求めるための枠組みである．実数領域や実数信号領域等の問題を，探索や数理解析に基づき効率よく扱うソルバーが開発されている．たとえば，述語論理式の充足性を判定する SMT（satisfiability modulo theories）ソルバーや，制約集合の元で目的関数の極値を求める制約付き最適化ソルバーがある．また，形式手法の分野では，検査対象モデルを制約の記述に符号化し，ソルバーを用いた充足性判定により，モデル検査を実施する手法が開発されてきた．しかし，制約の記述性やソルバーの性能には限界があり，現実的な検査対象を適切に符号化する手法や，制約を効率よく求解する手法に課題がある．

２．研究の目的

本研究の目的は，HS のための制約プログラミング技術を開発することである．とくに，現実的，大規模，複雑な CPS をモデル化した HS に対し，高信頼かつ有用な検査が実施可能な，制約ソルバーを用いた手法・ツールを提供することを目指す．そのような CPS を直接的にモデリング・解析することは困難なため，モデルの部品化や抽象化により，扱うモデル記述・振る舞いを限定する．既存の HS モデリング言語を対象とし，モデルから制約への符号化法と，大規模複雑な CPS 由来の制約が扱えるソルバーの開発に取り組む.CPS のモデルで重要となる,実数,整数,機械表現した数値，実数区間，真理値，時間関数（信号）等のドメインの制約プログラミングに注力する．さらに，提案手法・ツールを実際の車載システムモデルに適用することを目指す.

３．研究の方法



本研究では，CPS モデルとその安全性について，制約の記述に変換（符号化）し，変換後の制約をソルバーで解析することにより，検証を実施する手法を開発する．右図に示すように，制約プログラミング技術（制約ソルバー）を中心に研究を実施した（図中の数字は 4 節で述べる研究項目を表す）．CPS モデルとその安全性を制約に符号化する技術に関する研究項目，提案手法を CPS モデル例に適用することによる解析結果の正しさや性能を評価する研究項目，手法や実装を形式的に検証する研究項目に取り組んだ.

CPS モデルとしては,Simulink と Acumen で記述されたものを対象とし,安全性の検査や,網羅テストを検討した.

CPS のモデルや安全性の記述に必要な制約セットを明らかにするため，諸問題を制約に符号化する手法について研究した．Simulink の安全性検査について，述語論理式に符号化する手法を開発した．また，安全性のモニターを Acumen プログラム中に埋め込む方法を提案した.

制約プログラミング技術として,安全性を検査するための複数手法について研究した.おもに,SMT ソルバーを利用する手法，統計的な手法，両者のハイブリッド手法を開発した．数値計算を精密に検証するための技術として，浮動小数点数領域の制約を求解する手法を開発した．また，制約付き最適化問題の大規模並列化ソルバーの開発にも取り組んだ.

技術開発の結果については，提案手法による解析結果に対する実験的な評価と，使用する手

法・実装の正しさを保証するための形式的な検証に取り組んだ．この検証においても制約プログラミング技術を用い，再帰的な形で研究を実施した．

４．研究成果

以下，研究成果を研究項目別に順次説明する．

(1) Simulink モデルの SMT ソルバーを用いた検査

MATLAB/Simulink は CPS を HS としてモデリングするためのツールである （本研究では離散時間モデルを扱った）．学術界・産業界で広く利用されている．MathWorks 社が提供する商用ツールである．Simulink は，モデルをブロック線図の形で記述するためのグラフィカル言語と，モデルの実行結果を信号として求める数値シミュレーターを提供する．Simulink モデルは CPS の仕様書やプロトタイプの役割をもつため，その内容の形式的な検査が重要である．しかし，開発現場では標準ツールの SLDV （SimuLink Design Verifier） を用いることが多く，検査のスケーラビリティや，ブラックボックスツールゆえに検査内容が説明不足になる等の課題がある．本研究項目では，Simulink モデルに対して安全性を検査する手法について研究した．これにより，産業界で作成されるような Simulink モデルを適切かつ効率よく検査する手法を明らかにすることができたと考えている．既存の Simulink モデル検査の研究と比較して，より広範なモデルを対象とし，かつ精密な解析をすることを可能にした．提案手法は，モデルと安全性を制約（述語論理式）に符号化し，SMT ソルバー （既存の Z3 を利用） で解くことにより静的に検査を実施する．以下，符号化手法と検査手法に関する研究内容について述べる．

【符号化手法】Simulink モデルを述語論理式の記述に符号化する手法を設計し，MATLAB スクリプトとして実装した．符号化では，Simulink の各ブロックを入力値から出力値への関数として定義し，関数呼び出しを適切に構成することにより，実行結果の信号を論理式の形で表現する．Simulink が扱う入出力値はおもに浮動小数点数，固定小数点数，整数だが，これらを数学的な実数・整数に近似して符号化する手法と，ビット列表現により精密に符号化する手法をそれぞれ開発した．

符号化では，Simulink が提供する多様なブロック型とブロック結線方法に対応する必要がある．本研究では，38 種類のブロック型，多様な連結構造に対応し，複合レートシステムや複合信号を扱うことを可能にした．モデルが含むサブシステムを抽象化したり，安全性と関連するモデル記述をスライシングしたりする方法も開発した．

精密符号化法は，SMT ソルバーが提供するビット列および浮動小数点数の理論を用いて実現した．実装では論理式のプリント機能を部品化し，近似法と精密法を容易に切り替えられるようにした．また，区間解析に基づき状態を抽象化しながら符号化する手法も検討し，効果を実験的に確かめた．ただし本機能の符号化器への組込みは今後の課題である．

研究項目 (3) において，産業的な例を含む複数の Simulink モデルについて，符号化器が正しく動作することを確認した．

【検査手法】符号化手法を利用し，有界検査と k-induction による不変性検査を実施する手法を設計・実装した．多様なモデルを効率よく扱うための複数の方法を検討した．たとえば，検査対象となるブロックを含むサブシステムのみを検査したり，一部のサブシステムを抽象化し検査したりする機能を開発した．提案手法は，検査中，対象となるサブシステム階層数と信号の長さを調整しながら，符号化を繰り返し実施する．階層数と信号長を反復深化させて検査する方法を検討した．また，検査する性質が複数ある場合に，効率よく連続検査する方法を検討した．

研究項目 (3) において，検査手法の動作検証と，SLDV との性能比較をする実験をした．

(2) Simulink モデルの自動網羅テスト

MathWorks 社が定める Simulink のブロック型に応じたテスト基準に基づき，テスト用の入力信号を生成する手法について研究した．また，あるテスト項目を達成するテスト信号が存在しない場合には，デッドロジックである旨を出力する．産業界で作成した Simulink モデルを品質保証するため，このようなテスト基準に基づいた網羅テストが重要になっているが，(1) と同様にテストの効率性や結果の透明性が課題である．とくに，実行時間や計算的な難しさに起因し，テスト項目が未判定のまま残ってしまうという問題が生じている．そこで本研究では，効率よく高い達成率の網羅テストを可能にすることを目指した．とくに，(1) の SMT モデル検査法を用いた手法 （SMT 法） と，SMT モデル検査法とモンテカルロ法を連携した手法 （ハイブリッド法） に取り組んだ．学術的には，SMT ソルバーや統計的テスト手法の開発により，自動検証技術の適用範囲が広がっている一方，産業的 Simulink モデルへの適用事例は多くなく，どの程度扱えるかは自明でないため，実験により有効性を示した本研究は価値が高いと考えている．

SMT 法は，Simulink モデルからテスト項目のリストを抽出し，モデルと各テスト項目を制約の

記述に符号化し,SMT ソルバーを用いて検査を繰り返し実施する.その際,(1) で述べたように,徐々に検査パラメータを増加しつつテスト項目を列挙するようにして効率化を図った.

ハイブリッド法は,モンテカルロ法による入力信号の乱択と,SMT 法による静的解析を組み合わせた手法である.最初に達成テスト項目数がある程度飽和するまで前者を実施し,残ったテスト項目を SMT 法で処理する手法を提案した.前者はデッドロジック判定ができないため,後者が判定する.多様なモデルに対して効果的な両手法の切り替え条件を実験的に求めた.大規模な Simulink モデルを扱うため,数値シミュレーションで得たパス制約を用いてテストケース生成を効率化する手法も検討した.

SMT 法とハイブリッド法を MATLAB スクリプトとして実装し ((1) と合わせて約 10,000 行),(3) の実験により評価した.

(3) (1)と(2)の提案手法の評価実験

(1)と(2)の手法について,検査・テスト結果の正しさと性能を評価するため,実験を行った.大規模複雑で多様な Simulink モデルの例として,人工的モデルと産業的モデルを約 15 例収集した.手法 (1) について,各モデルについて複数の安全性を用意し,証明・反証する実験を実施した.手法 (2) について,各モデルが含むテスト項目に基づいた網羅テストの実験を実施した.また,それぞれの実験において,既存ツール SLDV との比較実験を実施した.実験結果では,提案した 2 手法が用意した問題に対して正しく動作することと,実行時間,検証可能な安全性の数,テスト網羅度について,SLDV と比較して良好な性能が得られることがわかった.用意した問題セットにおいて,(1) の手法が多数のテスト生成・デッドロジック判定に成功し,(2) の手法が高い網羅率を多く達成した.また,提案手法の検証過程が検査パラメータにより説明できる点や,一部の問題において SLDV が近似手法を用いるのに対し,提案手法は厳密な検証ができ,有利であることがわかった.

(4) Simulink モデルの部品化検証

一般に形式検証では,状態爆発や符号化した制約充足問題の計算的複雑さにより,扱える問題サイズに限界がある.そこで,サイズを抑えた部品に問題を分割し,部品ごとに検証を実施するのが常套手段である.一方で Simulink モデルを部品化検証する研究事例は多くなく,とくに広範なモデルを自動的に扱う手法は確立していない.本研究では,大規模複雑な Simulink モデルをサブシステム構造に基づき部品化して安全性を検査する手法を検討した.提案手法では,検証者が部品として扱うべきサブシステムを指定し,部品ごとに SMT モデル検査を実施する.部品の検査結果からシステム全体に関する結果を推論する手法を検討した.推論規則として,既存の部品化検証の規則の他,動作レートを変換する規則と,境界条件を設定し,実行パスを分割するための規則を提案し,用いた.推論の妥当性は SMT ソルバーで確認することができる.提案手法を既存手法で扱えない複数の例題に適用したところ,検査が可能となることが確認できた.

(5) Acumen ツールを用いた統計的モデル検査

Taha らが開発した Acumen は,HS のモデリング言語と,モデリングとシミュレーションを GUI 上で実施可能なツールからなる.Acumen はモデル検査機能を提供していない.また,Simulink 同様の近似的な数値シミュレーション機能の他,区間解析に基づく精度保証付きシミュレーション機能を提供するが,当該機能は開発途上である.本研究項目では,Acumen に対して 2 つの研究を実施した.

まず,Acumen に統計的モデル検査機能の追加を行った.提案手法では,検査する時相論理式のモニターを Acumen 言語で記述し,モンテカルロ法と仮説検定法により,統計的モデル検査を行う.Acumen ツールを拡張する形で提案手法を実装した.これにより,Acumen の GUI 上で,高水準言語によるモデリング,仕様記述,検証,結果の解析を連続的に実施することが可能になった.これらの作業を実施する複数例を用意し,有用性を確認した.

つぎに, OCaml 言語により Acumen 言語の処理系の実装を行った.本実装は,Acumen の形式的な意味論に基づいており,標準の処理系に比べて高信頼な実装といえる.実装は区間演算に基づいており,モデルの到達領域を精度保証付きで計算する.

(6) 区間演算プログラムと SMT モデル検査法の検証

制約プログラミング技術の高信頼実装のためのプログラム検証技術に取り組んだ.高信頼数値計算のための区間演算コード (四則演算や累乗) と,制約に基づく SMT モデル検査法につい

て，プログラム検証を実施した．これらの対象をプログラム検証したのは初の事例といえる．

区間演算は，精度保証付き数値計算の基本的な手続きであり，真解を含む区間値として実数式を評価する．区間演算では，引数区間値の場合分けや，浮動小数点数の丸め制御や特別値の扱いにより，区間演算コードは複雑化し，その正しさは自明でない．本項目では，四則演算とべき乗の区間演算コードについて，演算結果の区間値が健全であること，tight であること，0 除算を検出していること等を検証した．検証には検証ツール Why3 を用いた（複数の SMT ソルバーや証明支援系 Coq をプラグインとして含む)．コードに事後条件，アサーション，補助定理を付与し，検証を可能にした．また，一部のアサーションと補助定理は Coq により対話的に証明した．一部の区間演算に関する性質を検証するのに，当該性質の変数領域を実数としたものを合わせて検証することが有用である等の知見が得られた．

SMT モデル検査法は，述語論理式への符号化と，SAT/SMT ソルバーによる充足性判定により，状態遷移系の安全性を検査する手法である．(1) では Simulink への応用を研究した．さまざまな符号化方法や検査方法が提案されており，方法自体とその実装について正しさを機械的に検証するのが望ましい．本項目では，k-induction 法，IC3/PDR 法等を証明支援系 Coq 上で形式化し，手法の健全性の証明を形式的に記述した．証明のために状態遷移系とその実行パスに関する諸定理を形式化した．また，当該手法を Coq のタクティックとして用いる手法を併せて提案した．

(7) 浮動小数点数領域の制約（SMT）ソルバー

浮動小数点数（FP 数）を変数とする制約充足問題に関し，実数を変数とする制約に変換し，既存の SMT ソルバーを用いて求解する手法について研究した．最新の SMT ソルバーの多くは FP 数演算の理論をサポートするものの，ビット列理論に基づき求解しており，求解中にビット変数が多数生成されてしまう等により，求解性能に課題がある．本研究では実数理論に基づくアプローチを提案した．提案手法は FP 数を実数区間で保守的に近似する変換を施し，実数ソルバーにより近似的に求解を行う．2 種類の変換による求解プロセスを並列実行することにより，SAT・UNSAT 両方の場合を扱うことができる．ただし，判定に詳細な数値誤差が関わる場合は扱えない制限がある．Python 言語により変換器と，既存のソルバーZ3 と CVC4 により求解するスクリプトを実装した．ベンチマーク問題集を用いた実験を行い，提案手法が効果的であることを確かめた．とくに，丸め方向を変数とした問題について，FP 数理論を備える既存ソルバーよりも効率よく解くことができた．

(8) 制約付き最適化ソルバー

実数変数を含む制約付き最適化問題は，ロボットの制御や CPS の検証等において有用である．非線形制約と数値領域を扱う最適化ソルバーは計算量が大きく，また大規模並列化した既存研究はないため，効果を示すことができれば有益である．本研究項目では，制約および目的関数が非線形式で記述される問題を，区間解析と探索に基づき求解する手法を検討し，その求解プロセスを大規模並列化するための技術を開発した．とくに，PC クラスタ上で負荷分散と暫定最適解の分散とを両立させるための技術を検討した．最小解の上界を区間で近似する方法，暫定的な近似解を並列ワーカー間で共有，探索空間の枝刈りに役立てる方法等について研究を実施した．提案手法を X10 言語と C++言語により実装した．探索の負荷分散は，同形のワーカー間で大域的に負荷分散する既存の実装に基づくが，その上に暫定解を伝播する機構を導入し，ライブラリとして実装した．既存の木構造に基づくベンチマーク問題について性能評価実験を行ない，784 コア使用時に 429-824 倍の速度向上を達成した．

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　7件／うち国際共著　2件／うちオープンアクセス　1件）

１．著者名 Daisuke Ishii, Tomohito Yabu	４．巻 377
２．論文標題 Computer-assisted verification of four interval arithmetic operators	５．発行年 2020年
３．雑誌名 Journal of Computational and Applied Mathematics	６．最初と最後の頁 1～13
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.cam.2020.112893	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takashi Tomita, Daisuke Ishii, Toru Murakami, Shigeki Takeuchi, Toshiaki Aoki	４．巻 E103.A
２．論文標題 Template-Based Monte-Carlo Test-Suite Generation for Large and Complex Simulink Models	５．発行年 2020年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 451～461
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2019MAP0010	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Daisuke Ishii, Takashi Tomita, Toshiaki Aoki	４．巻 13260
２．論文標題 Approximate Translation from Floating-Point to Real-Interval Arithmetic	５．発行年 2022年
３．雑誌名 Proc. NASA Formal Methods	６．最初と最後の頁 733～751
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-06773-0_39	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Ishii Daisuke, Tomita Takashi, Aoki Toshiaki, Ngo The Quyen, Do Thi Bich Ngoc, Takai Hideaki	４．巻 13478
２．論文標題 SMT-Based Model Checking of Industrial Simulink Models	５．発行年 2022年
３．雑誌名 Proc. 23rd International Conference on Formal Engineering Methods (ICFEM)	６．最初と最後の頁 156～172
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-17244-1_10	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Ishii Daisuke, Tomita Takashi, Aoki Toshiaki, Ngo The Quyen, Do Thi Bich Ngoc, Takai Hideaki	4．巻 －
2．論文標題 Coverage Testing of Industrial Simulink Models using Monte-Carlo and SMT-Based Methods	5．発行年 2022年
3．雑誌名 Proc. 22nd International Conference on Software Quality, Reliability and Security (QRS)	6．最初と最後の頁 422～433
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/QRS57517.2022.00050	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Daisuke Ishii, Saito Fujii	4．巻 －
2．論文標題 Formalizing the Soundness of the Encoding Methods of SAT-based Model Checking	5．発行年 2020年
3．雑誌名 Proc. International Symposium on Theoretical Aspects of Software Engineering (TASE)	6．最初と最後の頁 105～112
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TASE49443.2020.00023	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Takashi Tomita, Daisuke Ishii, Toru Murakami, Shigeki Takeuchi, Toshiaki Aoki	4．巻 －
2．論文標題 A scalable Monte-Carlo test-case generation tool for large and complex simulink models	5．発行年 2019年
3．雑誌名 Proc. International Workshop on Modelling in Software Engineerings (MiSE)	6．最初と最後の頁 39～46
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/MiSE.2019.00014	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計14件（うち招待講演　1件／うち国際学会　1件）

1．発表者名 八田 竜起,石井 大輔
2．発表標題 SMTソルバを用いたSimulinkモデルのテストケース生成
3．学会等名 情報処理学会全国大会
4．発表年 2020年

１．発表者名
野村 亮太，石井 大輔

２．発表標題
区間制約ソルバにおけるパラメータ化制約の導入

３．学会等名
情報処理学会全国大会

４．発表年
2020年

１．発表者名
村上 涼星，薮 智仁，石井 大輔

２．発表標題
Why3を用いた区間べき関数のプログラム検証

３．学会等名
日本ソフトウェア科学会第36回大会

４．発表年
2019年

１．発表者名
石井大輔，野村亮太，八田竜起，冨田 尭，青木利晃

２．発表標題
区間解析法とモンテカルロ法の連携によるSimulinkテストケースの自動生成

３．学会等名
日本ソフトウェア科学会第35回大会

４．発表年
2018年

１．発表者名
冨田 尭，石井大輔，村上 徹，竹内成樹，青木利晃

２．発表標題
大規模複雑SimulinkモデルのためのMonte-Carlo最適化に基づいたテスト自動生成ツール

３．学会等名
組込みシステムシンポジウム

４．発表年
2018年

１．発表者名
Tomohito Yabu, Daisuke Ishii

２．発表標題
Machine-Aided Verification of Four Interval Arithmetic Operators

３．学会等名
International Symposium on Scientific Computing, Computer Arithmetic, and Verified Numerical Computations (SCAN)（国際学会）

４．発表年
2018年

１．発表者名
石井大輔, 藪 智仁

２．発表標題
Why3を用いた区間演算ライブラリの検証

３．学会等名
第2回 精度保証付き数値計算の実問題への応用研究集会（招待講演）

４．発表年
2018年

１．発表者名
藤井采人, 石井大輔

２．発表標題
証明支援系 Coq を用いた有界モデル検査アルゴリズムの検証

３．学会等名
第16回ディペンダブルシステムワークショップ

４．発表年
2018年

１．発表者名
藪 智仁, 石井大輔

２．発表標題
Why3 を用いた区間演算プログラムの検証

３．学会等名
第16回ディペンダブルシステムワークショップ

４．発表年
2018年

１．発表者名
泉 翔太，石井大輔，美添一樹

２．発表標題
スケーラブルな並列探索による最適化問題の求解

３．学会等名
第167回HPC研究会

４．発表年
2018年

１．発表者名
井上晃輔，石井大輔

２．発表標題
Acumen を用いたハイブリッドシステムの統計的モデル検査

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会

４．発表年
2019年

１．発表者名
武仲紘輝，石井大輔

２．発表標題
Simulink モデルの SMT-LIB エンコード方法に関する実験

３．学会等名
電子情報通信学会システム数理と応用研究会

４．発表年
2019年

１．発表者名
小嶋翔太，石井大輔

２．発表標題
Duracz らの操作的意味論に基づく ハイブリッドシステムの高信頼シミュレータの実装

３．学会等名
電子情報通信学会システム数理と応用研究会

４．発表年
2019年

１．発表者名
藤井采人，石井大輔

２．発表標題
証明支援系 Coq を用いた 有界モデル検査アルゴリズムの検証

３．学会等名
情報処理学会プログラミング研究会

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

PROMPT
https://www.gaio.co.jp/products/prompt-2/
Encoded results of Simulink models in SMT-LIB https://zenodo.org/record/6781295#.ZC6hrRVBwqs
Artifact for NFM'22 Submission
https://zenodo.org/record/6387089#.ZC6eQRVBwqs
SAT-based Model Checking in Coq
https://github.com/dsksh/coq-smc

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	上田　和紀 (Ueda Kazunori) (10257206)	早稲田大学・理工学術院・教授 (32689)	
研究協力者	青木　利晃 (Aoki Toshiaki) (20313702)	北陸先端科学技術大学院大学・先端科学技術研究科・教授 (13302)	
研究協力者	冨田　尭 (Tomita Takashi) (80749226)	北陸先端科学技術大学院大学・先端科学技術研究科・准教授 (13302)	

6．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	米崎　直樹 (Yonezaki Naoki) (00126286)	東京電機大学・システムデザイン工学部・研究員 (32657)	
研究協力者	美添　一樹 (Yoshizoe Kazuki) (80449115)	九州大学・情報基盤研究開発センター・教授 (17102)	
研究協力者	アレクサンドル　ゴールドシュタイン (Alexandre Goldztejn)	フランス国立科学研究センター・LS2N・Research associate	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
フランス	CNRS			
ベトナム	PTIT	VNU University of Science, Hanoi		