

令和 2 年 6 月 17 日現在

機関番号：17102

研究種目：基盤研究(C)（一般）

研究期間：2017～2019

課題番号：17K05346

研究課題名（和文）関係計算の形式化を用いた数学とソフトウェア検証のための理論構築

研究課題名（英文）Theory of relational calculus for formal verification of mathematics and software programs.

研究代表者

溝口 佳寛 (Mizoguchi, Yoshihiro)

九州大学・マス・フォア・インダストリ研究所・教授

研究者番号：80209783

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）：本研究の目的は、高信頼ソフトウェア開発の基礎となる数理論理学や離散数学、特に計算機による自動検証可能な形式証明を意識した関係計算による証明を用いた数学体系を広げることである。特に、関係計算系の基本公理やデデキント圏の公理をCoq定理証明支援系で定式化し、関係、関数に関する補題や定理を形式的に与えた。また、射の結合に関する基本補題の集積と自動証明を行う手順きをタクティクスとして実現した。さらに、Coq定理証明支援系の初歩的な補題を具体例とともに整理し、紹介文書、および、形式証明集を公表した。

研究成果の学術的意義や社会的意義

本研究は高信頼ソフトウェア開発の基礎となる数理論理学や離散数学、特に計算機による自動検証可能な形式証明を意識した関係計算による証明を用いた数学体系を広げることである。近年の計算機能力、および、定理証明支援系ソフトウェアの進歩により、数値計算、数式処理計算のみならず、論理計算についても自動検証可能になり、四色定理、ケプラー予想など、計算機でしか厳密に検証出来ない数学定理の証明も発表されるようになってきている。このような背景のもと本研究では論理計算を内包する関係計算に主眼を置いた数学理論の再構築、形式証明データベースの作成など、自動検証可能な数学理論体系を提案するものである。

研究成果の概要（英文）：The purpose of our research is to construct a fundamental theory of mathematical logic and discrete mathematics, which supports the reliable software developments. In particular, we use mathematical proofs using relational calculations. We consider formal proofs that can be automatically verified by a computer. Basic axioms of relational calculus and axioms of the Dedekind category are formalized using the Coq proof assistant system. Further, we implemented tactics of accumulating basic lemmas and automatic proofs for a combination of morphisms. Our results including formalized basic lemmas of the Coq system have been released with an introductory document, as well as the certificate collections with concrete examples.

研究分野：理論計算機科学

キーワード：数理論理学 関係計算 形式証明 形式手法 モデル検査 圏論のモナドの形式化

1. 研究開始当初の背景

1976年に Appel と Haken らにより解決された平面地図塗り分け問題である「四色定理」は計算機を利用した証明されたことで広く知られている。しかし、その証明過程(場合分けの十分性など)や計算プログラムの正当性は簡単に人で検証できるものではなかった。それに代わる形で、2004年に Gonthier は、Coq 定理証明支援系を用いて、グラフ理論の基本定理たちの形式証明ライブラリとともに四色定理の完全な形式証明を与えた。さらに、2012年には整数論の基本定理たちの形式証明ライブラリとともに群論の奇数位数定理の完全な形式証明を完成している。

1998年に Hales により提出された、3次元空間の球面充填に関する問題(ケプラー予想)の証明は査読者たちによる検証が得られなかったが、Hales 自身らにより計算機で検証可能な形式証明の構築が2003年より進められ、2014年8月10日にその自動検証可能な形式証明が報告された。その過程で、グラフの帰納集合や区間実数値演算に関わる形式証明ライブラリも構築されている。Voevodsky らはホモトピー理論と型理論を融合したホモトピー型理論の形式化(Univalent foundation project)に取り組み、新たな抽象数学の形式化を目指している。このように、2000年代に入り、定理証明支援系による**自動検証可能な形式証明による数学理論の構築**の重要性が認知され、**形式証明ライブラリの拡充**が始まっていた。

その中で、私自身が、形式証明とは独立に従前より行なっていたプログラム理論、オートマトン理論について圏論や関係計算理論を用いた定式化について、その礎の理論研究と同時に、応用のために必要な基礎数学としての形式証明の必要性の探求、プログラミング開発の現場での研究課題の調査や研究者・開発者らとの交流を行うと同時に、自動検証可能な形式証明としての関係計算理論の重要性を再認識し、既存の数学理論においても関係計算理論に基づく再構築の可能性を模索し、自動検証可能な数学理論の体系の確立への礎を築くために本研究を開始した。

2. 研究の目的

高信頼ソフトウェア開発の基礎となる数理論理学や離散数学、特に計算機による自動検証可能な形式証明を意識した関係計算による証明を用いた数学体系を広げることを目指して、研究計画を立案した。特に本研究では、論理計算を内包する関係計算に主眼を置いた数学理論の再構築、形式証明データベースの作成、および、抽象関係計算理論の構築をどこまで行えるか、また、自動検証可能な数学理論の体系をどこまで広げることが可能かを考察することが目的である。

3. 研究の方法

具体的には、以下の3つの項目について研究を進めた。

3.1 形式的体系としての関係計算理論の構築

集合論、圏論(トポス)などを基礎とする関係計算の一般理論は定式化されているが、その定式化は著者により公理の選択、証明手順が異なる。もちろん、同値であることが証明されている命題も少なくないが、それらの同値関係については未整理状態と言って良い。証明支援系を用いた形式化が行われれば、それらの同値関係も整理され、いつでも参照可能な形に整理される。このことは、従来の証明に不備がなかったかの確認にもなる。私自身の結果である圏論のモナドに関する関係計算理論、トポスをモデルにしたホーア論理によるプログラム検証体系、および、グラフ変換理論の関係計算による定式化について、関係計算証明を形式的に行うための理論の再構築を行なった。

3.2 計算実験環境としての関係計算システムの構築

応用可能な理論構築で大切なことは、計算実験環境の構築である。すなわち、計算実験のための形式証明ライブラリの実装である。証明支援系 Coq の形式証明で構成された理論の実験環境を Coq 内に構成することは、計算プログラムによる例示での命題候補の反例構築が可能になる。また、その計算プログラムの仕様検証の一般化としての新たな関係計算理論の命題の構築することも可能である。しかし、形式証明を備えた理論構築と具体的な自然数やそのリストやグラフ上の計算プログラムの仕様と検証のためのインターフェースを準備し、まとまった関係計算理論の形式証明ライブラリを構築した。

3.3 計算実験環境と理論構築との融合に関する問題点の解決と実応用

整数や実数などの数の計算理論である解析学においては、数値計算等のシミュレーションにより、理論構築の見通しを探ることが出来る。最近では、数だけでなく、数式も処理出来るようになって来たので、その判断材料は非常に大きくなっている。3.2の計算実験環境の構築により、離散構造物の計算プログラムの仕様検証の確認、すなわち、論理演算を含む関係計算代数式による概念の定式化を進めた。さらに、二項関係、圏論のモナド、ホーア論理、および、グラフ変換の形式化だけでなく、計算プログラムの仕様検証を通して、非形式証明の理論中の曖昧部分を顕在化する。そこでの、知見はさまざまな理論の形式化と計算プログラムの開発に役立つように分類し、実応用の視点から課題を整理した。

4 . 研究成果

3.1 について

博士課程大学院生(留学生)とともに関係データベース操作を具体的な関係計算式で与え、種々の証明をファジー関係計算式変形にて行う定式化を行い国際会議で発表した。また、ファジー関係における同値関係についても、関係計算式による定式化と計算証明を与えている。また、関係計算式を自動計算するソフトウェアの開発にも着手し、継続中である。

韓国釜山大学から九州大学フレンドシップ奨学生として滞在した博士課程大学院生とともに群演算から定まるケーリーグラフに関わる研究討論を行い、2018年2月韓国 Yeungnam 大学にて開催された代数と組合せ論の研究集会、および、2018年1月九州工業大学において開催された日本数学会九州支部会において発表した。

3.2 について

JSPS サマープログラムにおいて英国 UCL から来訪した博士課程大学院生とともに部分関数の圏論を用いた代数的形式化についての研究を進めた。その結果は2018年7月佐世保高専にて開催された Industrial Math Seminar において発表した。

CG(Computer Graphics)における図形変形の正当性については、2名の修士課程大学院生らとともに研究を続け、そのソフトウェア実装については、2018年7月の第1回論理と計算サマーセミナーにおいて発表した。

また、CGにおけるパターン画像生成にも応用される、Wang タイルによる与えられた境界条件を満たすタイルパターン生成アルゴリズムの提案とその正当性の証明を形式証明により行なった。レンガ型 Wang タイルと呼ばれるタイル集合による、境界条件を満たす解を線形時間で生成するアルゴリズムを提案し、その正当性証明を Coq 定理証明支援系により形式的に与えた。

3.3 について

2019年6月九州大学マス・フォア・インダストリ研究所短期研究員として滞在した株式会社スクウェア・エニックスの研究者らとゲーム開発へのモデル検査の適用に関して議論を開始した。彼らの最初のアイデアは、CEDEC2018(Computer Entertainment Developer Developers Conference)にて公表されている。その後も、関係計算理論、および、形式証明支援系の実応用に関する議論を継続中である。

多項式による最適化問題の求解ソフトウェアは高速かつ高性能なものが、既に開発されており、さまざまな論理問題についても、多項式による最適化問題で定式化することで解を求める方法が様々提案されている。この方法論に論理的側面、また、論理式変形による正当性証明の立場から、論理式表現の混合整数計画問題への変換について修士課程大学院生らとともに着手し、2017年11月日本数学会主催の異分野・異業種研究交流会ポスター発表等にて本数学ソフトウェアを紹介した。

本研究に関わる研究成果、講演発表資料、数学ソフトウェア等を一覧にし、ホームページに掲載した。<https://imi.kyushu-u.ac.jp/~ym/web/>

5. 主な発表論文等

〔雑誌論文〕 計3件（うち査読付論文 2件/うち国際共著 1件/うちオープンアクセス 1件）

1. 著者名 溝口佳寛	4. 巻 58
2. 論文標題 論理と計算について考えた人たち	5. 発行年 2018年
3. 雑誌名 数学セミナー	6. 最初と最後の頁 57-61
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 M.D.Akbar Y.Mizoguchi, Adiwijaya	4. 巻 971
2. 論文標題 Class dependency of fuzzy relational database using relational calculus and conditional probability	5. 発行年 2018年
3. 雑誌名 Journal of Physics: Conf. Ser.	6. 最初と最後の頁 12001
掲載論文のDOI（デジタルオブジェクト識別子） doi :10.1088/1742-6596/971/1/012001	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 該当する

1. 著者名 A.Derouet-Jourdan, S.Kaji, Y.Mizoguchi,	4. 巻 36
2. 論文標題 A linear algorithm for Brick Wang tiling,	5. 発行年 2019年
3. 雑誌名 Japn J. Indust. Appl. Math.	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） https://doi.org/10.1007/s13160-019-00369-z	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4件（うち招待講演 1件/うち国際学会 3件）

1. 発表者名 Y. Mizoguchi
2. 発表標題 Relational T-algebra and the category of topological spaces
3. 学会等名 Workshop on Logic, Algebra and Category Theory: LAC2018（招待講演）（国際学会）
4. 発表年 2018年

1. 発表者名 阿川真士, 溝口佳寛
2. 発表標題 位相空間の圏と同型な関係T代数の圏について
3. 学会等名 日本数学会2018年度年会
4. 発表年 2018年

1. 発表者名 M.D.Akbar Y.Mizoguchi, Adiwijaya
2. 発表標題 Class dependency of fuzzy relational database using relational calculus and conditional probability
3. 学会等名 The Internatiional Conference on Data and Information Science, ICoDIS2017 (国際学会)
4. 発表年 2017年

1. 発表者名 M.D.Akbar, Y.Mizoguchi
2. 発表標題 Formal Equivalence Classes Model of Fuzzy Relational Databases Using Relational Calculus
3. 学会等名 International Conference on Applied Computer and Communication Technologies (ComCom) (国際学会)
4. 発表年 2017年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

Workshop on Logic, Algebra and Category Theory http://www2.math.kyushu-u.ac.jp/~lac2018/ 関係計算の形式化を用いた数学とソフトウェア検証のための理論構築 https://imi.kyushu-u.ac.jp/~ym/web/

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
--	---------------------------	-----------------------	----